Secure Global Desktop™ Administrator Guide

A guide to the Management Console

TARANTE//A
Secure Global Desktop

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

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 Administrator Guide

Abstract

This book explains how to get started with the Management Console. It explains the concepts and provides help for using the Management Console. It also provides steps for troubleshooting. Further, it provides help on using the Secure Global Desktop Resource Kit. Additionally, this guide provides information on installing the Secure Global Desktop WBT add-on for Windows CE-based Wyse terminals.

ABOUT THIS BOOK 1

What's in this book? 1
Intended audience 1
Using this book 1
Book conventions 2
Related resources 2
Send us your comments 3
Printing This Book 4

INTRODUCTION TO SECURE GLOBAL DESKTOP 5

What's in this chapter? 5
What is Secure Global Desktop? 5
What are the benefits for system administrators? 5
Secure Global Desktop fits into your existing environment 5
Secure Global Desktop facilitates session management 6
Secure Global Desktop is simple to install and configure 6
Secure Global Desktop provides trouble-free object management 6
Secure Global Desktop enhances security 7
Secure Global Desktop facilitates operational-, capacity-, and strategic planning . 7
Secure Global Desktop facilitates license management 7
What is server-based computing? 7
What is application publishing? 8

GETTING STARTED 9

What's in this chapter? 9
Overview 9
Understanding the features 9
Application Server management 9
System administration 9
Application management 10
User management 10
Metering, reporting, and logging 10
Security 10
End-user experience 10
Understanding feature considerations 11
Application Servers 11
Configuration overview 11
Using a Windows 2000 Server or Windows 2000 Advanced Server 11
Using a Windows Server 2003 11

CONCEPTS 15

What's in this chapter? 15
Concepts 15
Secure product key 16
Types of product keys 16
Activation mechanism 17
Licensing 17
Domain objects 18
Active Directory synchronization 18
Retrieving list of groups and OUs 18
Retrieving application list 21
Connection settings 22
Connection settings templates 24
Delegated administrators in Secure Global Desktop 26
Delegated administrator tasks 26
Creating delegated administrators 27
Delegated administrators with multiple Admin roles 28
Prerequisites and restrictions 28
Client Groups 29
Terminology 30
Printers and Client Groups 31
Managing Client Groups 31
Use case analysis 32
Deployment scenario 38
Single Port Relay 39
Benefits 39
Traffic through Single Port Relay 40
Why choose port 443? 40
SSL handshake 40
Implementation details 41
Configuring a Relay Server 42
Managing Certificate for SPR 42
Monitoring 46
Diagnostics 47
Relay switch for Launch Pad 47
Single Port Relay in DMZ 47
DMZ 47
SPR in DMZ 47
Traffic Through DMZ Single Port Relay 48
Installing the Single Port Relay (SPR) Server Role on a DMZ Server – Prerequisites 49

Single Port Relay Server With DMZ Relay Server Role in the DMZ ***49***
Single Port Relay Server with Cascaded Relays ***50***
Implementation Details ***51***
Relay Configuration and DMZ Relay Configuration ***53***
DMZ Relay Configuration ***54***
Cascaded Relay Configuration ***54***
DMZ SPR Resource Kit ***54***
Changing Identity of DMZ Server Components ***55***
Displaying DMZ Server Certificate ***55***
Changing DMZ Server Certificate ***55***
Ticketing Authority **55**
Server Lockdown **57**
Manage Lockdown Policies **63**
..... **64**
View Lockdown Policy ***64***
Add Lockdown Policy ***64***
Update Lockdown Policy ***64***
..... **65**
Remove Lockdown Policy ***65***
Printer Driver Management Utility **65**
User Interface ***66***
IFS and Printer Data Compression **71**
Bandwidth Throttling Management **72**
Automated Administrator Tasks **72**
Change Password **75**
Connection Setting Monitoring **76**
Native Windows Client Connections **76**
Native Macintosh Client Connections **77**
Deploying Secure Global Desktop roles **78**
Role requirements ***79***
Server Identification in Secure Global Desktop ***81***
Web Server role ***82***
Load Balancer role ***82***
Relay Server role ***83***
Application Server role ***87***
Local server install **87**
Administrators and users ***87***
Limitations ***87***
Local server install and domain users ***88***
Publishing a Windows Desktop **88**

Steps for publishing a Desktop ***89***
Behavior ***89***
Security implications ***89***
Load balancing **90**
File associations **91**
Associating file extensions with applications ***91***
File associations and the user's computer ***92***
Interaction with other features ***93***
Security implications ***93***
Overriding file associations ***94***
Launch Pad **94**
Launch Pad features ***94***
Setting up the Launch Pad ***95***
Client upgrade **95**
Forcing a download ***96***
Pushing a client ***96***
Client on a computer ***97***
Shortcuts **98**
What is the Tarantella Client? ***99***
Installing the Tarantella Client and shortcuts ***99***
Configuring shortcuts ***100***
Printing **101**
Secure Global Desktop printing ***101***
How Secure Global Desktop Unidriver printing works ***104***
UniDriver printing ***105***
Linking to printers ***106***
Jobs framework **106**
File handling **106**
Configuration ***106***
Drive letter confusion on the client side ***107***
Security concern ***107***
System heartbeats **107**
Heartbeat variables ***107***
Diagnostics **109**
Reporting **112**
Active session management **114**
Session shadowing ***114***
Session disconnect and reconnect ***115***
Session log off ***116***
Achieving database redundancy **117**
Adding backup Database Server ***117***

Uses of the Database redundancy feature ***118***
Synchronization of the Backup Database Server ***120***
Seamless windows **120**
Security **121**
Design principles and practices ***121***
Features and security ***122***
Best practices ***124***
File logging **125**
Configuration settings for log file ***125***
Rollover of log file ***126***
Secure Global Desktop — Basic Configurations **126**
Single server configuration ***126***
Multi-server configuration ***127***
Advanced-server configuration ***128***

USING THE CONSOLE **130**

What's in this chapter? **130**
Management Console overview **130**
Management Console tabs ***130***
Common operations ***130***
What is application publishing? ***131***
Management Console Home tab **131**
Summary page ***131***
Getting Started page ***132***
Log On page ***132***
Download page ***132***
Product Keys page ***133***
About page ***134***
Management Console Manage tab **134**
Manage summary **134**
Manage applications **135**
Add application to Secure Global Desktop ***135***
Update application properties ***139***
Remove applications ***139***
Update file associations ***139***
Add applications to servers ***140***
Remove applications from servers ***140***
Add applications to groups ***140***
Remove applications from groups ***140***
Add applications to OUs ***141***

Remove applications from OUs ***141***
Add applications to users ***141***
Remove applications from users ***141***
Manage servers **142**
Add a server ***142***
Update server profile ***144***
Change server status ***144***
Diagnose server condition ***144***
Remove a server ***145***
Add roles to a server ***145***
Remove roles from a server ***146***
Add applications ***147***
Remove applications ***147***
Manage groups **147**
Add a group ***148***
Remove a group ***148***
Synchronize a group ***148***
Add applications to a group ***148***
Remove applications from a group ***149***
Manage OUs **149**
Add an OU ***149***
Remove an OU ***149***
Synchronize an OU ***150***
Add applications to an OU ***150***
Remove applications from an OU ***150***
Manage users **150**
Add a user ***151***
Remove a user ***151***
Add applications to a user ***151***
Remove applications from a user ***151***
Manage domains **152**
Add a domain ***152***
Remove a domain ***152***
Synchronize a domain ***152***
Manage Client Groups **153**
Add Client Group ***153***
Update Client Group ***155***
Update filters ***155***
Remove Client Group ***156***
Add applications to a Client Group ***156***
Remove applications from a Client Group ***156***

Add printers 156
Set default printer 156
Remove printers 157
Add clients 157
Remove clients 157
Manage connection settings 157
Add setting 158
Update setting 161
Remove setting 161
Select default 161
Manage Admin Roles 162
Add role 162
Remove role 163
Update role 164
Update delegated admin group 164
Add delegated admin users 164
Remove delegated admin users 164
Add groups to be controlled 164
Remove groups to be controlled 165
Add OUs to be controlled 165
Remove OUs to be controlled 165
Management Console Monitor tab 165
Overview page 165
Connections 165
Load Balancer 166
Database Connections 167
Relay Server 168
Job Status 169
Management Console Reports tab 169
Overview page 170
Sessions report 170
Applications report 171
Users report 171
Clients report 171
Servers report 172
Audit Log report 172
Product Key report 172
Management Console Options tab 173
Overview page 173
User options 173
Administrator options 175

Load Balancer options *177*
Database Servers options *178*
Relay Servers options *178*
System options *179*

TROUBLESHOOTING 182

What's in this chapter? 182
Troubleshooting Secure Global Desktop 182
Application-specific issues 183
Office XP application remains running after closing it *183*
User-specific issues 185
Add user fails *185*
User logon fails with "null" error *185*
Logon fails *185*
SSL enabled 186
Internet Explorer on Windows 95 client *186*
Secure Global Desktop version 186
Locating the version number for the Secure Global Desktop software *186*
Locating the server-side Tarantella Connection Manager version *187*
Active directory 188
Application list refresh based on group membership *188*
Client download 188
Considering administrative rights for the client computer *188*
Understanding the contents of the client computer's download *189*
Understanding the size of Client components *189*
Understanding why a user cannot log on to the Secure Global Desktop Launch Pad ***189***
Corrupt installation detected error *190*
Client problems 190
Application Server's screen saver appears on the client computer *190*
Client OS support *191*
Application launch hangs at Connecting to Application Server message *191*
Support for dial-up connections *192*
Launch Pad Favorites page is not displayed *192*
Painting issue with Microsoft's Office Assistant *194*
Application launch fails with Server Not Available error *194*
Copy and paste large files or bitmaps *195*
Desktop Windows commands and seamless windows mode *195*
Removing user name and domain from Wyse terminals *196*
Non-existent printer issue *196*
Second application launch from CE device *197*
Configuration 197

Specifying a command parameter for an application ***197***
Disconnecting a user versus logging off a user ***197***
Configuring published addresses for use with private/public networks ***198***
Running Secure Global Desktop with an ISA server ***199***
Cannot locate application executable when launching an application ***200***
Installing Secure Global Desktop on a domain controller ***200***
After installing the Application Server role, the server "blue screens" ***201***
Time-outs when using the Management Console ***201***
Cannot add groups from other domains ***202***
Changing the User Profiles storage location on an Application Server ***203***
Configuring SSL for the Management Console and Launch Pad sites ***204***
Supporting multiple domains ***204***
Diagnostics **205**
Settings Test failure ***205***
Disconnect **206**
Reconnecting a session after a client loses its network connection ***206***
Installation **206**
Cannot upgrade Secure Global Desktop ***206***
"Join Team" installation fails ***207***
Load balancing **208**
Explaining load balancing ***208***
All application sessions are being sent to one server ***208***
Explaining load limits ***209***
Launching spawned applications ***209***
Domain-specific issues **209**
Add Active Directory domain running on Windows Server 2003 from a different forest fails ***209***
Ports **210**
Changing the ports on which Secure Global Desktop runs ***210***
Identifying ports that must be opened on the client side for Secure Global Desktop ***210***
Configuring Secure Global Desktop for use with a firewall ***211***
Identify the ports that must be opened on the server side ***211***
Product keys **212**
IFSPort.dll fails to register during the install ***212***
Finding your Product keys ***212***
Managing your Product Keys ***213***
Expiry dates and product keys ***213***
Unable to add product key ***214***
Local file saving and printing **214**
Enabling/Disabling local file saving and printing ***214***
Using local file saving ***215***

A user cannot save to a local drive ***215***
Printer Drivers **216**
Adding new driver files to existing directories ***216***
Seamless windows **216**
Changing the client screen resolution ***216***
Server problems **217**
Terminal Server license error ***217***
The icon for the application is incorrect ***217***
Primary Database Server is down ***218***
Add server fails ***218***
Server shutdown ***219***
Installs on remote servers fail ***219***
Diagnose Server error ***220***
Incorrect Application Server Status ***220***
“Object Expected” Error ***220***
Server roles **221**
Problems adding the Application Server role ***221***
Secure Global Desktop Server roles ***221***
Shadowing **222**
A single session can only be shadowed once ***222***
Shadowing privileges and permissions ***222***
Notifying end users of session shadowing bids ***222***
Using a WTS Client for shadowing ***223***
Shortcuts **224**
Explaining the timing of shortcut creation ***224***
File associations **224**
File associations do not work as expected ***224***
IFS error ***225***
Launch Failed error ***225***
Load Balancing Failed error ***226***
Correct icons not displayed ***227***
SQL Server **227**
SQL server connection problem after an upgrade ***227***
Windows Terminal Services settings and seamless windows **228**
A WTS session cannot launch application in an NT 4 environment ***228***
Windows Terminal Services session with seamless windows ***228***
Launch Pad **229**
Netscape error ***229***
Slow logon ***230***
IE setting for SharePoint server ***230***
Security settings error ***231***

Event Log 232

SECURE GLOBAL DESKTOP TSE INSTALLING WBT ADD-ON FOR WINDOWS CE 2.12-BASED WYSE TERMINALS 233

What's in this chapter? 233
Getting Started 233
Installing Secure Global Desktop TSE WBT add-on for Wyse/WinCE 2.12 233

INSTALLING WBT ADD-ON FOR WYSE CE 2.12 OR WYSE CE .NET WITH RAPPORT 241

What's in this chapter? 241
Getting Started 241
Using Rapport to push the Secure Global Desktop TSE add-on 242

INSTALLING SECURE GLOBAL DESKTOP TSE CLIENT ON EMBEDDED TERMINALS. 245

What's in this chapter? 245
Getting Started 245
Installation. 245
Known problems 248
Write Filter Cache 248
Problems loading the Secure Global Desktop TSE Client software 248
Shortcuts not created 248

INSTALLING WBT ADD-ON FOR WINDOWS CE .NET-BASED WYSE TERMINALS 251

What's in this chapter? 251
Getting Started 251
Installing Secure Global Desktop TSE WBT add-on for Wyse/WinCE .NET 251

SECURE GLOBAL DESKTOP RESOURCE KIT 262

What's in this chapter? 262
Secure Global Desktop Resource Kit 262
Installing the CRK 262
Understanding the CRK 263
Exploring the CRK 263
Specifying options 264
Printing information 265
Checking administrator rights. 265
Stopping a command 265

Using the CRK **265**
Generating a transformed client ***265***
Synchronizing domain information with Task Scheduler ***266***
Altering the Secure Global Desktop Identity account ***267***
Adjusting the ports used by the Secure Global Desktop web sites ***267***
Migrating to a new Secure Global Desktop Database server ***267***
Reporting a support incident ***268***
Writing advance command lines **268**
Specifying multiple commands ***268***
Looping ***268***
Passing information between commands ***270***
Branching ***270***
Working with other tools ***271***
Putting it all together ***271***

ABOUT US **272**

What's in this chapter? **272**
About Tarantella **272**
About Secure Global Desktop from Tarantella **272**
Other sources of information **272**

SECURE GLOBAL DESKTOP CLIENTS **273**

What's in this appendix? **273**
Secure Global Desktop Clients **273**

ABBREVIATIONS **275**

What's in this appendix? **275**
Abbreviations **275**

COM+ COMPONENTS AND SECURE GLOBAL DESKTOP SERVICES **277**

What's in this appendix? **277**
COM+ Components **277**
Secure Global Desktop Services **277**

About This Book

What's in this book?

This book explains how to get started with the Management Console. It explains the concepts and provides help for using the Management Console. It also provides steps for troubleshooting. Further, it provides help on using the Secure Global Desktop Resource Kit. Additionally, this guide provides information on installing the Secure Global Desktop WBT add-on for Windows CE-based Wyse terminals.

Intended audience

This guide is for system and database administrators, and other persons who are responsible for deploying and administering Secure Global Desktop.

This guide assumes you are familiar with the following:

- Microsoft Windows 2000 Server Operating System
- Microsoft Windows Server 2003 Operating System
- Microsoft Windows 2000 Network Administration
- Microsoft SQL Server 7, SQL Server 2000, or MSDE
- Basic Web Server administrative functions

Using this book

This book is organized as follows:

TABLE 1. Contents and description

Chapter/Appendix	Brief Description
"Introduction to Secure Global Desktop"	This chapter presents an overview of Secure Global Desktop from Tarantella. It explains Secure Global Desktop and the benefits that you can derive from using Secure Global Desktop.
"Getting Started"	This chapter lists Secure Global Desktop features and helps you get started with the product. At a high level, this section identifies features, explains when to use them, how they work, and what you need to consider as you use them.
"Concepts"	This chapter explains the terms and concepts you should be familiar with to be able to use Secure Global Desktop applications effectively. This is the section that can answer questions such as how does Secure Global Desktop do this and why does Secure Global Desktop do that.
"Using the Console"	This chapter provides step-by-step procedures for using the Management Console to administer the Secure Global Desktop system.

TABLE 1. Contents and description

Chapter/Appendix	Brief Description
" Troubleshooting"	This chapter presents information about situations you may encounter and it also explains how to work with any related issues.
"Secure Global Desktop Resource Kit"	This chapter provides information about the Secure Global Desktop Resource Kit and using the CRK commands.
"About Us"	This chapter provides information about Tarantella and Secure Global Desktop.
"Secure Global Desktop Clients"	This appendix provides information on Tarantella Clients. It tabulates the Secure Global Desktop features along with their availability for various client operating systems.
"Abbreviations"	This appendix lists some common relevant abbreviations.
"COM+ Components and Secure Global Desktop Services"	This appendix lists the Secure Global Desktop Services and the COM+ Components.

Book conventions

Book conventions used throughout this book are as follows:

TABLE 2. Book Conventions in this Book

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.
`Courier` text	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 *italics*	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™ Administrator 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
- FAX:
  408.296.8600
  Attn: Technical Publications
- 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.

Introduction to Secure Global Desktop

What's in this chapter?

This chapter presents an overview of Secure Global Desktop™ from Tarantella®. It explains Secure Global Desktop and the benefits that you can derive from using Secure Global Desktop.

What is Secure Global Desktop?

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.

What is a Secure Global Desktop team?

A Secure Global Desktop team is a group of Secure Global desktop servers working together to provide a highly scalable and distributed Secure Global Desktop environment.

To create a Secure Global Desktop team, you need to install the Secure Global Desktop Server software on the Web Server. After this, you can bring other servers into the Secure Global Desktop team. All configuration information related to the servers in a Secure Global Desktop team is stored in a single database, which is also a part of the Secure Global Desktop team.

What are the benefits for system administrators?

This section explains the ways in which a system administrator benefits by using Secure Global Desktop.

Secure Global Desktop fits into your existing environment

Secure Global Desktop integrates into your existing enterprise environment by supporting the following:

- Microsoft's Active Directory or Microsoft's NT 4.0 Windows based domains
- Netscape or Internet Explorer Web browsers

- Microsoft IIS Web servers
- Microsoft SQL Server 2000, Microsoft SQL Server 7, or MSDE databases
- Windows Terminal Server for Windows® 2000, Microsoft Windows Server 2003

Secure Global Desktop facilitates session management

Secure Global Desktop provides powerful tools to help your system administrators manage active sessions.

Using Secure Global Desktop, a system administrator can do the following:

- View real-time dynamic data about active sessions
- Set thresholds to automatically permit, deny, or time-out a session
- Shadow, disconnect, log off, or send messages to one or more sessions
- Utilize and control load balancing on server teams
- Manage the number of sessions spawned for an application
- Manage file associations for applications
- Create delegated administrators to administer the system
- Create client groups based on specified criteria and assign applications, printers, and connection settings to the client groups

Secure Global Desktop is simple to install and configure

Secure Global Desktop resides in a complex environment; however, we have made Secure Global Desktop easy to setup and configure.

After completing the installation, a Secure Global Desktop administrator can quickly and easily configure the Secure Global Desktop system using the Web-based Management Console. The Management Console allows administrators to manage applications, domains, groups, OUs, client groups, servers, users, and other aspects of the Secure Global Desktop system.

Secure Global Desktop provides trouble-free object management

With Secure Global Desktop, object management is simple and powerful. Secure Global Desktop offers sophisticated administrative tools to provision, configure, monitor, and report on objects, their attributes, behaviors, and relationships.

To accomplish this, Secure Global Desktop works with your existing domain structure so that you can use only those objects within the Secure Global Desktop system that are valid within the existing corporate domain.

Adding a domain object from the existing domain to Secure Global Desktop is simple. Secure Global Desktop provides a wizard that displays a list of existing domain objects. A Secure Global Desktop administrator selects the object to use in the Secure Global Desktop application delivery environment by selecting the check box beside the object.

Maintaining domain objects in Secure Global Desktop is simple. Secure Global Desktop provides simple controls to synchronize the objects. Therefore, as the corporate domain administrator updates information, Secure Global Desktop can reflect the relevant information to your Secure Global Desktop environment.

Secure Global Desktop enhances security

Secure Global Desktop uses many features that enhance security. To help your system administrators keep your environment safe, Secure Global Desktop offers different levels and types of encryption, password and ID management, various types of launch and connection controls, and different types of compression.

Secure Global Desktop facilitates operational-, capacity-, and strategic planning

Secure Global Desktop provides information about your application delivery resources (CPU and memory) and their consumption. This information helps Secure Global Desktop administrators make informed decisions about the current and future allocation of resources.

Secure Global Desktop provides object- and session-level metrics to help Secure Global Desktop administrators answer questions such as who is using which resources when. Using these metrics, the Secure Global Desktop administrators can evaluate the sufficiency of the configured resources. For example, they can see the most frequently used applications, see the peak number of concurrent sessions, and determine if you have too many or too few application licenses.

Secure Global Desktop provides the data that you require to understand application usage trends. You can develop resource utilization targets, monitor application use, reallocate application delivery resources, and recognize when additional resources are required. In short, the Secure Global Desktop administrator obtains the data that is required to justify current resource allocation or reallocation, or to support planned resource acquisitions.

Secure Global Desktop facilitates license management

Secure Global Desktop provides tools to control the number of concurrent sessions.

Secure Global Desktop helps you meet your corporation's obligation to offer validly licensed applications sessions. Secure Global Desktop does this by monitoring the active application sessions against the concurrent third-party application licenses. In this way, Secure Global Desktop ensures that your corporation can comply with its third-party application contracts.

What is server-based computing?

In a server–based computing model, application processing happens on centralized servers. The application runs from the server, but displays on the client computers. This gives less powerful client computers access to resource-intensive applications without having to upgrade the client hardware.

Administrators can install applications and upgrade existing applications without having to touch all the desktops.

Server-based computing provides businesses ways to reduce PC expenses while enhancing security and resource availability.

What is application publishing?

Application publishing permits you to control application access to users, groups, and organizational units.

Once you have added an application into the system, you can provision this application to your users. Using Secure Global Desktop, you can provision applications to Domain Groups, Domain Organizational Units, and Domain Users.

Getting Started

What's in this chapter?

This chapter lists Secure Global Desktop features and helps you get started with the product. At a high level, this section identifies features, explains when to use them, how they work, and what you need to consider as you use them.

Overview

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

This section provides a list of features provided by Secure Global Desktop. This list aggregates features by business function.

Understanding the features

Developed by a team that includes experienced system administrators and data center managers, our products are designed with your needs in mind. Secure Global Desktop is designed to be intuitive and focused on the critical features required to gain the greatest efficiencies. Key features of Secure Global Desktop follow.

Application Server management

- Resource-based application-level load balancing
- One-click scalability™ of Secure Global Desktop components to any server "on-the-fly"
- Built-in redundancy of Secure Global Desktop components for multiple servers
- Real-time monitoring and management of server health from the console
- Full featured Terminal Services Web interface

System administration

- Central management of servers, applications, and users using Web-based Management Console
- Delegated administration
- High-performance UniDriver to eliminate printer driver conflict
- Self diagnostics of system functionality and user errors
- Command line tool for system maintenance

Application management

- One-click application publishing to users, groups, and organizational units (OUs)
- Support for multiple applications per RDP connection
- Intelligent file association
- Location-based application launch settings (for example, printer mapping)
- License management of third party applications

User management

- Central user authentication and access
- Tarantella Client Policy Engine™
- Dynamic, user-specific application shortcuts
- MSI based-seamless client deployment
- Auto download and version control of Microsoft RDP client

Metering, reporting, and logging

- Metering and reporting of application usage by user, client computers, and servers
- Peak concurrent usage by system and applications
- Exportable reports (for example, Microsoft Excel)
- Application usage metering and license management from published desktop
- Comprehensive audit trails and logs

Security

- Encryption of all sensitive information
- Secure Global Desktop Relay Server for easy firewall traversal via a single, configurable port
- Secure Terminal Server access
- Terminal Server lock-down to prevent uncontrolled sessions
- Location-based security policies (for example, shortcuts)
- Support for RSA SecureID authentication

End-user experience

- Seamless windows - applications operate seamlessly without Terminal Server frame
- Applications access via desktop shortcuts, Windows Start menu, documents with file associations, or browser-based via the Secure Global Desktop Launch Pad
- Local and network file saving
- Local, server, and network printing with client default printer support
- Automatic log-on and pass-through authentication
- Click-n-Go™ (one-click disconnect of active applications)
- Mulitple IFS connections from a single client

Understanding feature considerations

This section highlights limitations that may affect your use of some Secure Global Desktop features.

You need to consider this when you are planning the distribution of applications across application delivery servers or distributing Secure Global Desktop roles to servers.

Application Servers

In Secure Global Desktop v2.1 and later, the Application Server role, like all other roles, can be configured on a Windows 2000 Server or Windows 2000 Advanced Server with Terminal Services as well as on Windows Server 2003, Enterprise Edition and Windows Server 2003, Standard Edition.

Configuration overview

Before you begin, ensure that Secure Global Desktop has been installed.

Secure Global Desktop supports two servers: Windows Server 2003 and Windows 2000 with Windows Terminal Services configured in Application Server Mode.

Using a Windows 2000 Server or Windows 2000 Advanced Server

If you are using Windows 2000, you need to have the following installed:

- Service Pack 3
- IIS 5, if the server will be a Web Server
- MDAC 2.5 (without multiple-instance SQL server installations), MDAC 2.6 or MDAC 2.7 (MDAC 2.6 with Service Pack 1 is not supported)
- Terminal Services configured in Application Server Mode if the server will be an Application Server

NOTE

If you have more than one SQL Server 2000 instance running, so that the SQL Server is running in Named Instance mode, then you must have MDAC 2.6 or MDAC 2.7 installed on all Secure Global Desktop Servers. MDAC 2.6 or MDAC 2.7 must be installed on each Secure Global Desktop server, no matter which Secure Global Desktop server role each server holds.

Using a Windows Server 2003

If you are using Windows Server 2003, you need to have the following installed:

- IIS 6, if the server will be a Web Server
- MDAC 2.7
- Terminal Services configured in Application Server Mode if the server will be an Application Server

If you are using Windows Server 2003, you need to do the following before you install Secure Global Desktop.

- Install some Windows components
- Configure administrative settings for the server
- Start some services

The sections that follow discuss these in detail.

Installing the required Windows components

You need to add the Internet Information Services (IIS) along with support for Active Server Pages (ASP) if the server is to function as a Web Server. You need to add the WMI Windows Installer Provider on any additional servers, if you want to add servers to your team from the Console. In addition, you need to add the Terminal Server if the server is to function as an Application Server to allow the users to access the server.

NOTE

The Windows operating system CD should be present in the CD-ROM when you add these Windows components.

---

1. Select **Start>Control Panel>Add or Remove Programs**.
2. In the **Add or Remove Programs** dialog box, click **Add/Remove Windows Components**. The Windows Components wizard is launched.

To add support for ASP on the computer you will be using as the Web Server:

1. In the **Windows Components** panel of the Windows Components wizard, select the **Application Server** check box and click **Details**.
2. In the **Application Server** window, select the **Internet Information Services (IIS)** check box and click **Details**.
3. In the **Internet Information Services** window, select the **World Wide Web Service** check box and click **Details**.
4. In the **World Wide Web Service** window, select the **Active Server Pages** check box and click **OK** three times to return to the Windows Components wizard.

To add support for the installer used to install Secure Global Desktop on any additional servers through the Console:

1. In the **Windows Components** panel of the Windows Components wizard, select the **Management and Monitoring Tools** check box, and click **Details**.
2. In the **Management and Monitoring Tools** window, select the **WMI Windows Installer Provider** check box and click **OK** to return to the Windows Components wizard.

To install the Terminal Server on the computer you will be using as an Application Server:

1. In the **Windows Components** panel of the Windows Components wizard, select the **Terminal Server** check box, and click **Next** to install it. Follow the instructions in the wizard.
2. Select the **Relaxed Security** option.
3. Click **Finish** to complete the installation of the Terminal Server and close the Windows Components wizard.
4. Close the **Add or Remove Programs** window.

Configuring administrative settings

You need to configure the security settings for the COM+ component to allow distributed transactions over the network on the Database Server, verify that the group that you want to set as

the Secure Global Desktop Administrator group during the installation is in the Administrators group on the server now.

1. Select **Start > Settings > Control Panel > Administrative Tools**.
2. The **Administrative Tools** window opens.

To configure the COM+ component on the computer you will be using as the Database Server:

1. In the **Administrative Tools** window, double-click **Component Services**.
2. In the **Component Services** window, expand **Component Services>Computers** in the left pane to display the configured computers.
3. Right-click **My Computer** and select **Properties** from the shortcut menu.
4. Click the **MSDTC** tab and click **Security Configuration**.

NOTE

You may need to wait for a few seconds as the MSDTC tab may take some time to appear.

---

5. Select the **Network DTC Access** check box and verify that the **Network Administration**, **Network Client Access**, and the **Network Transactions** check boxes are selected.
6. Click **OK** twice to save your settings.

To verify the existence of the Secure Global Desktop administrator group in the Administrators group on a server:

1. In the **Administrative Tools** window, double-click **Computer Management**.
2. Expand **Local Users and Groups** in the left pane, and select **Groups**.
3. Double-click **Administrators** in the left pane to open the **Administrators Properties** dialog box.
4. Verify that the group you want to specify as the Secure Global Desktop administrators group during Secure Global Desktop installation is in the **Members** list and click **OK**.

Starting the required services

You need to start the Theme and Windows Audio services on the Application Servers — if the applications are likely to use these services — before you install Secure Global Desktop.

1. In the **Administrative Tools** window, double-click **Services**.
2. In the right pane of the **Services** window, double-click **Themes** to open the **Themes Properties** dialog box.
3. Select **Automatic** from the **Start-up type** list and click **Apply**.
4. Click **Start** to start the service.
5. Click **OK**.
6. In the right pane of the **Services** window, double-click **Windows Audio** to open the **Windows Audio Properties** dialog box.

7. Repeat Steps 3 to 5.
8. Close the **Services** window, and then close the **Administrative Tools** window.

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. This is the section that can answer questions such as how does Secure Global Desktop do this and why does Secure Global Desktop do that.

Concepts

This chapter explains the following concepts:

"Secure product key"

"Domain objects"

"Active Directory synchronization"

"Connection settings"

"Delegated administrators in Secure Global Desktop"

"Client Groups"

"Single Port Relay"

Ticketing Authority

"Local server install"

"Publishing a Windows Desktop"

"Load balancing"

"File associations"

"Launch Pad"

"Client upgrade"

"Shortcuts"

"Printing"

"Jobs framework"

"File handling"

"System heartbeats"

"Diagnostics"

"Reporting"

"Active session management"

"Achieving database redundancy"

"Seamless windows"

"Security"

"File logging"

"Secure Global Desktop — Basic Configurations"

Secure product key

Secure Global Desktop uses secure product keys to prevent the keys required to use the product from being passed around to other people. Secure Global Desktop uses four types of keys.

Types of product keys

Secure Global Desktop can be installed with either an evaluation key or a base key. An evaluation key expires 30 days after installation. A Base Key needs to be added to the system to be able to use it. The base key expires 60 days after installation. The system has to be activated with an activation key. An upgrade key can be added any time to increase the number of Secure Global Desktop licenses.

This section describes the four different types of product keys.

Base key

If you installed your product with a base key, you will not be able to delete the base key. You can only increase the numbers of licenses by using an upgrade key. An upgrade key will upgrade the number of licenses available to your Secure Global Desktop solution.

The base key expires in 60 days. Once a base key is entered, administrators will have to generate an activation request that is a combination of the base key in the system and some installation specific data. The administrators should send this activation request to Tarantella.

Activation key

A key generated by Tarantella using the activation request sent by a Secure Global Desktop administrator. An administrator can use an activation key only on the Secure Global Desktop installation where its corresponding activation request was generated.

NOTE

Tarantella keeps track of all the base keys activated. If somebody attempts to reuse the same base key on a different installation, the activation key request is rejected by Tarantella. Further, a combination of base of key and activation key cannot be reused, because the activation key is 'tied' to the Secure Global Desktop installation on which it was generated.

Upgrade Key

You can purchase an upgrade key when you are ready to upgrade the number of licenses available to your Secure Global Desktop solution permanently. You can purchase an upgrade key for as few as five additional licenses. Upgrade keys are tied to the base key in the system, and upgrade keys from one system cannot be used on another system. You can delete the upgrade keys that exist in the system.

Evaluation key

An evaluation key commonly expires in 30 days. The number of licenses granted for the evaluation key depends upon the situation. You can increase of the number of licenses in the evaluation system by using an Evaluation upgrade key.

NOTE

It takes a few minutes for a product key that is added to the Secure Global Desktop System to take effect.

Activation mechanism

An evaluation key expires 30 days after the system install, and a base key expires 60 days after the system install. After the administrator adds the base key to the system, an **Activate System** link is available in the left pane. Once the system is activated, the **Activate System** link is no longer displayed on the Console. Administrators need to activate the base key in the system. Once the base key has been activated, the system is fully functional and the base key does not expire. Any additional upgrade keys in the system do not need activation.

NOTE

The administrator can generate an activation request only if the system is using a base key. If the system is using an evaluation key, the Activate System link is not available on the console.

Steps for activation

Following are the steps an administrator should follow to activate the system after installing Secure Global Desktop with a base key.

1. The administrator launches the console and goes to the **Home>Product Keys>Activate System** page to generate an activation request string.
2. The administrator emails this activation request to Tarantella support at the email ID keys@tarantella.com.
3. Tarantella support generates an activation key using the activation request string. For more information, refer to "Activate System".
4. The activation key is emailed to the administrator.
5. The administrator adds this new activation key from the console. For more information, refer to "Add Key".
6. The system is fully functional.

Failure to activate

If the administrator fails to activate the base key, the Secure Global Desktop team will stop accepting new application launches after 60 days from the date that this base key was entered into the system.

Licensing

Secure Global Desktop v4.0 offers Concurrent User Licensing.

Concurrent User Licensing

If the Secure Global Desktop administrator installs a base key with concurrent user license for, say 5 users, any five users can launch, logon to Secure Global Desktop, and launch applications concurrently. If a sixth user tries to launch an application, Secure Global Desktop does not license a session until one of the earlier 5 users exits all sessions. Hence, 5-user concurrent licensing means that not more than 5 users can have active/disconnected sessions concurrently.

Domain objects

Domain objects include items such as servers, groups, organizational units (OUs), and users.

Secure Global Desktop must use a domain object, because all the authentication and user-group membership information is stored at the domain level by Windows. With Secure Global Desktop v2.1 and later, it is also possible to do a local server install where the local server may or may not be a part of a domain. For more information, refer to "Local server install".

Secure Global Desktop snaps on to the existing domain of an enterprise to gain this access. It then retrieves user, group, rights, and authentication information. Secure Global Desktop operates with the two most common domains, the Windows NT Domain and the newer Active Directory.

The ability of Secure Global Desktop to snap on to an existing domain is important because this eliminates the need for Secure Global Desktop to recreate a second user directory. It also allows Secure Global Desktop to leverage the time administrators dedicate to designing, implementing, and managing the network's domain controllers.

Secure Global Desktop design optimizations

Secure Global Desktop implements the following design precautions when interfacing with this critical enterprise resource:

- It implements read-only rights to the domain.
- It does not write to the Active Directory.
- It limits the number of times it reads from the Active Directory to minimize the load placed on the domain controller.

Once an administrator understands the importance of non-invasive interaction with the existing domain, the administrator can easily appreciate other nuances of the Secure Global Desktop design.

Domain objects in Secure Global Desktop

In Secure Global Desktop Domains, Groups, OUs, and Users are domain objects. An administrator can add domain objects to Secure Global Desktop from the existing domains, and the administrator can synchronize the Secure Global Desktop domain objects with the existing domain objects periodically.

Active Directory synchronization

Whenever a user logs on to the Secure Global Desktop team, Secure Global Desktop performs a synchronization involving the steps that follow.

Retrieving list of groups and OUs

At each user logon, Secure Global Desktop retrieves a list of all groups and OUs to which the user belongs.

Group retrieval process happens for the following:

- AD domains

- NT4 domains
- Local Server

NOTE

An OU is an Active Directory specific feature and works only in case of an AD domain.

Group memberships are retrieved recursively and nesting of groups in Active Directory is considered.

For example, consider a user John who belongs to a global group called Company, and in turn, Company belongs to a local group called Engineering. Secure Global Desktop retrieves the following groups for John:

- Company
- Engineering

Similarly, if a user belongs to an OU, the complete OU hierarchy is retrieved. The following figure explains this concept.

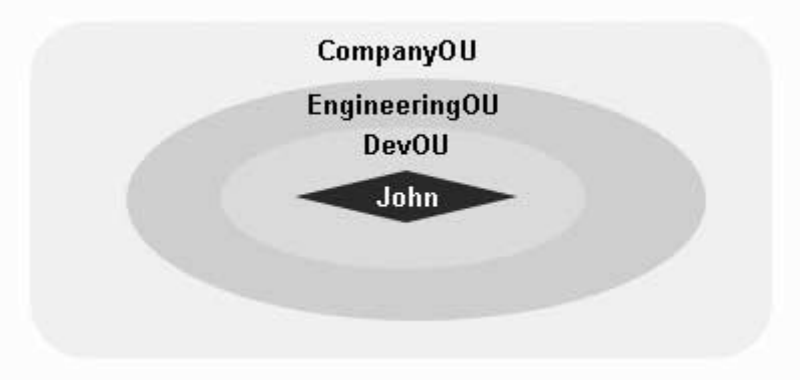


FIGURE 1. User and OU Hierarchy

If a user belongs to the Organizational Unit DevOU, DevOU belongs to EngineeringOU, which in turn belongs to CompanyOU, the logon process retrieves the following OUs:

- DevOU
- EngineeringOU
- Company OU

NOTE

If a user is added to a group in a different domain, the correct membership is retrieved only after replication of the relevant domains takes place.

Prerequisites

For Active Directory synchronization to take place, the user account selected as the Secure Global Desktop Identity account should have sufficient permissions to access information from the Active Directory.

To ensure this, the administrator needs to know the permission options chosen when the Active Directory was installed.

FIGURE 2. Active Directory Installation Permission Options

An administrator can choose from one of the following permissions options while installing Active Directory:

- Permissions compatible with pre-Windows 2000 servers
- Permissions compatible only with Windows 2000 servers

If the administrator installed the active directory with the **Permissions compatible with pre-Windows 2000 servers** option, no extra steps are required.

If the administrator installed the active directory with the **Permissions compatible only with Windows 2000 servers** option, then the system administrator should do one of the following to enable Active Directory synchronization:

- Identify the user account selected as the Secure Global Desktop Identity account during the Secure Global Desktop install, and add this account to the "Pre-Win2K compatible access group", “Account Operators”, or “Administrators” group in the Active Directory.

  NOTE

  The system administrator needs to do this for all the domains in the Secure Global Desktop system.

  While membership in the last two groups,” Account Operators” and “Administrators”, gives unrestricted access to the user and group accounts in the domain, membership in the “Pre-Win2K compatible access group” provides a more secure option. By default, all users and groups in domain have 'Read' permission granted to the “Pre-Win2k compatible access group”. This makes sure that the members of this group can only read information from the domain and cannot modify anything.
- Give 'Read' permissions to the Secure Global Desktop Identity account on all users and groups in the domain. For more information, refer to "Giving read permissions to Secure Global Desktop Identity account"

NOTE

After making this change, the administrator may have to restart Secure Global Desktop services and components on the Web Server for the change to take effect.

Giving read permissions to Secure Global Desktop Identity account

The administrator should give Read permissions to the Secure Global Desktop Identity account on all the users who will logon to Secure Global Desktop. To do this:

1. Run the **AD Users and Computers** snap-in.
2. Select **View>Advanced Features**.
3. Right-click a user and select **Properties** from the shortcut menu.
4. Click the **Security** tab.
5. Add the Secure Global Desktop Identity account.
6. Select the Secure Global Desktop Identity account from the Name list, and then from the **Allow** column in the **Permissions** list, select the **Read** check box.
7. Click **Advanced**, select the Secure Global Desktop Identity account from the Permission Entries list, and click **View/Edit**.
8. Click the **Properties** tab, and then from the **Allow** column in the **Permissions** list, select the **Read Group Membership** check box permission to the Secure Global Desktop Identity account.
9. Click **OK** thrice to save your settings.
10. Repeat Steps 2 to 9 for all users those in all domains who are likely to use the Secure Global Desktop system.

Alternatively, you can assign the required permissions to an OU and the set the permissions to cascade to all members of the OU. To do this:

1. From the tree in the left-pane, right-click an OU where all user accounts reside and select **Properties** from the shortcut menu.
2. Click the **Security** tab.
3. Add the Secure Global Desktop Identity account.
4. Select the Secure Global Desktop Identity account from the Name list, and then select the **Read** check box from the **Allow** column in the **Permissions** list.
5. Click **Advanced**, select the Secure Global Desktop Identity account from the Permission Entries list, and click **View/Edit**.
6. From the **Apply onto** list, select **This object and all child objects**.
7. Click **OK** thrice to save your settings.

Retrieving application list

After retrieving a complete list of groups and OUs, Secure Global Desktop checks the database to see if the Secure Global Desktop administrators have assigned any application directly to the users, or indirectly to the users by assigning the applications to groups and OUs. The user gets the assigned applications and the membership information is stored in the database.

This process ensures that the user logging on to Secure Global Desktop always gets a correct set of applications based on the user's current group and OU memberships.

NOTE

The system does not reflect any change to a user's membership 'during' the user's session. The user has to log off and log on again to make the membership changes known to Secure Global Desktop. Alternatively, the user can click the **Refresh Application List** *link on the* **Favorites** *page in Launch Pad.*

If a user has not logged on to Secure Global Desktop for some time and the user's group or OU membership has changed, Secure Global Desktop does not reflect this in the Console.

However, there is an option for a Secure Global Desktop administrator to synchronize group and OU information from the Console and to update application assignment. For more information on this option, refer to "Synchronize a domain".

Connection settings

What does this do?

One of the primary operations of Secure Global Desktop is making RDP connections between client and server computers. Connection settings objects set the parameters of these connections. The Secure Global Desktop connection settings object is similar to the Remote Desktop files that the Windows RDP client creates to save connection settings, except the Secure Global Desktop settings are stored in the Secure Global Desktop database instead of the client file system. Administrators can create connection settings to accommodate the needs of different network connections, users, or applications. Since Secure Global Desktop keeps connection settings objects in its database, connection settings are a management tool rather than an administrator's burden.

How does this work?

Secure Global Desktop divides the parameters of the connection settings into two sections:

- Those that govern the RDP connections
- Those that govern the Secure Global Desktop features

The RDP section contains settings that are familiar to any administrator of terminal services. These include display resolution and performance parameters. The Secure Global Desktop features section contains parameters that alter the way Secure Global Desktop enhances RDP. These enhancements include local resource sharing, load balancing, single port relay, and idle and disconnected timers. The Secure Global Desktop features section also includes Windows 2003 specific settings.

Administrators can create and manage settings from the Management Console's **Manage>Connection Settings** tab. From this tab, administrators can create a new connection setting based on predefined templates. Secure Global Desktop has templates for low, medium, and high bandwidth connections. Additionally, Secure Global Desktop has templates to run the Windows shell application, to run applications in full screen mode, for shared terminals, to run messenger applications, and to limit idle time in applications. This tab also allows settings to be altered, removed, and marked as the system default setting.

Administrators can assign a connection setting to an individual application to override the system's default setting. This feature allows administrators to accommodate the special needs of a specific application. For example, administrators may want a few applications to have a different idle time-out setting. When applications are assigned a special connection setting, they are launched in their own connection.

Initially, users connect with the setting that administrators mark as the default setting. If a user needs to override the default connection setting for a particular client, the user can choose the setting from the **Option** page of the Launch Pad. The chosen setting is remembered on the client computer. In this way, administrators can tailor the connections used on a particular computer to the network performance of the computer.

Thus, the administrator can assign existing Connection Settings to Client Groups and also to applications. In addition, a user can select Connection Settings from the Launch Pad.

Unspecified Connection Settings

The administrator can now leave Connection Settings unspecified at two levels:

- Select the "Unspecified" option for one or more values in a set of Connection Settings
- Select the "Unspecified" option instead of a set of Connection Settings for an application or Client Group

While adding or modifying Connection Settings, the administrator can now give “Unspecified” as the value for a Connection Setting to leave it unspecified. For example, for creating Connection Settings to apply to high security applications the administrator may specify Connection Setting values for Secure Global Desktop Drive Sharing, etc. and may not really care for things such as seamless windows, color depth etc. The administrator can create Connection Settings for secure applications and specify only the relevant Connection Setting values. The values for the other settings will be left as unspecified.

In addition, the administrator can now give “Unspecified” as the value for Connection Settings for an application or Client Group to avoid specifying Connection Settings at the Application level or the Client Group level.

Effective Connection Settings

The effective Connection Settings that are returned to the users can be a combination of the Client Group Connection Settings, Application Connection Settings, User Connection Settings, and Default Connection Settings. The precedence order for each Connection Setting individually is Client Group, Application, User. If none of these values is specified, the Connection Setting specified in the Connection Settings set as Default Connection Settings is used.

NOTE

The Connection Settings set as Default Connection Settings cannot have any unspecified values.

The following table explains this concept of effective Connection Settings for some settings when a user launches an application from a computer that is a part of a Client Group. The effective Connection Setting is shaded.

TABLE 3. Example of effective Connection Settings

Connection Setting Name	Client Group Connection Setting	Application Connection Setting	User Connection Setting	Effective Connection Setting
Screen Size	800x600	1024x768	640x480	800x600
Launch Full Screen	Unspecified	On	Off	On
Seamless Windows	Unspecified	Unspecified	Always	Always
Enable Single Port Relay	Off	On	Unspecified	Off
Logoff Idle Connections	Unspecified	Unspecified	Unspecified	Default

Suppose a user uses two Connection Settings - low bandwidth and high bandwidth (say, depending on whether he is working from home or from office). In addition, the administrator has set some properties for secure applications. It is now possible to run this secure application in low bandwidth and high bandwidth settings by leaving these specific Connection Setting values as unspecified for Client Group and applications Connection Settings. The effective Connection Setting value is then taken from the User Connection Settings.

NOTE

The administrator should not publish a desktop with connection settings that allow multiple launches in one session as logging off a published desktop closes all the application launches in the session.

Special Cases in Connection Settings

Certain applications such as “Shadow” and “Remote Windows Desktop” are considered as special applications. In case of special applications, the Connection Settings precedence is different; the Connection Settings assigned to that application are the effective Connection Settings. However, if any of the Connection Setting values is unspecified in the Connection Settings for this application, then the value for this Connection Setting is picked up from the following Connection Settings in the precedence order: Client Group>User>Default Connection Settings.

Connection settings templates

Secure Global Desktop provides a variety of connection templates that a user can choose from while adding connection settings. For a complete list of property definitions, see the following table on default values of connection settings.

TABLE 4. Default values of Connection Settings in templates*

	Default	**Bandwidth**			**Security**	**Kiosks/ Shared Terminals**		**Application Server types**		**Idle time-out**	**Messenger apps**	**Windows desktop**
		Low	**Medium**	**High**	**Secure apps**	**Internal**	**External**	**Windows 2000 only**	**Windows 2000 and Windows 2003**			
Display												
Screen Size Default	Default	800 x 600	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp
Launch Full Screen	Off	Off	Off	Off	Unsp	Unsp	Unsp	Off	Off	Unsp	Unsp	On
Color Depth	16 bit	8 bit	16 bit	24 bit	Unsp	Unsp	Unsp	8 bit	24 bit	Unsp	Unsp	Unsp
Experience												
Bitmap Caching	On	On	On	On	Off	Unsp	Unsp	On	On	Unsp	Unsp	Unsp
Enable Compression	On	On	On	On	On	Unsp	Unsp	On	On	Unsp	Unsp	On
Secure Global Desktop Features												

TABLE 4. Default values of Connection Settings in templates*

	Default	Bandwidth			Security	Kiosks/ Shared Terminals		Application Server types		Idle time-out	Messenger apps	Windows desktop
		Low	Medium	High	Secure apps	Internal	External	Windows 2000 only	Windows 2000 and Windows 2003			
Seamless Windows	Except during logon	Never	Except during logon	Except during logon	Unsp	Unsp	Unsp	Except during logon	Except during logon	Unsp	Unsp	Never
Launch in Existing Connections	If available	If available	If available	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp	Unsp
Reconnect	On	Unsp	Unsp	Unsp	Off	Off	Off	Unsp	Unsp	On	Off	Unsp
Enable Single Port Relay	Off	Unsp	Unsp	Unsp	Unsp	Off	On	Unsp	Unsp	Unsp	Unsp	Unsp
Logoff Disconnected Connections	Never	Unsp	Unsp	Unsp	10 min	10 min	10 min	Unsp	Unsp	10 hours	10 min	Unsp
Logoff Idle Connections	Never	Unsp	Unsp	Unsp	10 min	10 min	10 min	Unsp	Unsp	30 min	10 hours	Never
Client Drive Sharing												
Windows 2000	SGD	Off	SGD	SGD	Off	Off	Off	SGD	SGD	Unsp	Off	Unsp
Windows 2003	SGD	Off	SGD	SGD	Off	Off	Off	Off	SGD	Unsp	Off	Unsp
Client Printer Sharing												
Windows 2000	SGD	Off	SGD	SGD	Off	SGD	SGD	SGD	SGD	Unsp	Off	Unsp
Windows 2003	SGD	Off	SGD	SGD	Off	SGD	SGD	Off	SGD	Unsp	Off	Unsp
Unidriver (for SGD printing only)	If vendor driver not available	Never	If vendor driver not available	If vendor driver not available	Never	If vendor driver not available	If vendor driver not available	If vendor driver not available	If vendor driver not available	Unsp	Never	Unsp
Windows 2003 Specific												
Enable Serial Ports	On	Off	Off	Unsp	Off	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp
Enable Sound	On	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp
Desktop Background	Off	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp

TABLE 4. Default values of Connection Settings in templates*

	Default	Bandwidth			Security	Kiosks/ Shared Terminals		Application Server types		Idle time-out	Messenger apps	Windows desktop
		Low	Medium	High	Secure apps	Internal	External	Windows 2000 only	Windows 2000 and Windows 2003			
Show Contents of Window While Dragging	On	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp
Smooth Scroll	On	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp
Menu and Window Animation	On	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp
Themes	On	Off	Off	Unsp	Unsp	Unsp	Unsp	Off	Unsp	Unsp	Off	Unsp

* - Unspecified is tabulated as Unsp
SGD stands for Secure Global Desktop

Delegated administrators in Secure Global Desktop

Secure Global Desktop allows the administrator to create delegated administrators that have restricted administration rights on the Secure Global Desktop system. The administrator can create Admin roles and add one delegated group or a set of delegated users to these roles. Further, the administrator can assign specific tasks to each role. The administrator can specify the groups and OUs controlled by each role. Each member of the group, or an individual user, to whom the administrator has delegated an Admin role, becomes a delegated administrator, and can perform the assigned tasks on the controlled groups and OUs added to the role.

The advantage of this feature is that the administrator can delegate tasks to users or groups without giving full control of the Console. Moreover, the administrator can restrict the groups that the delegated administrator manages.

Delegated administrator tasks

The administrator can assign one or both of the following tasks to each Admin role:

Monitoring

When an administrator assigns the Monitoring task to an Admin role, all the delegated administrators that are delegated this role can monitor sessions. They can monitor the sessions of all the users that either are members of the groups, or belong to the OUs the administrator has assigned to them as controlled groups. The delegated administrators can:

- View sessions of these users
- Shadow sessions provided they have the appropriate right on the Application Servers
- Send messages
- Disconnect sessions

- Log off sessions
- Monitor Load Balancer, Database Connections, Relay Servers, and Jobs. These are read-only pages; no action is supported on these pages.

NOTE

The **Summary** *page displays the total number of licenses currently consumed and not the number of licenses consumed by only the users that the delegated administrator can monitor.*

Application provisioning

When an administrator assigns the Application Provisioning task to an Admin role, all the delegated administrators that are delegated the role can provision existing applications to the users that belong to the groups or the OUs the administrator has assigned to them as controlled groups. The delegated administrators can:

- Assign applications to controlled users, groups, and OUs
- Revoke the assignment of applications to controlled users, groups, and OUs

Creating delegated administrators

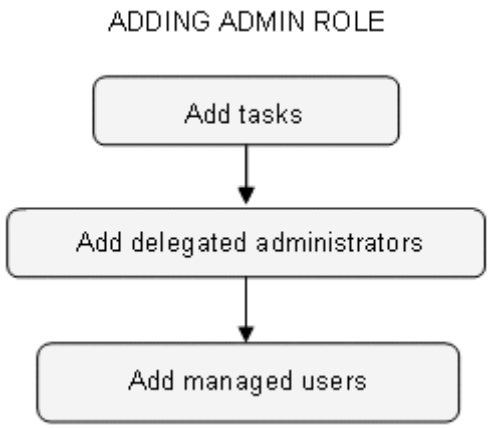


FIGURE 3. Steps to Add Admin Role

Following are the steps to create delegated administrators:

1. Add a role to the Secure Global Desktop team and identify it with a unique name. Assign one or more of the following tasks to the role:
   - Monitoring
   - Application Provisioning
2. Delegate the role to delegated administrators. The administrator can delegate the role to:
   - One group, where all members of the group become delegated administrators with this role
   - Multiple users
3. Assign controlled users the delegated administrators will control. The administrator can add:
   - Multiple OUs
   - Multiple groups

For more information, refer to "Add role".

Delegated administrators with multiple Admin roles

If an administrator assigns multiple roles with different tasks to a delegated administrator, and each of these roles has its own set of controlled groups and OUs, the delegated administrator can perform all those tasks that the administrator assigns to each role. However, the delegated administrator can perform each task assigned to an Admin role only on the controlled groups and OUs of each corresponding role.

NOTE

If an administrator is also made a delegated administrator, there is no effect on the administrator's rights. The administrator is not restricted to the delegated administrator's tasks, but can perform all the tasks on the system.

Consider the scenario in the following table.

TABLE 5. Delegated administrator scenario with multiple admin roles

Role	Marketing Admin	Sales Admin	First Admin
Tasks	Monitoring	Application Provisioning	Monitoring and Application Provisioning
Delegated administrators	Mary Robert	John Mary	John
Controlled Groups and OUs	Marketing OU Jill	Sales OU Jill	Net OU

In such a scenario, the three delegated administrators can execute the following tasks when they logon to the Console:

TABLE 6. Delegated administrator with resulting rights

Delegated Administrator	**Tasks: Groups and OUs**
John	Monitoring: Net OU Application Provisioning: Sales OU, Net OU, Jill
Mary	Monitoring: Marketing OU, Jill Application Provisioning: Sales OU, Jill
Robert	Monitoring: Marketing OU, Jill

Prerequisites and restrictions

Application provisioning

Delegated administrators cannot add new applications to the system. They can only provision existing applications.

Shadowing

Delegated administrators must have the appropriate rights on the application servers. For more information, refer to http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/ts_cmd_n_001.htm.

Task assignment

If an administrator changes the rights of a delegated administrator while the delegated administrator has the console open, the delegated administrator still continues to have access to the same pages as before the administrator changed the rights, until the Console is closed. However, the delegated administrator is unable to perform any of the tasks that have been removed.

Consider the case when a delegated administrator with Application Provisioning role logs on to the Console, and the administrator removes the delegated administrator from the role. The delegated administrator will still see the **Manage** tab in the console but will not be able to provision applications. If the delegated administrator selects any application and clicks the **Add Group** link, he will not see any groups to add to the application.

When the delegated administrator logs on the next time, the changed settings become effective and the Console displays the appropriate tabs based on the current Admin role membership. In the example mentioned earlier, the **Manage** tab will not be displayed.

Client Groups

A Client Group is a group of client computers. Secure Global Desktop allows you to group client computers based on criteria you specify from the Console. Secure Global Desktop Administrators can create a Client Group that will have client computers as members. A Secure Global Desktop v2.1 (or later) installation always creates a Default Client Group that will have all clients not assigned to any group.

When the client logs on to the Launch Pad or when the Connection Manager starts, the client sends its computer specific identification data to the server. The server matches the client data with Client Group filters and places the client in one of the groups. If the client fits into multiple groups, then the system places it in the default group with a flag indicating the conflict.

This unique feature thus allows the Secure Global Desktop administrators to

- Assign applications to client computers just as they assign applications to users, groups or OUs
- Assign printers to the client computers instead of depending on the user printer list
- Make groups of client computers based on some predefined criteria and then assign them connection settings or decide other client side behavior such as
  - Taking care of the security aspect by specifying whether to allow saving of passwords, allow creation of user short cuts.
  - Turning off Secure Global Desktop file associations.
  - Taking care of public terminal users by hiding the Tarantella Connection Manager tray icon. This feature is useful on terminals where the administrator expects users to launch client applications using shortcuts and does not expect them to delete/refresh shortcuts, or go to the Launch Pad.

NOTE

This unique feature is an important feature for server based computing world as it gives administrators more control on client computers.

Terminology

This section describes the terms used in connection with the Client Groups feature.

Client Group

A bucket created by an administrator where clients connecting to Secure Global Desktop are stored. The administrator can assign this group of clients some applications and printers that will be available to the client (user) if it matches the connection settings of the Client Group.

Sort

Sort refers to the process of finding out the appropriate Client Group for a client at the run-time.

Filter

Criteria defined by the administrator for a Client Group that decides the sorting behavior.

Default Client Group

A group created in Secure Global Desktop system during install. The system places the clients not belonging to any Client Group in this group. This group cannot be deleted and cannot have filters defined on it.

Contention flag

If a client can be placed in more than one group, the system assigns it to Default group with a flag indicating the conflict. This flag is called the Contention Flag.

Dynamic sorting

If every time a client connects, the system places the client in an appropriate Client Group, Dynamic Sorting is said to be ON in the system. The system does Dynamic Sorting based on the current Client Group settings the administrator makes on the Console. The administrator can select the **Sort Client into Client Group on each connect** check box on **Options>User** page in the Console to turn Dynamic Sorting ON.

If Dynamic Sorting is ON, then sorting occurs each time the client connects to the server, and thus the Client Group assigned to this client is updated each time the client connects.

NOTE

Dynamic Sorting is OFF by default.

If the administrator does not turn Dynamic Sorting ON, then sorting occurs only when the client connects to the server for the first time after a client group is assigned to this client. In this case, the assigned client group for this client changes only if:

- The administrator removes the client from the Client Group using the **Manage>Client Groups>Remove Clients** page on the Console.
- The administrator moves this client into another client group using:
  - **Manage>Client Groups>Remove Clients**
  - **Manage>Client Groups>Add Clients**
  - **Manage>Client Groups>Update Filters**

NOTE

Uninstalling and reinstalling the Tarantella Client from the client computer also forces re-sorting.

Printers and Client Groups

An administrator can assign printers to Client Groups. When a user launches an application on an Application Server from a client computer in the Secure Global Desktop system, the user has access to the client computer and the Application Server's printers for printing. However, if the client computer is sorted to a Client Group, the printers assigned to the Client Group are also available. In addition, the default Client Group filter overrides the default printer set on the client for applications launched through Secure Global Desktop.

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

Printer enumeration

The **Add Printers** page in the **Add Client Group** sequence and the **Add Printers** sequence enumerates printers. Using this page the administrator can assign printers to a Client Group.

When the page displays for the first time, it enumerates all the printers in the default domain, the default domain being the domain to which the Web Server belongs. Using the **Domain Name** field the administrator can search for printers in another domain.

NOTE

A trust relationship must exist between the domain to which the Web Server belongs and the domain being searched for printers.

The Domain Name and Printer Name are case-insensitive. If the administrator initiates a printer search leaving the **Domain Name** field blank, the page enumerates the printers in the domain to which the Web Server belongs.

Additionally, the administrator can use the **Name** field to search for a particular printer in the domain specified. In this case, a domain search is initiated for the printer in the domain specified. Printer Name can also be the full UNC path of the printer, or the first few characters in the Printer Name.

Managing Client Groups

In order to manage Client Groups the administrator needs to

- Create a Client Group
- Assign properties to the Client Group

Create a Client Group

An administrator can create a Client Group in two ways:

- Policy based automatic sorting, based on one or more of the following filters
  - IP address of the client computer
  - NetBIOS name of the client computer
  - Client operating system

- OU of the client in the domain

For example,

IP address is between 192.168.5.10 to 192.168.5.50

OR between 192.168.6.110 to 192.168.6.210

OR client computer NetBIOS name is AB* OR *M

OR OS type is Windows 95 *OR* Windows 98

OR Client OU is SalesOU

In this case, the system sorts a client computer satisfying even one of the conditions to this Client Group.

- Manually, by adding individual clients from Default Client Group. The members of the Default Client Group that are automatically added to the Client Group due to policy based sorting appear selected on the page.

Assign properties to the Client Group

An administrator can assign the following to each Client Group

- Applications
- Direct settings
- Restrictions on
  - Allowing save password
  - Allowing user shortcuts creation
  - Disabling Secure Global Desktop file associations
  - Hiding Tarantella Connection Manager tray icon
- Printers
- Connection settings

For more information, refer to "Add Client Group".

Supported clients

- Windows PC client
- Windows CE client

Use case analysis

New system install

When Secure Global Desktop is installed:

- The default client group is created as a holder for any client computer that accesses Secure Global Desktop.
- There is just one client group ‘Default Client Group’, and it gets all the clients.
- No filters can be set on this default group.
- By default, there are no applications assigned, and no printers added to this group.
- By default, there are no Connection Settings assigned to this group so that it does not override user or application connection settings.

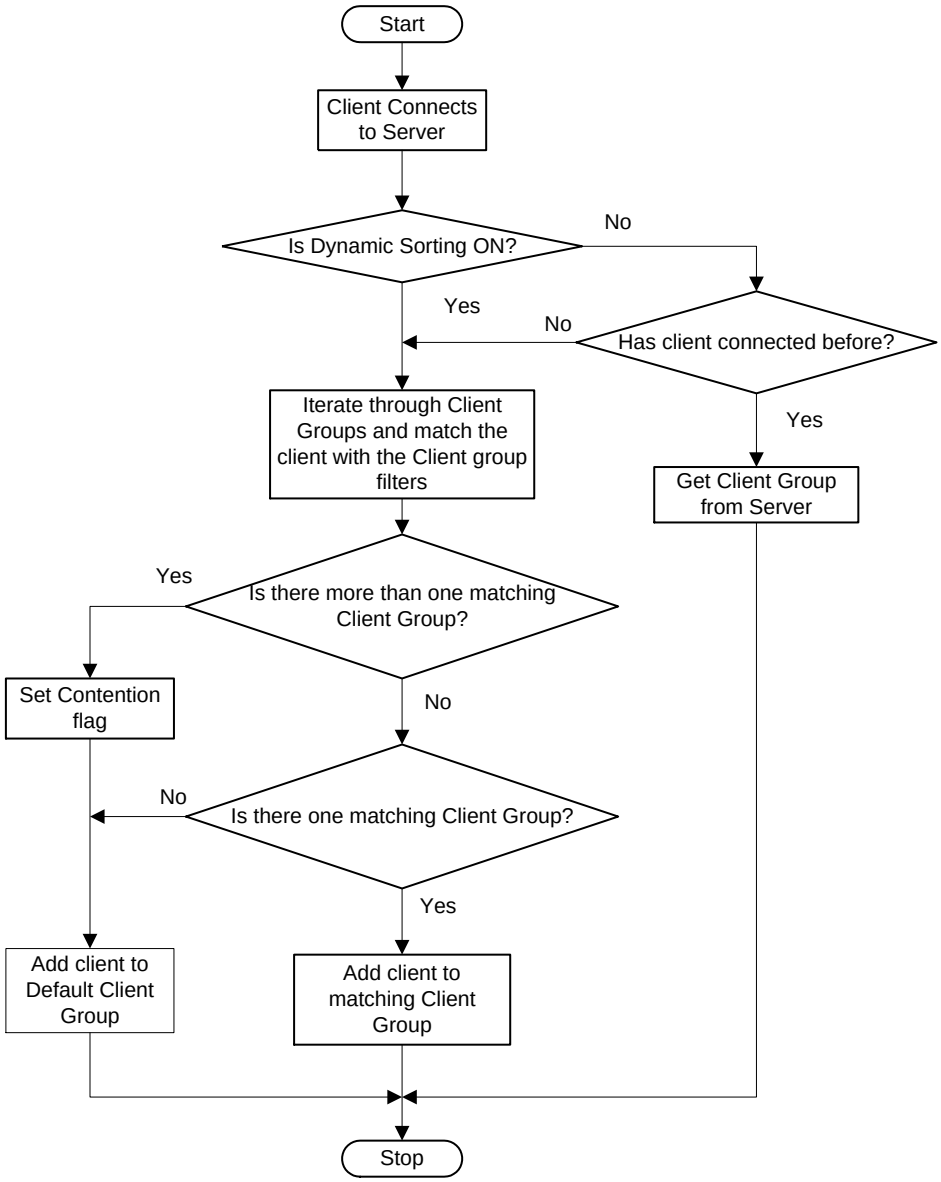
Administrator adds new client group

An administrator adds a new Client Group by following the steps mentioned in "Add Client Group".

Client connects to server

When a client connects to a server:

- Tarantella Connection Manager sends computer specific information to the Secure Global Desktop server.
- Server decides the Client Group for the client based on the following flow-chart.



1. If the client matches the policy for one Client Group, the client is placed in that Client Group.

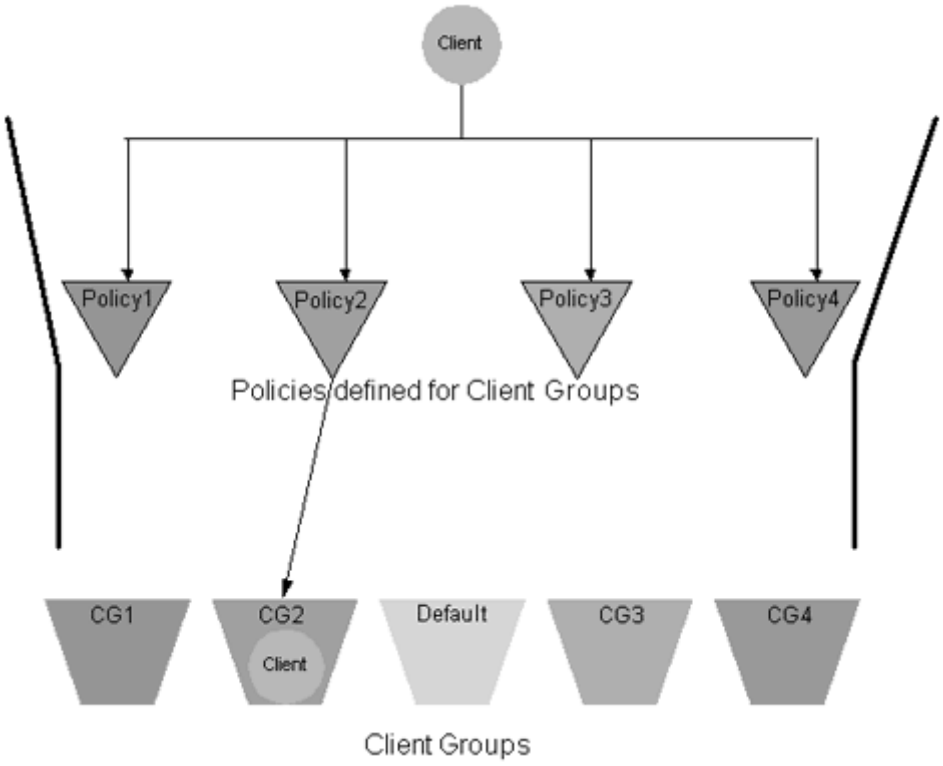


FIGURE 4. New Client is placed in a Client Group

2. If the client matches more than one policy, the Contention flag is set and the client is placed in Default Client Group.

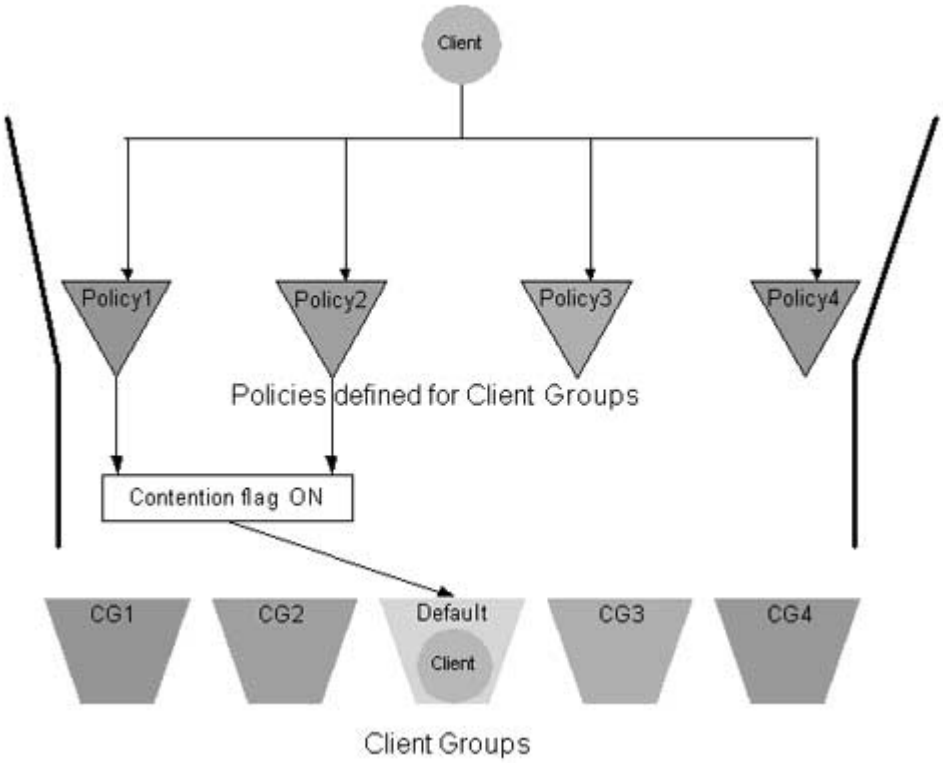


FIGURE 5. New Client is placed in Default Group

The client receives a list of printers assigned to the Client Group.

NOTE

Even if a client has a default printer, for applications launched through Secure Global Desktop, the default printer for the Client Group to which the client belongs becomes the default printer.

The Tarantella Connection Manager tray icon is displayed or hidden depending on the settings for its Client Group. In case the Connection Manager is used to connect to multiple Secure Global Desktop teams, the icon is hidden if even one of the teams has a setting to hide it. If administrator changes the option on the server from “show tray icon” to “hide tray icon” or vice-versa then the status of icon changes the next time the client computer connects to a Secure Global Desktop server.

Client launches an application assigned to Client Group

When a user launches an application on the client computer and the application is assigned to a Client Group in the Secure Global Desktop team:

- Authentication dialog box appears
- The application is launched if user authentication is successful.

The precedence for determining the value of EACH setting in the connection settings is:

1. Client Group
2. Application

3. User

For a specific connection setting item, if no connection setting is assigned for the Client Object, or the value for the Connection Setting item is unspecified, the system takes the setting from Application Connection Settings.

If there is a setting for Application, the system takes it and ignores the setting for the User for this item. However, if no connection setting is assigned for the Application, or the value for the Connection Setting item is unspecified, the system takes the setting from User Connection Settings.

If the setting for the item is not defined in any object, then the system takes it from default Connection Settings.

NOTE

Default Connection Setting cannot have unspecified values.

Administrator manually moves client between Client Groups

Any manual moves of the clients between Client Groups do not make sense if dynamic sorting is ON. This is because even if the administrator moves the client to another Client Group it will be re-sorted when the client connects the next time, based on the policies. Hence, the administrator must switch the dynamic sorting off before making any manual overrides to the sorting mechanism.

- A Secure Global Desktop administrator can view the clients present in one Client Group at a time.
- The administrator can remove clients from the group. The removed clients move to Default Client Group.
- The administrator can add clients that have already been sorted to other Client Groups to this Client Group when Dynamic Sorting is OFF.

The diagram that follows illustrates this.

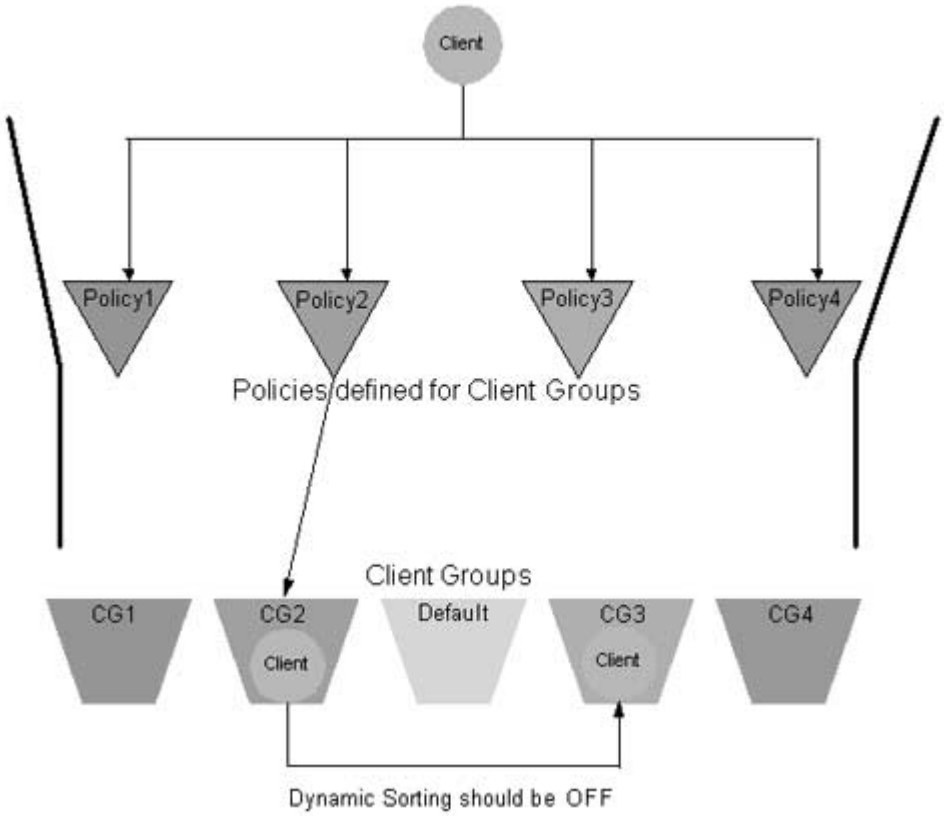


FIGURE 6. Client is moved to another Client Group

NOTE

When the administrator explicitly adds clients to a Client Group, the clients might not match the selection filters of the group.

Administrator deletes Client Group

Administrator can view all the Client Groups at one place on the Console and may select one or more groups for deletion.

- The selected Client Groups are removed from the database.
- Clients present in the group move back into Default Client Group.
- For clients computers that were in this client group, the client shortcuts got from this Client Group are removed whenever the next refresh shortcuts happens.

Administrator updates Client Group

Administrator has the ability to update Client Group properties, add or remove applications, add or remove printers, set default printer, add or remove clients, and update filters for a Client Group

After the administrator updates the filter, it is possible that clients in the group do not match with the new filter.

- If Dynamic Sorting is ‘On’, then the next time the client connects to the Secure Global Desktop team, its Client Group is updated accordingly.

- If Dynamic Sorting is ‘Off’, then the client stays in the same Client Group until the administrator moves him out.

NOTE

If administrator updates a Client Group and changes its filters, it is possible that clients already present in the group do not conform to the new filter, but remain in that group if Dynamic Sorting is ‘Off’. Administrator will have to move these clients to default group for ‘sort’ to take effect.

Deployment scenario

This section explains a typical deployment scenario using the Client Group feature.

Public Terminal

A hospital, where the application users are doctors of the hospital: There are 30 client computers and 1000 doctors who will be accessing the applications from these computers.

The procedure for setting up shortcuts on a public terminal is as follows:

1. Add a Client Group through the Console. Set the selection criteria such that all client computers to be used as these public terminals fall under this Client Group. Assign the applications whose shortcuts we want to create, to this Client Group.
2. Set the Client Group properties appropriately. We recommended that you select the **Do Not Allow Creation of User Shortcuts** check box. If users login to Secure Global Desktop through Launch Pad on these computers, this setting does not allow their user application shortcuts to overwrite the Client Group shortcuts either on the Start menu or the desktop.

NOTE

To disable access to the Launch Pad through the Tarantella Connection Manager tray icon, on the **Options>System>Update System Options** *page, delete the Secure Global Desktop Team Name.*

3. Select the **Do Not Allow Save Password** check box and **Disable Secure Global Desktop File Associations** check box.
4. To the relevant Group, assign the applications to needed by the doctors. For example, if the doctors belong to the Domain Group “GroupDoctors”, then assign the applications to this group.
5. The Client Group shortcuts need to be created on the client computers, the public terminals in this case. Use some dummy domain user to which you have not assigned these applications. The preferred way to create Client Group application shortcuts is to transform the Tarantella Connection Manager msi and push it to the client computer or install the Tarantella Connection Manager as a local administrator.

NOTE

If you use a user who has these applications assigned, then these applications are not created as client applications.

Single Port Relay

The Single Port Relay (SPR) feature allows all the RDP and Secure Global Desktop traffic, except the Web traffic, to travel over a single port using the SSL protocol. This feature makes Secure Global Desktop more firewall friendly, so the administrator has more flexibility in deploying Secure Global Desktop. The standard SSL port 443 is generally open for communication in most server-client environments. Single Port Relay enhances security by using this SSL port as the SPR port, thus eliminating the need to open any other ports on the corporate firewalls. This brings down the number of ports that must be open — other than port 80 for Web traffic — to just one.

All traffic from clients is routed to the appropriate Application Server through the Single Port Relay. The administrator can configure more than one Single Port Relay Server.

Benefits

The use of a Single Port Relay Server provides the following benefits.

Only one open port

The administrator can configure the system to work on a particular port, which is already open on the firewall. For example, 443 — the well-known SSL port — is open most of the times.

Only one routable IP address

As the Single Port Relay Server relays the traffic between clients and all the Application Servers, the Application Servers can reside on the internal network. The Application Servers need not have a routable IP address. Only the Single Port Relay Server needs to have a routable IP address. This address can be a NAT address, which can also be mapped to an FQDN address.

Enhanced security

The shielding of Application Servers from external world, and the fact that a reduced number of ports are open on the firewall, makes the system more secure.

SSL handshake

The administrator can further enhance security by enforcing an SSL handshake between external clients and the Single Port Relay Server before it actually starts relaying the data to the internal Application Servers.

NOTE

This initial SSL handshake might be mandatory, as some firewalls require a proper SSL handshake, before they allow any traffic to pass through.

Single Port Relay does the following:

- On the client side, the Single Port Relay multiplexes the RDP and IFS traffic and transmits that on the same port.
- On the server side, Single Port Relay demultiplexes the traffic and forwards it to the appropriate Application Server as indicated by the Load Balancer.

Traffic through Single Port Relay

Single Port Relay handles the following:

- Internet File Sharing
- Printing
- RDP sessions

Why choose port 443?

Port 443 is the preferred port for Relay Servers as:

- 443 is the most commonly open port in corporate firewalls
- SSL handshake is sometimes required by some firewalls to allow traffic on port 443

The Relay Server can be configured to use any other available port. For more information, refer to "Relay Server role".

If you change the relay port, the existing connections are disconnected. However, the user can reconnect the disconnected sessions from the Launch Pad Connections page, depending on the connection settings.

SSL handshake

When enabled, the SSL handshake is done only for the initial session start. After that, the session is not encapsulated in an SSL session. The SSL handshake is only one-way. That is, only the server is authenticated by the client. The client is not authenticated by the server. Since each type of traffic — IFS, printing, RDP — have their individual encryption settings, they are not encrypted again. The administrator can enable handshake for all the Single Port Relays in the system from the **Options>Relay Servers>Update Options** page. For more information, refer to "Relay Servers options".

Implementation details

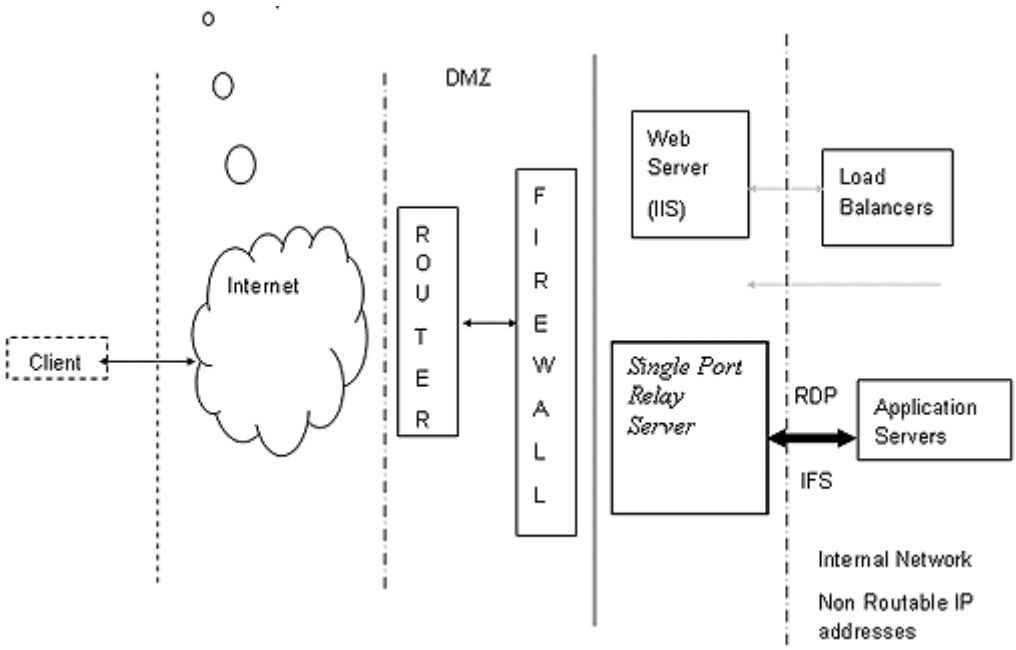


FIGURE 7. Single Port Relay in Secure Global Desktop

The Single Port Relay Server is a Service that runs on Windows 2000 Server or Windows Server 2003, which has routable IP address. This service listens on the specified port and forwards all the RDP or IFS traffic to the appropriate port on the Application Server. The Single Port Relay service listens on a configurable port (443 by default).

All the RDP and IFS data is sent to the Single Port Relay Server instead of the Application Server. The Single Port Relay forwards the data to the appropriate Application Server.

If the Single Port Relay is configured to use SSL handshake, then every connect first tries to establish a valid SSL session by completing a proper SSL Handshake. It is possible to configure different Single Port Relay Servers to use different "Server Authentication Certificate" type certificates. However, all the Single Port Relay Servers use the same port number. The Tarantella certificate is installed in the "Personal" folder of the computer account and Tarantella CA is installed in the "Trusted Root Certification Authorities" folder of the computer account when the relay server role is installed on the server. The Tarantella Certificate is valid for one year and the Tarantella CA is valid for 20 years. For more information on handling SPR certificate, refer to "Managing Certificate for SPR".

During uninstall, both the Tarantella certificate and the Tarantella CA are uninstalled from the "Personal" and the "Trusted Root Certification Authorities" stores of the computer.

NOTE

Web traffic is not tunneled through the Single Port Relay. It still uses either port 80 or port 443, or any other port depending on the Web Server configuration. Web Server still needs to be behind the firewall.

Configuring a Relay Server

The steps for configuring a Relay Server are as follows:

1. Update the Relay Server configuration to set the relay port and enable or disable SSL for all Relay Servers. By default, port 443 is the relay port and SSL is enabled. The administrator should make sure that the specified port:
   - Is available for use
   - Can be successfully bound to
   - Can listen successfully

   For more information, refer to "Relay Servers options"
2. Add the server to the Secure Global Desktop system. The administrator should know the NetBIOS name of the server. For more information, refer to "Add a server".
3. Add role to the server. The administrator can choose the certificate to use for SSL handshake if the system options have SSL enabled. By default, we install a Tarantella certificate to enable SSL handshake. To replace this certificate by another certificate, first install the certificate on the server that is to be the Single Port Relay Server, and then choose the certificate from the Console. The Console displays a list of certificates from the server's Personal certificate store. The administrator can specify a particular certificate file or use the default Tarantella provided certificate. For more information, refer to "Add roles to a server".

NOTE

After the certificate is changed, the administrator should restart the Secure Global Desktop Single Port Relay service.

The Single Port Relay Server starts functioning immediately after the administrator successfully pushes this role on to a server, without any need of further settings or manual configurations. For more information on deploying the Relay Server role, refer to "Relay Server role".

Managing Certificate for SPR

The administrator can configure the Single Port Relay to use SSL. SPR uses a certificate for SSL handshake. This section explains the type of certificate, its location, and step-by-step procedures for setting up SSL handshake.

Certificate Type that SPR requires

Certificates are of various types, some of which are:

- IP Sec
- Client Authentication
- Server Authentication
- Email Protection certificate
- Code Signing certificate

SPR requires "Server Authentication Certificate" type of certificate. The Tarantella certificate is installed in the "Personal" folder of the computer account and Tarantella CA is installed in the "Trusted Root Certification Authorities" folder of the computer account when the relay server role is installed on the server. The Tarantella Certificate is valid for one year and the Tarantella CA is valid for 20 years.

The administrator may configure the SPR to use any other certificate generated locally on a Certificate Server or obtained from a vendor such as VeriSign. Each SPR Server can use a different certificate.

Following are the steps the administrator should follow to generate a certificate on a local Certificate Server and use it on the SPR server:

1. Create a certificate on the SPR Server
2. Issue a certificate from the Certificate Server
3. Install the certificate on the SPR Server in the Personal store of the Current User
4. Export the CA from the Certificate Server
5. Import the CA to the Computer account on the SPR Server
6. Import the certificate to the computer account on the SPR server
7. Select the certificate for the SPR server from the Console

NOTE

The administrator needs to follow the steps for each SPR Server. However, the administrator can follow the steps for just one SPR Server and then use the same certificate for other SPR servers by exporting the certificate and the CA from the SPR Server on which they are installed, and importing them in the computer account of all the SPR Servers.

Following are the steps the administrator should follow to use a certificate issued by a certifying authority:

1. Import the certificate to the computer account on the SPR Server
2. Import the CA to the computer account on the SPR Server

NOTE

The administrator should follow the steps for each SPR Server in the Secure Global Desktop system.

Create a certificate on SPR Server

The administrator needs to create a certificate only if a locally generated certificate is to be used in the Secure Global Desktop system.

1. Open Internet Explorer and access the Certificate Server using a URL of the following format

   `http://<certificateserver name>/certsrv`

2. Click the **Request a Certificate** link, and then click the **Advanced Certificate Request** link.
3. Click the **Submit a request to this CA** link.
4. Enter the required details.
5. Select the **Server Authentication Certificate** option from the **Type of Certificate Needed** list.
6. If the certificate would be exported in PFX format, select the **`Mark Keys as Exportable`** check box.

7. Click **Submit**.
8. Click **Yes** on the message boxes that display to proceed.
9. Note down the **Request ID** that is displayed after the certificate is created. This is required when issuing a certificate.

Issue a certificate on the Certificate Server

The administrator needs to issue a certificate on the Certificate Server only if a locally generated certificate is to be used in the Secure Global Desktop system.

1. Select **Start>Programs>Administrative Tools>Certification Authority** to open the Certification Authority mmc snap-in.
2. Expand the tree on the left hand side pane and select **Pending Requests**.
3. Select the certificate with the Request ID you noted in Step 8 of "Create a certificate on SPR Server" in the right hand side pane.
4. Select **Action>All Tasks>Issue** or right-click the certificate and select **All Tasks>Issue** from the shortcut menu.

A message indicating that a certificate has been issued is displayed.

Install a certificate on the SPR Server

The administrator needs to install a certificate on the Certificate Server only if a locally generated certificate is to be used in the Secure Global Desktop system.

1. Open Internet Explorer and access the Certificate Server using a URL of the following format

   ```
   http://<certificateserver name>/certsrv
   ```

2. Click the **View the status of a pending Certificate request** link.
3. Identify the certificate based upon the Certificate Type (Server Authentication Certificate in this case), the date and the time and click on the certificate link.
4. Click the **Install Certificate** link.
5. Click **Yes** on the message boxes that display to proceed.

The certificate is installed on the SPR Server in the Personal store of the Current User.

Export the Certificate in .PFX Format to a file on the SPR Server

The administrator needs to do this only to use the certificate generated earlier instead of requesting multiple certificates.

1. Open the Certificates mmc snap-in for Current User.
2. Expand the tree in the left hand pane and select **Personal>Certificates**. The certificate that was installed should be listed in the right hand side pane.
3. Right-click the certificate and select **All Tasks>Export...** from the shortcut menu.
4. In the wizard select the **Yes, export private key** option. Accept all the other default options.
5. Enter the password and the name of the file along with the path.

The certificate is exported as .PFX file on your drive.

Export the CA in .CER format on the Certificate Server

The administrator needs to export the CA on the Certificate Server only if a locally generated certificate is to be used in the Secure Global Desktop system.

NOTE

The CA can never be exported in PFX format. It is exported only in PKCS and CER format.

For SPR we export the CA in .CER format.

1. Open the Certificates mmc snap-in for Current User.
2. Expand the tree in the left hand side pane and select **Trusted Root Certification Authorities>Certificates**.
3. Select the required CA from the list of CAs in the right hand side pane.
4. Right-click the certificate and select **All Tasks>Export** from the shortcut menu.
5. Select the **Base 64 format** option and proceed.
6. Enter the path and name of the file. Save the file.

Import the CA in Trusted Root Certification Authorities store of the Computer Account on the SPR Server

The administrator should follow these steps to import a locally generated CA.

1. Open the Certificate mmc snap-in for the local computer.
2. Expand the tree in the right hand side pane and expand **Trusted Root Certification Authorities**.
3. Right-click **Certificates** and select **Import...** from the shortcut menu.
4. Enter the path of the .CER file and proceed to import it.

NOTE

The administrator can also drag and drop the CA from the Current User store to the Local Computer store.

Import the certificate in the Personal Store of the Computer Account

The administrator should follow these steps to import a locally generated certificate or a certificate obtained from a certifying authority.

1. Open the Certificate mmc snap-in for the local computer.
2. Expand the tree in the right hand pane and expand **Personal**.
3. Right-click **Certificates** and select **Import...** from the shortcut menu.
4. Enter the path of the .PFX file.
5. Enter the password and proceed to import the certificate.

NOTE

The administrator can also drag and drop the certificate from the Current User store to the Local Computer store.

Select a Server Certificate for SPR Server from Management Console

To use the newly created certificate for the SPR role:

1. From the Management Console, select **Manage>Servers**.
2. Select the server with the SPR role and click **Update Server**.
3. Select the imported certificate from the **Server Certificate** list.
4. Click **Update**.

Secure Global Desktop will now start to use this certificate. Test the launches via the SPR prior to deploying.

Monitoring

The administrator can monitor the current load on each Relay Server. The administrator can view the information by:

- Relay Servers
- Clients

NOTE

The relay speed and the connection speed in BPS are calculated by taking into consideration the number of bytes for last 60 seconds.

For more information, refer to "Relay Server"

Consider the following symbolic configuration:

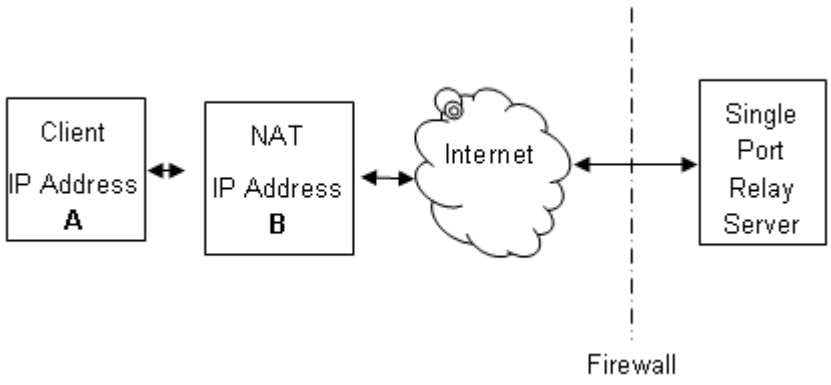


FIGURE 8. Client IP Addresses and Relay Server

In this case, the Client IP Address column displays **A** and the Relay Peer IP Address field displays **B**.

Diagnostics

The administrator can run the following diagnostics tests on the Single Port Relay Server:

- Check if port is available and if the Single Port Relay Server was able to grab it.
- Check if the Single Port Relay Server was able to load the certificate correctly.

Relay switch for Launch Pad

A user can override all settings and force the URL to get all sessions via the Single Port Relay. For example, consider a roaming user, maybe a sales guy, trying to connect to the corporate applications. The user is sure that the location the user is connecting from has a locked-down firewall (required ports are closed). The user uses the URL switch to get all sessions via the Single Port Relay, irrespective of what other policies may say. To do this, a user adds relay=1 in the query string and the query string must begin with a question mark (?).

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

Single Port Relay in DMZ

Secure Global Desktop Terminal Services Edition (TSE) v4 and later provide an additional role, the DMZ SPR role, which allows the administrator to place the Single Port Relay in the DMZ and introduce an additional layer of security between the internal network and the external network by functioning as a secure gateway for the clients. The system administrator needs to expose only one routable address, that of the SPR in the DMZ.

DMZ

The DMZ, short for ‘DeMilitarized Zone’, is a computer or a small sub-network that is placed between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

A DMZ is the physical zone behind an Internet facing firewall and in front of a second level firewall that protects the internal systems and data. In a typical Internet application scenario, the DMZ is the physical virtual local area network (VLAN) on which the Web servers are deployed. It is also known as a 'Perimeter network'. Packet filtering often separates more trusted networks from the DMZ networks at the perimeter. Packet filtering may also separate the Internet from the DMZ. The military metaphor comes from the idea that you let un-trusted users onto the DMZ networks, but they can't "bring guns." For example, packet filtering might allow HTTP fro m the Internet to reach the DMZ but prohibit telnet, ftp, SMTP and other protocols that might easily allow an attack on your trusted networks to be launched.

SPR in DMZ

The Single Port Relay Server in the DMZ (henceforth referred to as DMZ SPR) in TSE v4 is the only exposed server with a routable address. All the other SPR Servers, Web Servers, Application Servers, and Load Balancers lie in the internal secure network (henceforth referred to as the Secure Network).

The RelayServerEngine service runs on the DMZ SPR. This service is like the Secure Global Desktop Engine service that runs on the TSE servers in the Secure Network. The RelayServerEngine, however, does not make DCOM calls into the Secure Network, as the ports to run DCOM are usually not open in the inner firewall. Instead, the RelayServerEngine relies on the DMZRelayServerAssistant component that runs on the Web Server. The RelayServerEngine communicates with the RelayServerAssistant using HTTP.

SPR in the DMZ functions like SPR in the internal network, with the following exceptions that are applicable to the DMZ SPR:

- Diagnostics are not performed on the DMZ SPR.
- The DMZ Relay Server role has to be installed manually on the server and cannot
- be pushed from the Console.
- The DMZ Relay Server role has to be uninstalled manually and can only be
- removed from the TSE database from the Console.
- The monitored status of the DMZ SPR is read from the TSE database, and is updated by the DMZ SPR every two minutes.
- The DMZ SPR has to contact to either another SPR or the Application Servers.
- Web traffic can be routed through the DMZ SPR or through a separate Web Server.

Benefits

The use of a Single Port Relay (SPR) Server provides the following benefits:

Only One Open Port. The administrator can configure the system to work on a particular port, which is already open on the firewall. For example, 443 — the well-known SSL port — is open most of the times.

Only One Routable IP Address. As the Single Port Relay Server relays the traffic between clients and all the Application Servers, the Application Servers can reside on the internal network. The Application Servers need not have a routable IP address. Only the Single Port Relay Server needs to have a routable IP address. This address can be a NAT address, which can also be mapped to a FQDN address. There is no need to expose the Web Server. The DMZ SPR is also capable of routing the HTTP traffic. Users outside the Secure Network can access the TSE Launchpad via the DMZ SPR using <DMZ IP>/Launchpad, and administrators on the move can also monitor the system from the Web-based TSE Management Console using <dm zip>/console.

Enhanced Security. The shielding of Application Servers from the external world, and the fact that a reduced number of ports are open on the firewalls, makes the system more secure. The number of ports open on the inside firewall can also be reduced by putting SPRs in a ‘cascade’. The DMZ SPR also puts additional check on the authenticity of application launches by checking for tickets (see also“Ticketing Authority”). The ticket is issued to the client by the Load Balancer when it servers the launch request. This ticket is checked by the DMZ SPR when the client actually launches the application. The DMZ SPR acts as a HTTP pass-thru. Before passing the HTTP data to the Secure Network, the SPR will authenticate it. This protects the web server in the Secure Network from malicious attacks.

SSL Encryption. In Secure Global Desktop TSE v2.1 the SPR performed only a SSL handshake with the client, the RDP and IFS data flow was not SSL encrypted. In TSE v4 security is much enhanced by encrypting the whole data stream.

- Any communication from the SPR to the Secure Network will need to go through a firewall friendly port (http 80 or 443). This typically excludes the RDP & IFS ports, as for performance reasons it will be desirable to open these ports in the innermost firewall. However, in the case where administrators desire completely secured communication even through the innermost firewall, one more optional cascaded SPR can be placed in the Secure Network.

Traffic Through DMZ Single Port Relay

The DMZ Single Port Relay (DMZ SPR) handles the following types of data:

- HTTP Traffic
- Internet File Sharing
- Printing
- RDP Sessions

Installing the Single Port Relay (SPR) Server Role on a DMZ Server – Prerequisites

Before the administrator installs the SPR role on server in the DMZ, the administrator should have:

- At least a single- machine (‘unibox’) installation of Secure Global Desktop TSE that consists of a Secure Global Desktop TSE installation with Web Server, Application Server and Load Balancer roles on a single server in the Secure Network.
- If SPRs are being cascaded, that is, if the SPR in the DMZ connects to the internal network via an SPR in the Secure Network, the SPR role should be installed on a server in the internal network before installing the SPR role on a DMZ server.

SPR in DMZ Installables

To install the SPR role on a server in the DMZ, the administrator can do one of the following:

- Run SGD-TSE-DMZ.msi from the CD drive of the server in the DMZ or from a network share that can be accessed from the server in the DMZ.
- Click the appropriate link on the Home>Download page of the Console to download and run the appropriate msi from the Depot folder on the Web Server.

SPR in DMZ Installation Information

Additionally, the administrator needs to have knowledge of the following information as the installation program prompts for it:

- The IP address of the Web Server OR
- The IP address of the cascaded SPR Server in the Secure Network if SPRs are being cascaded.
- The port of the web server or of the cascaded SPR.
- Status of this server (secured or not).
- The user name and password of the account under which the DMZ SPR Services run. It is recommended that this be the low privileged user account. This user need not have any access to the Secure Global Desktop Servers in the Secure Network.

Single Port Relay Server With DMZ Relay Server Role in the DMZ

The following diagram is a symbolic representation of the protocols and ports used by the Secure Global Desktop TSE components when it has the DMZ Relay Server role installed on it.

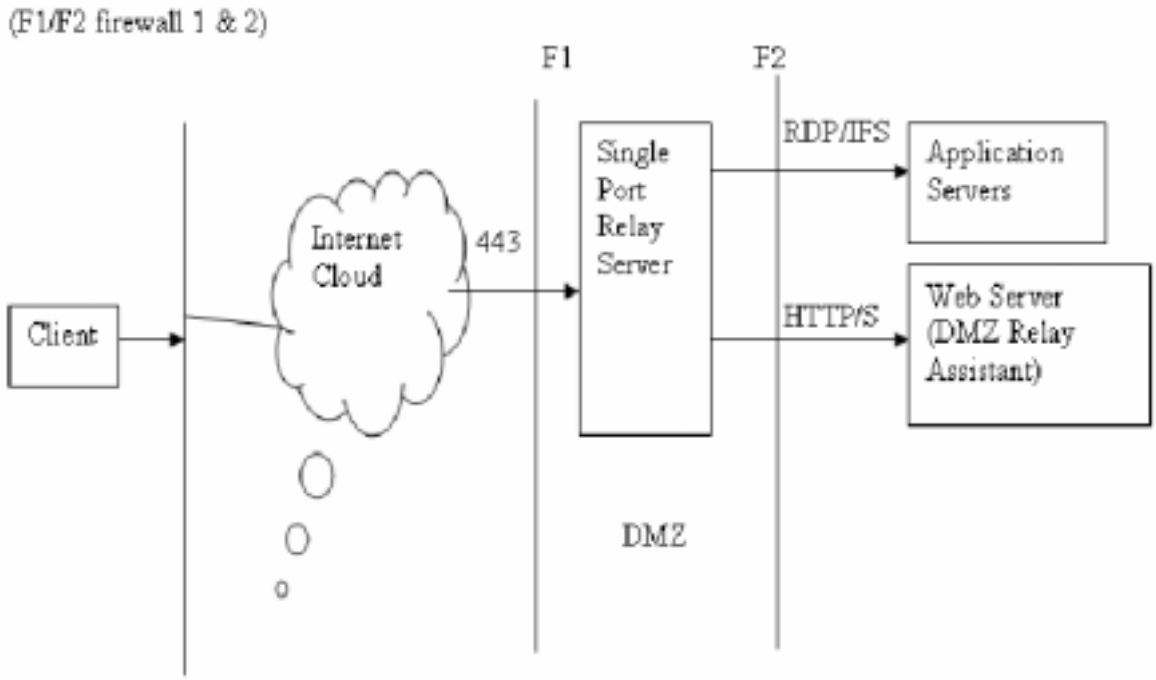


FIGURE 9. Single Port Relay Server in the DMZ

This setup allows the administrator to only open the secure port 443 for communication with external clients and port 80 for web traffic. The Web Server is also placed in the Secure Network and all RDP, IFS and web traffic is routed through the DMZ SPR. The advantage here is that the secure ports need to be opened on only one server on the external firewall. Hence, only the DMZ Server has to have a routable address.

Single Port Relay Server with Cascaded Relays

The configuration shown in Figure 9 has the disadvantage that port 3389 and port 4660 have to remain open on the internal firewall for RDP and IFS traffic. The administrator can avoid this by configuring another SPR in the Secure Network. The DMZ SPR is cascaded with the SPR in the internal network. In this case, only the secure ports need to be open on the internal firewall. Additionally, the administrator can configure whether to route either or both web traffic and RDP/IFS traffic through the cascaded SPR from the **Options>Relay Servers** page.

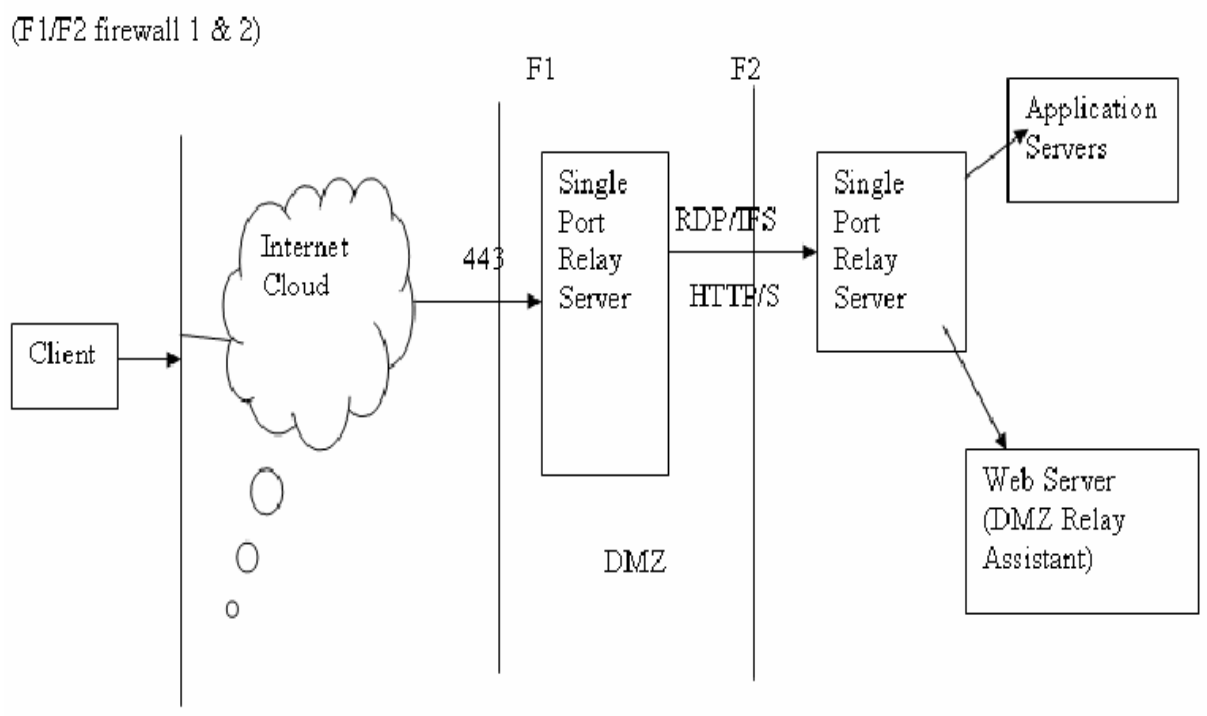


FIGURE 10. Cascaded SPR with Single Port Relay in the DMZ and in the Secure Network

Implementation Details

The Single Port Relay Server is a Service that runs on Windows 2000 Server or Windows Server 2003, which has a routable IP address. This service listens on the specified port and forwards all the RDP or IFS traffic to the appropriate port on the Application Server. The Single Port Relay service listens on a configurable port (443 by default).

The DMZ SPR uses the DMZRelayAssistant on the Web Server in the Secure Network to update its status in the TSE database.

Users coming from outside can access the Launchpad using <dmzip>\launchpad. The DMZ SPR acts as a HTTP pass-thru shielding the internal web servers from the un-secured network.

All RDP and IFS data are also sent to the Single Port Relay Server instead of the Application Server. The Single Port Relay forwards the data to the appropriate Application Server.

In this scenario the administrator needs to open HTTP/S (80/443), RDP (2287) and IFS (4660) in the inside firewall (F2).

If the Single Port Relay is configured to use SSL handshake, then every connection first tries to establish a valid SSL session by completing a proper SSL handshake. It is possible to configure several Single Port Relay Servers to use different types of "Server Authentication Certificates". However, all the Single Port Relay Servers use the same port number. The Tarantella certificate is installed in the "Personal" folder of the computer account and the Tarantella Certification Authority (CA) is installed in the "Trusted Root Certification Authorities" folder of the computer account when the relay server role is installed on the server. The Tarantella Certificate is valid for one year and the Tarantella CA is valid for 20 years.

During uninstall, both the Tarantella certificate and the Tarantella CA are uninstalled from the "Personal" and the "Trusted Root Certification Authorities" stores of the computer.

Monitor DMZ Relay Servers

You can access this page in the TSE Management Console to view the load on the DMZ Relay Server (DMZ SPR) in the Secure Global Desktop TSE team. This is an optional role, so you may see no information (if you have no DMZ Relay Server installed).

NOTE

*You can change your DMZ SPR settings from the **Options>Relay Server** page.*

You can view the current load in the following ways:

- "View By Server"
- "View By Client"

View By Server

This is the default view. It displays the following information:

Relay Server. Displays the name of the DMZ Relay Server.

Number of Connections. Reflects the number of total connections made through this port.

Number of Web Server Connections. Reflects the number of HTTP connections made through this port.

Number of Application Server Connections. Reflects the number of RDP/IFS connections made through this port.

Relay Speed (BPS). Reflects total throughput from all clients to the Applic ation Servers through the DMZ SPR. The throughput speed has an inverse relation to the Number of Connections value. The value appears as bytes per second (BPS).

Available Memory (MB). Shows the difference between the total memory and the memory in use by active processes.

Available CPU Cycles (MHz). Shows the difference between the total CPU capacity and the capacity in use by active processes.

View By Client

This is an alternate view. It displays the following information:

Client Name. Shows the NetBIOS name of the client computer.

Client IP Address. Shows the IP address of the client computer.

Source Address. Shows the NAT IP address. If there is no NAT, this displays the client IP address.

Relay Server. Shows the name of the DMZ Relay Server.

Connection Speed. Reflects throughput from each client to the Application Server. The throughput speed has an inverse relation to the Number of Connections value. The value appears as bytes per second (BPS).

Update Server Profile

To update the properties of any servers, go to Manage Server in the Management Console and select the DMZ SPR server (which must already have been added previously by installing the role on that server). Use the Update Server action to update the properties of a DMZ SPR server.

Server Information

Server name*. The server name is used to identify the server. In case of the DMZ SPR this name is not used in any way to communicate with the DMZ SPR like with some other Secure Global Desktop TSE roles.

Description. This provides free-form text that identifies the server or clarifies other information.

Published Address. When you specify a server IP address or fully qualified domain name (FQDN) in this field, a client will use this address to connect to this server. If you do not specify an address in this field, Secure Global Desktop TSE routes the client connections to the Internal IP Address.

In the case of the DMZ SPR, make sure to specify an address that is available to a client because a server may have several IP addresses and some of these addresses may be unavailable for client connections. If not specified otherwise, the internal IP address is used as External, but it will fail in case of the DMZ SPR.

NOTE

In the case of the DMZ SPR, make sure to specify an address that is available to a client because a server may have several IP addresses and some of these addresses may be unavailable for client connections. If not specified otherwise, the internal IP address is used as External, but it will fail in case of DMZ SPR.

Disable Best Internal Address Discovery. By default, Secure Global Desktop TSE will discover the best address to use for its internal communication. If you wish to specify a particular address, clear this check box to disable the discovery mechanism and enter an Internal IP Address or DNS name in the Internal Address to use field.

NOTE

Check this setting, if HTTP access to the DMZ SPR fails, or if application launches fail even though everything looks ok on the firewall. The DMZ SPR might be using the wrong internal IP interface to connect to the Secure Network. Specify the correct internal IP, and thne clear this check box.

Internal Address to Use. Members (servers) of the Secure Global Desktop TSE Team use this address to communicate with each other. Enter the internal IP address, NetBIOS name, or FQDN name in this field. If you do not specify an Internal Address, TSE will use the address that best communicates with your Web Server IP / Cascaded SPR IP that you specified while installing the DMZ SPR role.

Relay Configuration and DMZ
Relay Configuration

This can be changed from the **Options->Relay Servers**.

NOTE

For security reasons, servers in the Secure Network don't talk back to the DMZ SPR. However, the DMZ SPR reads the configuration changes every 2 minutes, which means it takes atleast 2 minutes or more for DMZ SPR configuration vlaues to take effect.

DMZ Relay Configuration

Relay Port. This setting allows you to assign the relay port for a SPR server. In general, you might want to use port 443 (SSL) if you have no specific objection to using it as it is generally open for communication in most server-client environments. However, if you cannot use or don't want to use port 443, this port assignment is configurable.

NOTE

If you change the relay port, the existing connections are disconnected. However, the user can reconnect the disconnected sessions from the LaunchPad Connections page, depending on the connection settings.

Enable SSL. The SSL protocol generally begins with a handshake phase that negotiates an encryption algorithm, checks the keys (public and private), and authenticates the server to the client. This also enables the encryption of data that flows to the SPR from its client.

Cascaded Relay Configuration

Enable Cascaded Relay. Select this to enable cascaded relay configuration. You must select this, and either or both of the following check boxes to enable routing:

Enable HTTP Routing. Select this setting if you have enabled cascaded relay and want to route all the web traffic through the cascaded SPR. If this box is not checked, the inside SPR won't be used to route HTTP traffic. The administrator needs to open the Web Server's IP/Port on the inside firewall.

The Web Server IP/Port is given to the DMZ SPR (as DMZRelayAssistant). This configuration can be changed using the resource kit (CRK) that is available for Secure Global Desktop TSE.

Enable RDP/IFS Routing. Select this setting if you have enabled cascaded relay and want to route the RDP and IFS traffic through the cascaded SPR. If this box is not checked, the inside SPR won't be used to route RDP/IFS traffic. The administrator needs to open all Application Server IP and RDP/IFS ports on the inside firewall.

DMZ SPR Resource Kit

To install the Secure Global Desktop TSE Resource Kit on a DMZ SPR server in the DMZ, the administratorcan do the following:

- Run SGD-TSE-RK.msi from the CD drive of the server in the DMZ or from a network share that can be accessed from the server in the DMZ.

Changing Identity of DMZ Server Components

Changes the identity under which DMZ components and services are running. Identity is the security context that these components use while running. This command will generate appropriate progress messages as well as error messages.

Logging: Event log entries will get generated indicating failure or success of the operation.

- Type in following command on the Tarantella CRK prompt

  c:\ Sgd-rk dmzidentity /action:set /domain:xxx /user:xxx /password:xxx

- If the operation is successful you will get a proper message or else an error will be shown.

Displaying DMZ Server Certificate

Displays the current server certificate that is being used by the DMZ server. This command can be used just for verification by the admin before changing the certificate.

- Type in following command on the Tarantella CRK prompt.

  c:\Sgd-rk dmzcertificate

- Existing certificate name will get displayed on the prompt.

Changing DMZ Server Certificate

Changes the certificate used by the DMZ server. If the certificate name contains a space, delimit it with quotation marks; otherwise it will generate appropriate error messages.

Logging: Event log entries will get generated indicating failure or success of the operation.

- Type in following command on the Tarantella CRK prompt

  dmzcertificate /action:set /certificatename:xxxxx

- This command will change the certificate that is being used by the DMZ server.

Known Issues

On the DMZ SPR the application log gets full with the event logs from PerfLib saying “Access to performance data was denied to ‘DMZUser’ “. Admin might get the “Event log full” messages and need to set the event log to Overwrite Events as needed.

Ticketing Authority

Overview

The new Ticketing Authority (TA) feature in Secure Global Desktop TSE v4 serves the purpose of providing an additional security check in deployments that involve a DMZ. It will be responsible for issuing session tickets to an already authorized Secure Global Desktop TSE user. This ticket will be validated at the DMZ when the user tries to launch an application. Any user presenting an invalid ticket will be rejected in the DMZ. The TA feature is enabled by default whenever the DMZ SPR is in use. Ticketing can not be turned off when the DMZ SPR is enabled.

What and How is the Ticketing Authority Protecting Aganist

Without a Ticketing Authority (TA), it is conceivable for a client to launch a ‘man in the middle’ attack, bypassing TSE and directly launching an (un-provisioned) application on an application server. It would be conceivable for an attacker to retrieve the IP address of the application server

and to launch directly from the application server bypassing TSE. With the new TA feature in TSE v4 such unauthorized accesses can be prevented. When an application launch request comes in, TSE will issue a session ticket only after a successful authenticity check and other checks such as application validation. Thus the administrator can be assured that the user who is requesting access to an application server, is really an authorized user.

Implementation Details

By default, the Ticketing Authority (TA) installs as a COM+ component on all web servers in the Secure Network. The sequence of events is as follows (see figure 11):

- When a client wants to launch an application, it comes to the TSE Load-Balancer Assistant (LBA) first.
- After handling the user authentication, application validation and after receiving a suitable application server from the Load-Balancer (LB), the LBA contacts the TA.
- The TA then generates a session ticket for the served request. The session ticket reaches the client as part of the LB response. The LB response will not contain the IP address of the application server and thus there will be no way for a user to get access to the application server directly.
- The client then presents this ticket to the DMZ SPR at launch time as part of the SPR handshake.
- The DMZ SPR retrieves this ticket and presents it to the TA.
- The TA checks the validity of the ticket (time stamp check). If an invalid ticket is presented an event will be logged.
- If the ticket is valid, the TA returns the IP address and port of the application server to the DMZ SPR and then removes the ticket from the database. A valid ticket will let the connection in, otherwise an error message will be created during the SSL handshake and the connection will be dropped.

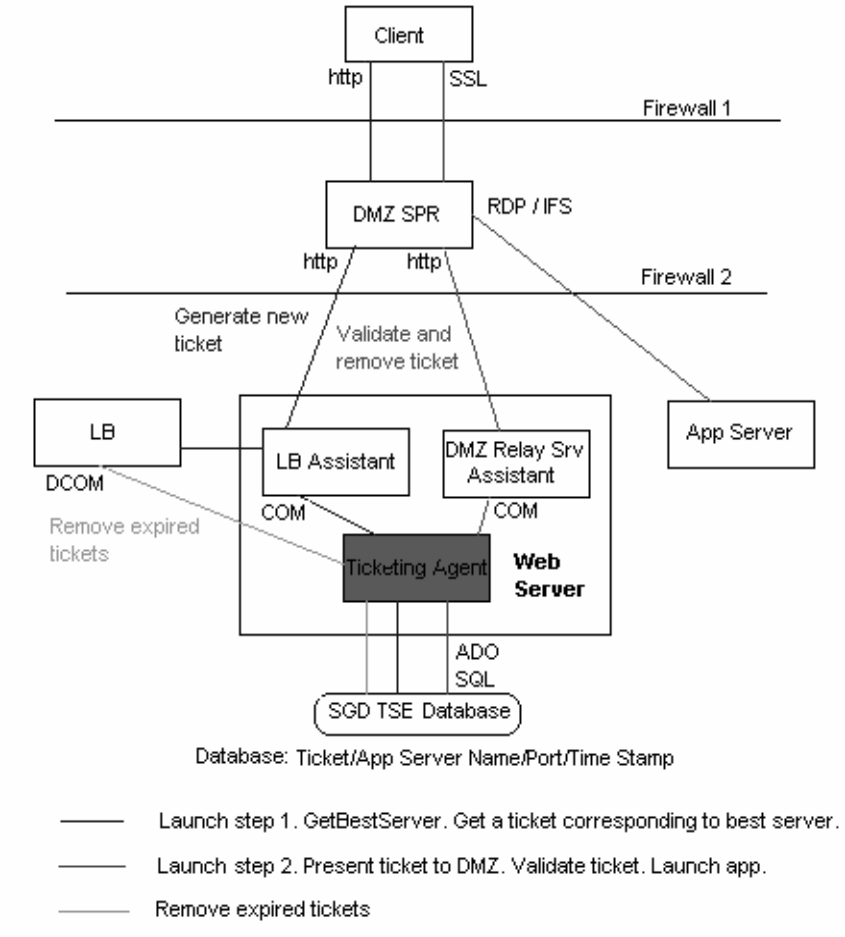


FIGURE 11. Ticketing Authority

Server Lockdown

By default, when the administrator adds an Application Server to the Secure Global Desktop system, the server has no restrictions applied to it. The server lockdown feature restricts access to the Application Servers, so that the users can only execute those applications that are provisioned to them and thus cannot tamper with the Application Server. The feature makes the system less prone to malicious use, consequently rendering it more stable. This feature is particularly useful if the administrator intends to provision the Windows desktop from the Application Server. The administrator can restrict or configure the Windows explorer and some of the standard dialog boxes, such as the **File>Save** or **File>Open** dialog boxes.

Lockdown Policy

A single lockdown setting enables or disables a particular UI element. For example, a setting can remove the **Run** submenu from the Windows Explorer's **Start** Menu. A set of settings is termed as a Lockdown Policy. Secure Global Desktop TSE v4 offers 4 predefined system policies:

1. No restrictions.
2. Low restrictions.
3. Medium restrictions.
4. Highest restrictions.

A Secure Global Desktop administrator can also create a customized Lockdown Policy suitable for a specific need from the **Options>Lockdown Policies** page of the TSE Management Console by selecting desired settings from a predefined set. This set is actually a small subset of Microsoft's Group Policy Settings.

Initially, when a server is added to the Secure Global Desktop system, it does not have any Lockdown Policy applied to it, that is a newly added server has a "No Restriction" Lockdown Policy applied to it. Administrators can assign a Lockdown Policy to an Application Server from the **Manage>Servers>Update Server** page of the Console.

The following table describes which settings are applied in the four predefined system lockdown policies:

Lockdown Policy Setting	No Restriction	Low Restriction	Medium Restriction	Highest Restriction
Disable Windows Explorer's default context menu	False	True	True	True
Disable registry editing tools	False	True	True	True
Disable command prompt	False	True	True	True
Remove File Menu from Windows Explorer	False	True	True	True
Remove Run Menu from Start Menu	False	False	True	True
Remove Search button from Windows Explorer	False	False	True	True
Remove Search Menu from Start Menu	False	False	True	True
Disable Context Menu for Taskbar	False	False	True	True
Disable changes to Taskbar and Start Menu settings	False	False	True	True
Disable Control Panel	False	False	False	True
Hide A, B, C & D drive in My Computer	False	False	True	True
Prevent access to A,B, C & d drive in My Computer	False	False	False	True
Hide the common dialog places bar	False	False	False	True
Disable and remove links to Windows update	False	False	False	True
Disable Task Manager	False	False	False	True
Disable Change Password	False	False	False	True
Disable Active Desktop	False	False	False	True
Disable changing wallpaper	False	False	False	True
Remove the Folder options menu item from Tools Menu	False	False	False	True
Prevent user from changing My Document path	False	False	False	True

Lockdown Policy Setting	No Restriction	Low Restriction	Medium Restriction	Highest Restriction
Remove common program groups from Start Menu	False	False	False	True
Remove Documents menu from Start Menu	False	False	False	True
Remove User's folder from Start Menu	False	False	False	True
Allow Only Secure Global Desktop Sessions on this server (Disable Direct RDP Sessions)	False	False	False	True

Microsoft Group Policy has a very large number of settings. The set in Secure Global Desktop TSE is actually a small subset of Microsoft's Group Policy Settings. The following section lists all the settings used in Secure Global Desktop TSE v4.

1. Remove Windows Explorer's default context menu: - Removes shortcut menus from the desktop and Windows Explorer. Shortcut menus appear when you right-click an item. If you enable this setting, menus do not appear when you right-click the desktop or when you right-click the items in Windows Explorer. This setting does not prevent users from using other methods to issue commands available on the shortcut menus.
2. Prevent access to registry editing tools:- Disables the Windows registry editor Regedit.exe. If this setting is enabled and the user tries to start a registry editor, a message appears explaining that a setting prevents the action. To prevent users from using other administrative tools, use the Run only allowed Windows applications setting.
3. Prevent access to the command prompt:- Prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this setting and the user tries to open a command window, the system displays a messageexplaining that a setting prevents the action.

NOTE

Secure Global Desktop does not prevent the computer from running batch files for users that use Terminal Services.

4. Remove File menu from Windows Explorer:- Removes the File menu from My Computer and Windows Explorer. This setting does not prevent users from using other methods to perform tasks available on the File menu.
5. Remove Run menu from Start Menu:- Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager. If you enable this setting, the following changes occur:

   1. The Run command is removed from the Start menu.
   2. The New Task (Run) command is removed from Task Manager.
   3. The user will be blocked from entering the following into the Internet Explorer Address Bar:

   A UNC path: \\<server>\<share> ---Accessing local drives: e.g., C: --- Accessing local folders: e.g., \temp> Also, users with extended keyboards will no longer be able to display the Run dialog box by pressing the Application key (the key with the Windows logo) + R. If

you disable or do not configure this setting, users will be able to access the Run command in the Start menu and in Task Manager and use the Internet Explorer Address Bar.

NOTE

This setting affects the specified interface only. It does not prevent users from using other methods to run programs. It is a requirement for third-party applications with Windows 2000 or later certification to adhere to this setting. However, it is possible that some older applications may not follow this requirement.

6. Remove Search button from Windows Explorer:- Removes the Search button from the Windows Explorer toolbar. This setting removes the Search button from the Standard Buttons toolbar that appears in Windows Explorer and other programs that use the Windows Explorer window, such as My Computer and My Network Places. It does not remove the Search button or affect any search features of Internet browser windows, such as the Internet Explorer window. This setting does not affect the Search items on the Windows Explorer context menu or on the Start menu. To remove Search from the Start menu, use the Remove Search menu from Start menu setting (in User Configuration\Administrative Templates\Start Menu and Taskbar). To hide all context menus, use the Remove Windows Explorer's default context menu setting.
7. Remove Search menu from Start Menu:- Removes the Search item from the Start menu, and disables some Windows Explorer search elements. This setting removes the Search item from the Start menu and from the context menu that appears when you right-click the Start menu. Also, the system does not respond when a user presses the Application key (the key with the Windows logo)+ F. In Windows Explorer, the Search item still appears on the Standard buttons toolbar, but the system does not respond when the user presses Ctrl+F. Also, Search does not appear in the context menu when you right-click an icon representing a drive or a folder. This setting affects the specified user interface elements only. It does not affect Internet Explorer and does not prevent the user from using other methods to search. Also, see the Remove Search button from Windows Explorer setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer.

NOTE

This setting also prevents the user from using the F3 key.

8. Remove access to the context menus for the taskbar:- Hides the menus that appear when you right-click the taskbar and items on the taskbar,such as the Start button, the clock, and the taskbar buttons. This setting does not prevent users from using other methods to issue the commands that appear on these menus.
9. Prevent changes to Taskbar and Start Menu Settings:- Removes the Taskbar and Start Menu item from Settings on the Start menu. This setting also prevents the user from opening the Taskbar Properties dialog box. If the user rightclicks the taskbar and then clicks Properties, a message appears explaining that a setting prevents the action.
10. Prohibit access to the Control Panel:- Disables all Control Panel programs. This setting prevents Control.exe, the program file for Control Panel, from starting. As a result, users cannot start Control Panel or run any Control Panel items. This setting also removes Control Panel from the Start menu. (To open Control Panel, click Start, point to Settings, and then click Control Panel.) This setting also removes the Control Panel folder from Windows Explorer. If a user tries to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action. Also, see the Remove Display in Control Panel and Remove programs on Settings menu settings.

11. Hide these specified drives in My Computer:- Removes the icons representing selected hard drives from My Computer and Windows Explorer. Also, the drive letters representing the selected drives do not appear in the standard Open dialog box. To use this setting, select a drive or combination of drives in the drop-down list. To display all drives, disable this setting or select the Do not restrict drives option in the drop-down list.

NOTE

This setting removes the drive icons. Users can still gain access to drive contents by using other methods, such as by typing the path to a directory on the drive in the Map Network Drive dialog box, in the Run dialog box, or in a command window. Also, this setting does not prevent users from using programs to access these drives or their contents. And it does not prevent users from using the Disk Managment snap-in to view and change drive characteristics. It is a requirement for third party applications with Windows 2000 or later certification to adhere to this setting.

---

12. Prevent access to drives from My Computer:- Prevents users from using My Computer to gain access to the content of selected drives. If you enable this setting, users can browse the directory structure of the selected drives in My Computer or Windows Explorer, but they cannot open folders and access the contents. Also, they cannot use the Run dialog box or the Map Network Drive dialog box to view the directories on these drives. To use this setting, select a drive or combination of drives from the drop-down list. To allow access to all drive directories, disable this setting or select the Do not restrict drives option from the drop-down list.

NOTE

The icons representing the specified drives still appear in My Computer but if users double click the icons, a message appears explaining that a setting prevents the action. Also, this setting does not prevent the users from using programs to access local and network drives. And it does not prevent them from using Disk Managment snap-in to view and change drive characteristics.

---

13. Hide the common dialog places bar:- Removes the shortcut bar from the Open dialog box. This setting, and others in this folder, lets you remove new features added in Windows 2000 Professional, so that theOpen dialog box looks like it did in Windows NT 4.0 and earlier. These policies only affect programs that use the standard Open dialog box provided to developers of Windows programs. To see an example of the standard Open dialog box, start Notepad and, on the File menu, click Open.

NOTE

It is a requirement for third-party applications with Windows 2000 or later certification adhere to this setting. However, it is possible that some older applications may not follow this requirement.

---

14. Remove links and access to Windows Update:- Prevents users from connecting to the Windows Update Web site. This setting blocks user access to the Windows Update Web site at http://windowsupdate.microsoft.com. Also, the setting removes the Windows Update hyperlink from the Start menu and from the Tools menu in Internet Explorer. Windows Update, the online extension of Windows, offers software updates to keep a user's system

up-to-date. The Windows Update Product Catalogue determines any system files, security fixes, and Microsoft updates that users need and shows the newest versions available for download. Also see the Hide the Add programs from Microsoft option setting.

15. Remove Task Manager:- Prevents users from starting Task Manager (Taskmgr.exe). If this setting is enabled and users try to start Task Manager, a message appears explaining that a policy prevents the action. Task Manager lets users start and stop programs; monitor the performance of their computers; view and monitor all programs running on their computers, including system services; find the executable names of programs; and change the priority of the process in which programs run.
16. Remove Change Password:- Prevents users from changing their Windows password on demand. This setting disables the Change Password button on the Windows Security dialog box (which appears when you press Ctrl+Alt+Del). However, users are still able to change their password when prompted by the system. The system prompts users for a new password when an administrator requires a new password or their password is expiring.
17. Prevent changing wallpaper:- Prevents users from adding or changing the background design of the desktop. By default, users can use the Desktop tab of Display in Control Panel to add a background design (wallpaper) to their desktop. If you enable this setting, the Desktop tab still appears, but all options on the tab are disabled. To remove the Desktop tab, use the Hide Desktop tab setting. To specify wallpaper for a group, use the Active Desktop Wallpaper setting. Also, see the Allow only bitmapped wallpaper setting.
18. Removes the Folder Options menu item from the Tools menu:- Removes the Folder Options item from all Windows Explorer menus and removes the Folder Options item from Control Panel. As a result, users cannot use the Folder Options dialog box. The Folder Options dialog box lets users set many properties of Windows Explorer, such as Active Desktop, Web view, Offline Files, hidden system files, and file types. Also, see the Enable Active Desktop setting in User Configuration\AdministrativeTemplates\Desktop\Active Desktop and the Prohibit user configuration of Offline Files setting in User Configuration\Administrative Templates\Network\Offline Files.
19. Prohibit user from changing My Documents path:- Prevents users from changing the path to the My Documents folder. By default, a user can change the location of the My Documents folder by typing a new path in the Target box of the My Documents Properties dialog box. If you enable this setting, users are unable to type a new location in the Target box.
20. Remove common program groups from Start Menu:- Removes items in the All Users profile from the Programs menu on the Start menu. By default, the Programs menu contains items from the All Users profile and items from the user's profile. If you enable this setting, only items in the user's profile appear in the Programs menu.To see the Program menu items in the All Users profile, on the system drive, go to Documents and Settings\All Users\Start Menu\Programs.
21. Remove Documents menu from Start Menu:- Removes the Documents menu from the Start menu. The Documents menu contains links to the non-program files that users have most recently opened. It appears so that users can easily reopen their documents. If you enable this setting, the system saves document shortcuts but does not display them in the Documents menu. If you later disable it or set it to Not Configured, the document shortcuts saved before the setting was enabled and while it was in effect appear in the Documents menu.

NOTE

This setting does not prevent Windows programs from displaying shortcuts to recently opened documents. See the Do not keep history of recently opened documents on exit

policies in this folder. This setting also does not hide document shortcuts displayed in the Open dialog box. See the Hide the Dropdown list of recent files setting.

22. Remove user's folders from the Start Menu:- Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden. This setting is designed for use with redirected folders. Redirected folders appear on the main (bottom) section of the Start menu. However, the original, user-specific version of the folder still appears on the top section of the Start menu. Because the appearance of two folders with the same name might confuse users, you can use this setting to hide user-specific folders. Note that this setting hides all user-specific folders, not just those associated with redirected folders. If you enable this setting, no folders appear on the top section of the Start menu. If users add folders to the Start Menu directory in their user profiles, the folders appear in the directory but not on the Start menu. If you disable this setting or do not configure it, Windows 2000 Professional and Windows XP Professional display folders on both sections of the Start menu.
23. Remove Favourites menu from Start Menu:- Prevents users from adding the Favourites menu to the Start menu or classic Start menu.If you enable this setting, the Display Favourites item does not appear in the Advanced Start menu options box. If you disable or do not configure this setting, the Display Favourite item is available.

NOTE

The Favourites menu does not appear on the Start menu by default. To display the Favourites menu, right click Start, click Properties and then click Customize. If you are using the Start menu, click Advacned tab and then under Start menu items, click the Favourites menu. If you are using the classic Start menu, click Display Favourites under Advacned Start menu options.

NOTE

The items that appear in theFavourites menu when you install Windows are preconfigured by the system to appeal to most uusers. However, users can add and remove items from this menu, and system administrators can create a customized Favourites menu for a user group. This setting only affects the Start menu. The Favourites item still appears in Windows Explorer and in Internet Explorer.

24. Allow Only Secure Global Desktop sessions on this Server. (Disable Direct RDP Sessions):- This is a Secure Global Desktop TSE-specific setting. This setting does not use any of the Microsoft Group Policy Object functionality and is implemented entirely through the Secure Global Desktop TSE product. If this setting is applied then any ordinary user who is not a member of either the Secure Global Desktop Administrator Group or Local Servers Administrator Group will not be able to establish a direct RDP session with this Server using the Microsoft's Remote Desktop Connection.

Manage Lockdown Policies

Use the **Options>Lockdown** Policies page of the Secure Global Desktop Management Console to view, add, update, or remove lockdown policies. You can apply the policies you add here to the Application Servers from the **Manage>Servers>Update Server** page of the Console.

NOTE

You cannot modify or delete predefined lockdown policies.

This section provides step-by-step procedures to do the following:

View Lockdown Policy

You can view all the policies configured in the Secure Global Desktop system from the **Options>Lockdown Policies** page of the Console. To view the details of a particular policy, click the Policy Name of the relevant policy. The Console displays the lockdown policy details such as the name and description of the policy and the lockdown policy settings.Click **Show All Policies** to return to the Lockdown Policies page.

Add Lockdown Policy

The Add Policy action allows you to add a new lockdown policy to the Secure Global Desktop system.

1. To add a set of lockdown policy restrictions:
2. From the Options>Lockdown Policy page, click Add Policy.
3. On the Add Policy page, select/enter the relevant information and click Next.

The Add Policy page displays the choices you make. Review the information, and click Add.

Following are the fields you need to specify while adding a lockdown policy.

Policy Name

This Lockdown Policy name appears on the Secure Global Desktop Console. You should specify a meaningful name for a Lockdown Policy.

Description

This is a free-form description of the lockdown policy that identifies the policy or provides other clarification.

Policy Settings

Select the relevant restrictions you want to include in the lockdown policy.

After you add a lockdown policy, you can apply it to a server from the **Manage>Servers>Update Server** page of the console.

Update Lockdown Policy

The Update Policy action permits you to change the restrictive properties of the selected lockdown policies.

NOTE

You cannot update the properties of a built-in lockdown policy.

To update a set of lockdown policy restrictions:

1. From the Options>Lockdown Policy page, select a lockdown policy and click Update Policy.
2. Change the relevant fields and click Update.

Remove Lockdown Policy

The Remove Policy action permits you to remove the selected lockdown policies. You cannot remove a lockdown policy template.

NOTE

You cannot remove a built-in lockdown policy.

To update a set of lockdown policy restrictions:

1. From the Options>Lockdown Policy page, select a lockdown policy and click Remove Policy.
2. The Remove Policy page displays the lockdown policies you choose. Click Remove to remove the displayed lockdown policies.

NOTE

When you remove a lockdown policy that is applied to an Application Server, the server reverts to the default setting of no restrictions.

Printer Driver Management Utility

During application launch, the client printer is mapped onto an application server. The corresponding printer driver is installed on the server, if it is not already there. This driver installation might fail or get aborted if it is not completed in one minute. Finding such failures and correcting them was not possible in previous versions of Secure Global Desktop TSE; there is now a tool in TSE v4 whic h allows the administrator to accomplish this task.

The new Printer driver management utility in TSE v4 enables the administrator to find failed driver installations in the Secure Global Desktop TSE team and provides a way to map these failed drivers to an alternate driver. With that, any subsequent attempts to install the failed driver will be replaced by installing the alternate driver.

In addition, the utility provides the following features:

1. Displays list of installed drivers in the Secure Global Desktop TSE server team. Administrator can replicate the installed driver to all remaining application servers in the team that have the same operating system.

2. Uninstall of drivers from all application servers having the same operating system.

3. Custom driver mapping: The administrator can map a client driver to a server driver without having to wait for it to fail (and then do the mapping).

4. Delete and edit user defined driver mappings.

5. Create an allow-only or deny list of drivers. If the administrator creates an allow only list, then only those drivers are allowed to install on the application server. If the administrator creates a deny list, then all the drivers except those in the list are allowed to install onto the application server.

6. Delete a driver from failed driver list.

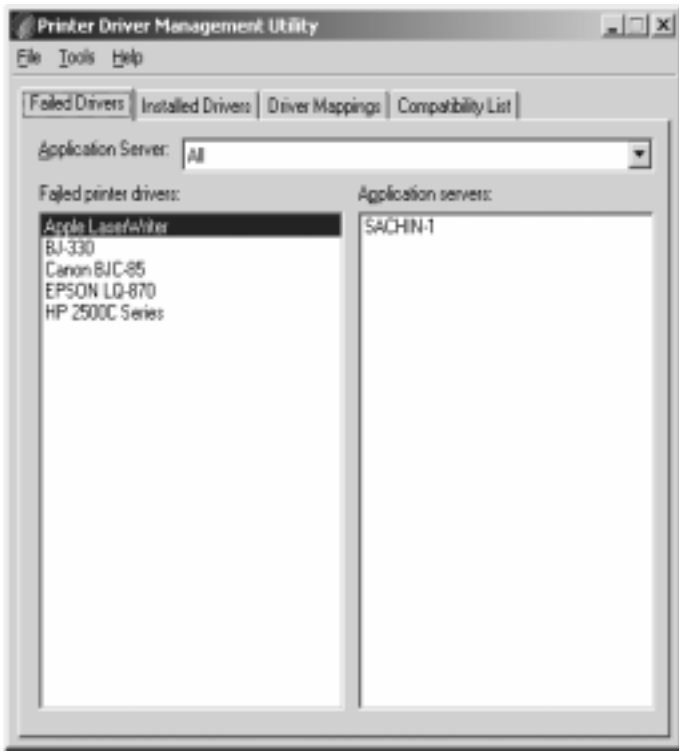
User Interface

Use the **Manage>Servers** page of the Secure Global Desktop Management Console to launch the Printer Driver Management (PDM) utility. The launch is through Secure Global Desktop TSE.

The printer driver utility has four tabs. This section explains their usage in detail.

Failed Driver Tab

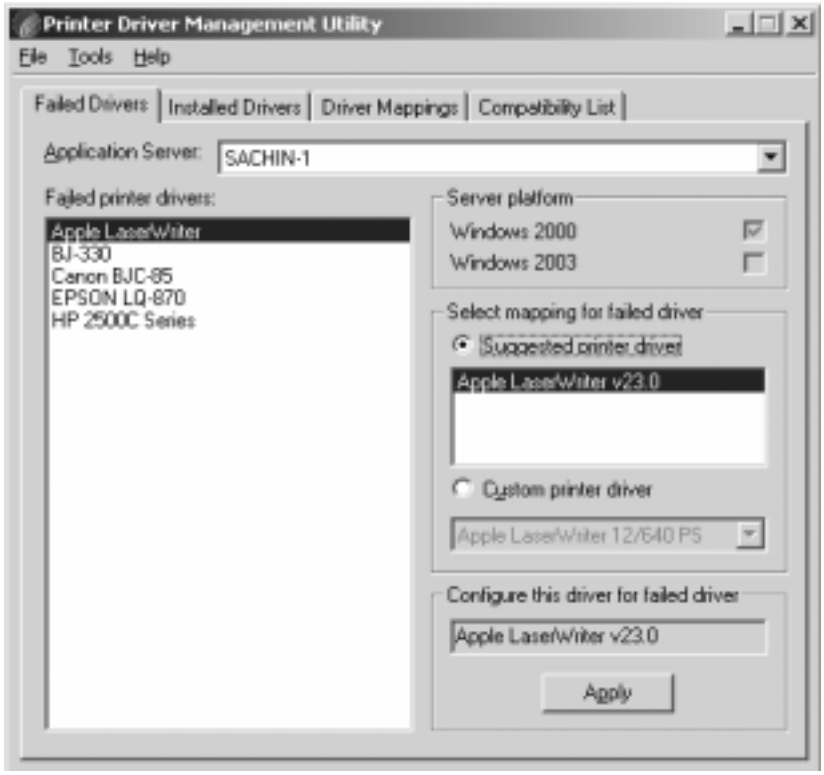
This tab shows a list of failed drivers for the Secure Global Desktop TSE team and allows a user to map an alternate driver for the failed one.



To view the server(s) on which the driver failed, click on a driver in the list. The **Application Servers** list box shows servers on which the installation failed.

To view all failed drivers in the team select **All** from the **Application Servers** combo box.

To view a server-specific list of failed drivers, select the particular server from **Application Servers** combo box.



To map a failed driver, select a particular applic ation server and click on the driver name. The right side of the UI shows driver-specific information, such as the operating system of the application server, a suggested list of alternate drivers, or a custom list of drivers. The suggested list shows recommended drivers which should be used as an alternative for the failed driver. This list is populated from the Secure Global Desktop TSE database. If the administrator wants to use any other driver that is not in the suggested list, she can do so using a custom driver list.

The selected alternate driver is shown in the **Configured** driver edit box. To apply the

mapping click **Apply** button on the tab.

When the user hits the **Apply** button the mapping is done and added to the Secure Global Desktop TSE

database. The new setting is displayed in the **Driver Mappings** tab.

NOTE

NOTE: *The mapping is done for all servers that have the same operating system installed. The administrator can remove the driver from the failed list. Select the server on which the driver has failed, right click on the driver and select the Delete menu item.*

Installed Driver Tabs

This tab shows all installed drivers in the team.

If **All** is selected in the **Application Servers** combo box then the installed drivers list shows all the drivers installed within the server team. To view the applic ation server on which this driver is installed, select a particular driver; the right side list of Application servers shows all servers on which this driver is installed.

To view all drivers installed on a particular server, select the server from the **Application Servers** combo box.

Replicate installed driver

Select a server from the **Application Servers** combo box. To replicate a driver on all remaining application servers in the team that have the same operating system installed as that of the selected server, right click the driver and select **Replicate** menu item. The utility will attempt to install the driver on all remaining application servers with the same OS type. It then shows a message box with details including on which servers the installation has succeeded or failed.

Uninstall driver

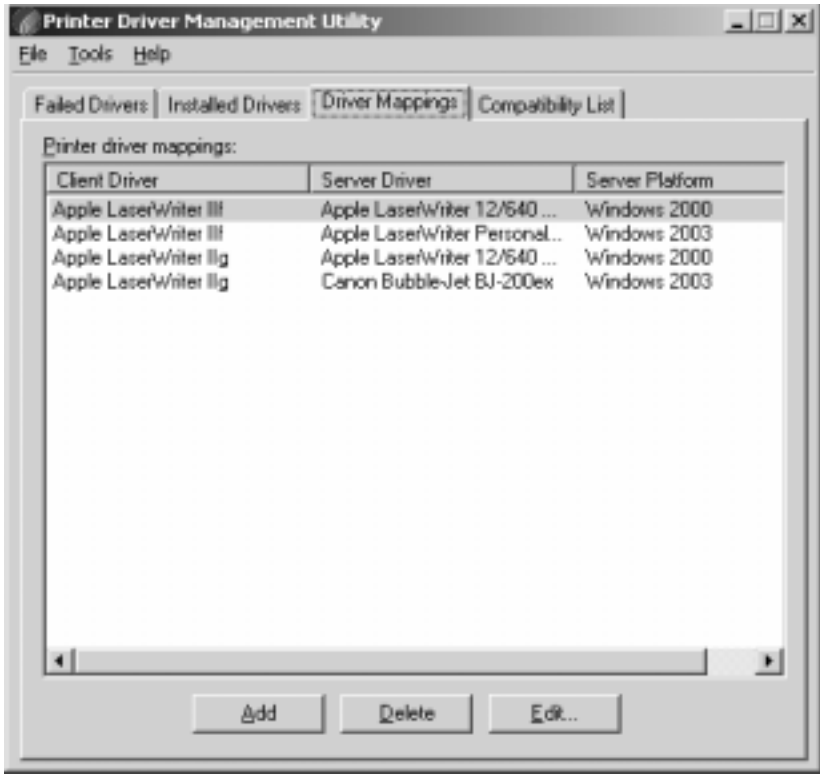
Select a server from the **Application Servers** combo box. Select a driver and right click, a pop-up menu is then displayed. Now select Uninstall from the pop-up menu and click on it. The utility will attempt to uninstall the driver from all application servers with the same operating system installed as that of the selected server. It shows a message box with details including on which servers the uninstall has succeeded or failed.

NOTE

NOTE: *The driver installation will fail if the driver is in use, that is if some printer is using the said driver.*

Driver Mapping Tab

This tab shows all the user defined mapping.



The user can add a new custom mapping or delete/edit driver mapping.

Add custom mapping

Click the **Add** button. It shows a dialog box with fields for server platform, client driver and server driver. Select server driver from the given list, select client driver from the given list or enter the driver name if it is not in the list. Select alternate driver and click on the OK button. The mapping is added to the Secure Global Desktop TSE database. The user cannot assign any custom server driver name.

Delete custom mapping

Select mapping to be deleted from Printer Driver Mappings list and click the **Delete** button. The system asks for confirmation before deleting the mapping. If the user clicks on the Yes button the mapping gets deleted from the database.

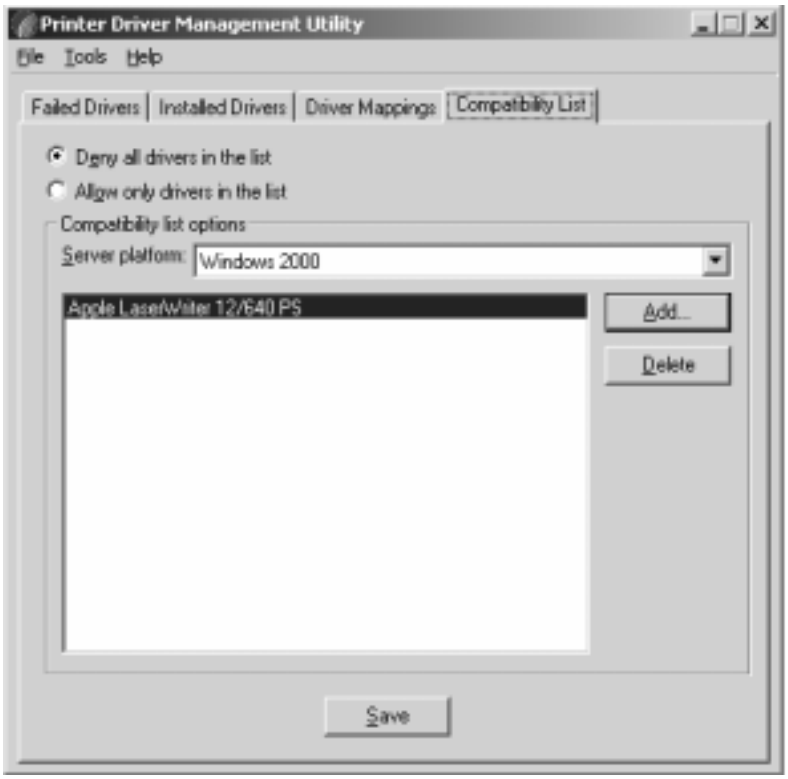
Edit custom mapping

To change any existing user defined mapping, select it and click the **Edit** button. A dialog box appears which shows the server platform, client driver and the server driver combo box. The user is allowed to edit the server driver only. Select the alternate driver and click the OK button.

Compatibility Tab

Here the administrator can create an allow-only/deny list of drivers.

Allow-only list – Only the drivers present in this list are allowed to be installed on an application server. Any other driver won't get installed and if any attempt is made to install, an entry will be made to the event log by the application server.



Deny list – All drivers except those in the list are allowed to be installed on the application server. If a client tries to install a denied driver, an entry is made to the event log by the application server.

The user can either create an allow list or a deny list. The list can be created for application servers running Windows 2000 Server or Windows Server 2003.

To add drivers in the list click the **Add** button. It pops up a dialog box showing a list of drivers, select the driver and click OK.

To delete a driver from list, select the driver and click the **Delete** button.

To save the list into the database click the **Save** button. A message box pops up asking for confirmation. Click **OK** to save the list.

If user closes the application without saving the changes in the tab, then during application close, a message box is shown indicating that there are some changes in the compatibility tab, and asking whether the user wants to save these changes. Click **Yes** to save the changes.

Refresh Installed Drivers List

The installed drivers list is maintained in the TSE database. Whenever a driver is installed on an application server through TSE, its entry is added to the list of installed drivers. However, if the administrator installs a driver manually, then its entry is not added to the database. This option allows the administrator to enumerate all installed drivers on all application servers in the team.

Go to **Tools->Refresh installed drivers** and click the menu item. This operation might take some time since the utility tries to collect the information from all application servers

in the team.

Update Bad Drivers List

Bad drivers are drivers that have shown not to be fully compatible with Windows Terminal Services. The list of such bad drivers is kept in the database. The list also contains the mapping information for the alternate driver (if applicable) for the bad driver. Tarantella keeps the latest list of bad printer drivers on a public web server. This list can be downloaded by the client if so desired. Go to **Tools->Update bad drivers list** and click the menu item. This operation might take some time depending on the connection speed.

IFS and Printer Data Compression

Data compression typically improves the perceived application performance and hence the end user experience in server-based computing. There are several means of compressing data. In the latest version of Secure Global Desktop TSE v4, the product uses the lossless scheme. This scheme is also called non-destructive because the initial data can always be recovered later.

Data compression reduces the amount of data transferred across the RDP session to increase IFS or printing performance over bandwidth-limited connections. Effective performance improvements depend on:

- Time taken by compressed data to travel across client-server network.
- Time taken to compress/decompress the data.

For instance, on low-bandwidth connections, the time taken by the data to travel across a client-server network is of major concern. So a higher compression-ratio algorithm will be preferred, even though it takes more time to compress/decompress the data. This is due to the fact that the majority of the time is consumed for the data transfer over the network, while only a minor part of the time is consumed for compressing/decompressing the data. However, for high-bandwidth

connections, the time taken by the data to travel over the network is minor. Therefore, a compression algorithm that executes faster is preferred.

The Connection Settings page of the Secure Global Desktop Management Console shows the following data compression related fields:

- **Client File System Sharing – Compression:-** This setting dictates whether IFS data will be compressed or not. This field can have values: **ON, OFF** or **UNSPECIFIED**. By default, it's **OFF**.
- **Client Printer Sharing - Compression (for Secure Global Desktop printing only):-** This setting dictates whether printer data will be compressed or not. This field can have values: **ON, OFF** or **UNSPECIFIED.** By default, it's **OFF.**

Bandwidth Throttling Management

Terminal sessions typically don't consume much bandwidth for RDP traffic. However, a large print job may consume available bandwidth in such a way that users are not able to use their terminal sessions until these print jobs are finished, especially on low-bandwidth connections. In previous versions of TSE there was no way by which an administrator could avoid performance problems in terminal sessions caused by large print jobs.

Therefore, the goal of this new feature in TSE v4 was to prevent performance problems with terminal sessions caused by large print jobs happening concurrently. Since printing is a job which can run in the background while the user can continue to work with other applications in a terminal session, the goals set out for effective bandwidth throttling management were:

- Consistent application performance over different network connections.
- Enhancing the usability of printing over low-bandwidth connections.

"Bandwidth throttling" is used to optimize network bandwidth usage to get more consistent application performance. It provides the administrator with a way to set a maximum threshold for the amount of bandwidth a print job may use. While it can slow down printing, it does prevent performance problems with terminal sessions that are running at the same time.

A typical bandwidth throttling implementation involves following steps:

- Slicing of network packets to a specified size.
- Sending these packets over a network in such a way that they don't exceed the specified bandwidth limit.

The Connection Settings page of the Secure Global Desktop Management Console shows the following bandwidth throttling related field:

- Client Printer Sharing - Limiting Bandwidth (for Secure Global Desktop printing only) :- This field specifies the bandwidth limit for printer traffic. It can have the following values: Low (28.8 kbps), Medium (56.6 kbps), High (128 kbps), and Unlimited. By default, the value is set to **"Unlimited"**.

Automated Administrator Tasks

This feature adds simple, but common and important tasks like Reboot Server, Synchronize Backup database and Synchronize Database with domain to servers in the Secure Global Desktop TSE team. These tasks can be scheduled to run at a specified time and on the specified server(s).

Secure Global Desktop TSE ships with two System Defined Tasks:

1. **Synchronize Backup Database Task** - This task will synchronize the backup database with the primary database. This task is scheduled to run daily at 4 AM.

2. **Synchronize Domain Task –** This task will synchronize domain objects like users, groups, OU and their memberships in the Secure Global Desktop TSE database with actual domain objects. This will run daily at 3 AM.

NOTE

NOTE: *System defined tasks cannot be removed. You cannot add or remove servers to System Defined tasks. You can only change the schedule of these tasks.*

Use **Manage->Tasks** tab to add, update or remove tasks.

This section provides step-by-step procedures to do the following:

- Add Task
- Remove Task
- Update Task
- Update Schedule
- Add Servers
- Remove Servers

Add Task

To add a new task:

1. On the **Manage>Tasks** page, click **Add Task**.
2. The **Add Task** page opens. While adding an Admin Role you need to define the “Task Information”.

Task Information. These are the Task information properties.

Name. This name identifies this task. Try to make this name descriptive of its responsibilities.

Description. This free-form field permits you to describe information about the new Task.

Task Settings. These are the Task settings:

Write Task status to application event log:- If this check box is selected, then whenever the task runs on a server it will make an event log entry specifying information if the task ran successfully or not.

Enabled:- If this check box is unchecked then the Task will not run on assigned servers.

Task Actions. These are the action settings for the Task:

Action to be performed:- Currently only one action is supported for a Task, which is Reboot Servers.

Run Only if No Active Session:- If this check box is checked then the Task will run on assigned Secure Global Desktop TSE application servers only if there are no active sessions running on that server.

Time To Give Active Session To Logoff:- If “Run Only If No Active Session” is not selected then before the rebooting of the application server starts, the Task will automatically logoff active sessions on that server. To specify the time interval to log off active sessions use this setting. Select one of the intervals from the drop down box.

Click **Next** to proceed to the **Select Servers** page.

Select Servers. The **Select Servers** page allows you to select the Servers on which this Task will run. Select the Servers and click **Next** to proceed to the **Set Schedule** page.

Set Schedule. This page will allow you to schedule this new Task.

Run This Task:- You can choose the Task to run daily or weekly depending on your needs. If you choose the Task to run weekly then the day selection page will appear only after you click **Next.**

Start Time (hh:mm):- Specify the start time (hh:mm) to run the Task on the servers. Click **Next** to go to day of week selection page if you have chosen to run the Task weekly, else **Next** will take you to the confirmation page.

Day of Week:- This page will allow you to select the day(s) of the week on which you want to run the Task. Click **Next** to go to the confirmation page, verify all the details about the new Task and then click **Add** to add the Task.

Remove Task

The **Remove Task** action allows you to remove an existing Task from the Secure Global Desktop TSE system.

To remove a Task:

1. From the **Manage>Tasks** page, select the Tasks you want to remove and click **Next**.
2. The **Remove Task** page lists the roles you choose. Review the information and click **Remove**.

NOTE

You cannot remove system defined Tasks (see above) from the system.

Update Task

The **Update Task** action allows you to change Task information and the Tasks settings.

To update a Task:

1. From the **Manage>Tasks** page, select the Task you want to update and click **Next**.
2. Change the relevant fields and click **Update**.

For more information on the fields on this page, refer to "Add Task Information".

Update Schedule

The **Update Schedule** action allows you to change the Task Schedule.

To update the Task Schedule:

1. From the **Manage>Tasks** page, select the Task for which you want to update the schedule and click **Next**.
2. On **Update Schedule** page change the current schedule to the new schedule to run the Task and click **Next**.
3. Review the task schedule information and then click **Update**.

For more information on the fields on this page, refer to "Set Schedule".

Add Servers

You can add servers from the Secure Global Desktop TSE team for existing Tasks to run.

To add servers to the Task:

1. From the **Manage>Tasks** page, select Tasks, and then click **Add Servers**.

2. Select the servers on which you want to run the selected Tasks, and click **Add**. These Tasks will now run at scheduled intervals.

NOTE

NOTE: *You can add multiple tasks to multiple servers at one time by selecting multiple tasks t oadd and selecting multiple servers to receive.*

Remove Servers

To stop Tasks from running on servers:

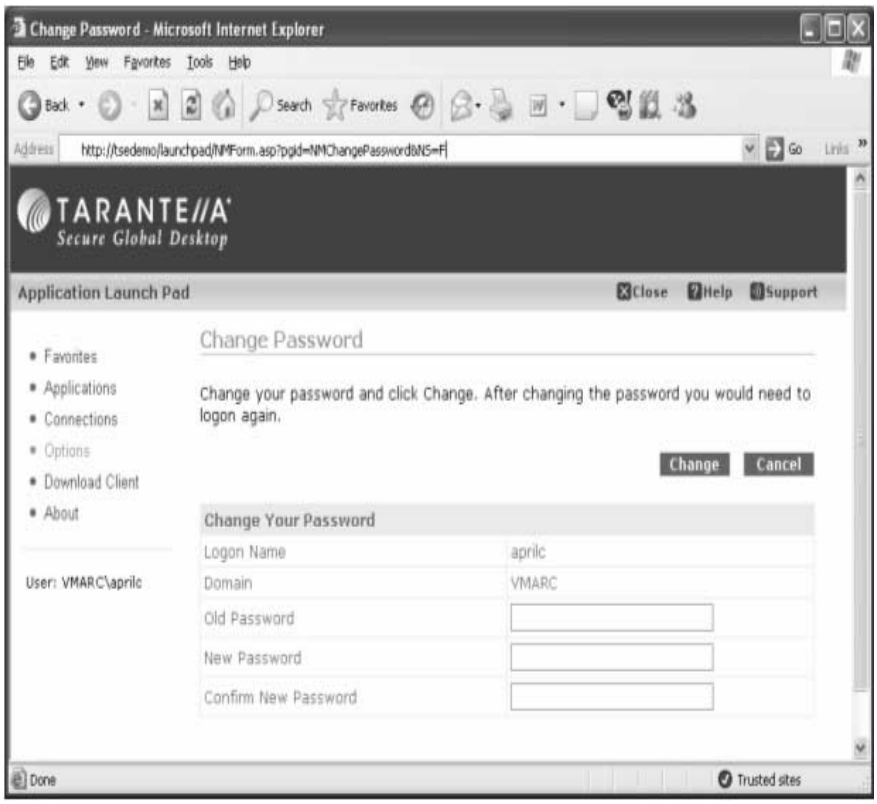
1. From the **Manage>Tasks** page, select a Task, and then click **Remove Servers**.
2. Select the servers and click **Remove**.

Change Password

The Change Password feature will allow users to change their domain password from the Secure Global Desktop – TSE Launchpad. By default this feature is enabled. Secure Global Desktop TSE Console administrators can disable this feature from **Console -> Options -> User** page.

When a user logs into the Secure Global Desktop TSE Launchpad, she will see a **Change Password** button on the **Options** page. After clicking this button the user will be directed to the **Change Password** page. To change your password, type your old password and new password and click **Change**. You will be asked to re-login into Launchpad again after this.

If the password is expired you will get a warning to change your password upon logging into the Launchpad. At this stage you can either change the password using the **Options** page or launch an application. The application launch will pop up a Windows Change Password dialog box on the application server. Use this dialog to change your password.



Connection Setting Monitoring

Feature Monitor -> Connections -> View Session Details

One of the primary functions of Secure Global Desktop TSE is to facilitate secure and managed RDP connections between client and server computers. Connection settings objects set the parameters of these connections. Administrators can assign a connection setting to an individual application to override the system's default setting.

Initially, users connect with the settings that are marked as the default settings. If a user needs to override the default connection setting for a particular client, the user can choose the setting from the **Option** page of the LaunchPad. The chosen setting is remembered on the client computer. This way, administrators can tailor the connections used on a particular computer to the network performance of the computer.

Thus, the administrator can assign existing Connection Settings to Client Groups and also to applications. In addition, a user can select Connection Settings from the LaunchPad.

The effective Connection Settings that are returned to the user can be a combination of the Client Group Connection Settings, Application Connection Settings, User Connection Settings, and Default Connection Settings. The precedence order for each type of Connection Settings is Client Group Settings, Application Connection Settings, and User Connection Settings. If none of these values is specified, the Connection Settings specified in the Connection Settings set as Default Connection Settings are used.

As connection settings can be applied at various levels (see above) and as there is some logic applied that calculates the effective connection settings, it can become a challenge for an administrator to determine or troubleshoot the effective set of connection settings that controls the behaviour of a particular session.

Therefore, a new feature has been added in TSE v4 to help the administrator view and manage individual Connection Settings. In the **Monitor -> Connections** page of the TSE Management Console, select any particular session and click on **View Session Details**. This page shows the effective Connection settings being applied to the session.

Native Windows Client Connections

Overview

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 a server-based TSE application via a Native RDP Client Connection provides several key benefits:

- Support for RDP 5.x feature set
- Publishing of applications to web-based interface (TSE Launchpad)
- Resource-based load-balancing for the native RDP session
- No additional installation of a vendor-specific client component

On the other hand, when launching applications using a Native RDP Client Connection, you will lose many feature enhanceme nts that Tarantella's Secure Global Desktop TSE clients provide. The following features will **NOT be available** in case of a Native RDP Client Connection launch:

- Seamless windows
- SPR Support
- File Associations
- Desktop and Start menu Shortcuts
- Enhanced Secure Global Desktop TSE Printing support

Native Client on Windows

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

The TSAC ActiveX control and hence the Native RDP Client Connection feature for Windows will not work if the security settings of the Internet Explorer for "ActiveX controls and plugins" are not configured to enable "Run ActiveX controls and plugin" and "Script ActiveX controls marked safe for scripting".

How to Access the Feature?

To launch applications using the Native RDP Client Connection feature one may append a "?Client=native" string to the launchpad URL. For example if the Launchpad URL is http://www.company.com/launchpad, then, to access the Launchpad via the Native RDP Client, use the following URL:

http://www.comp any.com/launchpad?Client=Native

Alternately, you can go to the Download Client page on the TSE Launchpad and select the "Use Native Client" button.

Description

When you launch an application through the TSE Launchpad using the Native RDP Client, then this launch is marked as a Native launch. For Native launches, an additional browser window is popped up and you can see the application or the remote deskt op in this new browser window. On the Connections page of the TSE Launchpad, the Active Connections list will mark any such launches as "Native" in the third column named "Client Type". The "Client Type" column in the "Active Connections on other clients" indicates "Native" in case of sessions that are launched using the Native Client. The Connections page in the Monitor tab of the Management Console will always specify a "Client Type" as either Native or Secure Global Desktop, as appropriate.

Reconnecting/Disconnecting a Native RDP Client Session

Even if you launch an application using the Native RDP Client Connection feature from one machine, you will be able to reconnect to this application from a different machine that has the Secure Global Desktop TSE Client Software installed. However, while the new machine has the proper client software installed, the application will still be reconnected as a Native RDP Client Launch. In other words, an application launched with the Native RDP Client Connection feature will always remain a natively run application, no matter whether the Secure Global Desktop TSE client software is installed or not on the machine that you use to reconnect to the application.

Native Macintosh Client Connections

Overview

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 a server-based TSE application via a Native RDP Client Connection provides several key benefits:

- Support for RDP 5.x feature set
- Publishing of applications to web-based interface (TSE Launchpad)
- Resource-based load-balancing for the native RDP session
- No additional installation of a vendor-specific client component

On the other hand, when launching applications using a Native RDP Client Connection, you will lose many feature enhancements that Tarantella's Secure Global Desktop TSE clients provide. The following features will **NOT be available** in case of a Native RDP Client Connection launch:

- Seamless windows
- SPR Support
- File Associations
- Desktop and Start menu Shortcuts
- Enhanced Secure Global Desktop TSE Printing support

Native Client on Apple Macintosh

Launching Secure Global Desktop 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 Secure Global Desktop 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.

How to Access the Feature?

To access TSE from an Apple Macintosh device for the first time you will need to have the Microsoft RDP client for Macintosh as well as the Tarantella Plug-in for TSE installed. Please complete the following steps:

- First, make sure that the Microsoft RDP client for Macintosh is already installed on your device; if you don't have the latest RDP client installed on your device, you can download it at

  http://www.microsoft.com/downloads/details.aspx?FamilyID=6573f9f1-8ae1-4da9- ab5c-f8457ecdaf2d&DisplayLang=en#filelist
- Next, point the browser on your Macintosh to the TSE Launchpad. TSE will sense the Macintosh operating system on your device and will offer you to download a 'native client' for your device.
- Clicking on the Download button will install the Secure Global Desktop TSE plug-in (1SGDMacPlugin) for Macintosh OS X by running the Apple Installer.
- Follow the instructions of the Apple Installer.
- Upon completion of the Apple Installer, the Secure Global Desktop TSE plug-in will be installed to the /Library/Internet Plug-Ins/ path of the drive you selected.
- Close your browser, restart it, and point it to the TSE Launchpad. You will now be able to launch an application from any application icon on the Launchpad.

A current limitation of the Microsoft Remote Desktop Connection Client for Mac is that there can be only one application launched from an application server at a time.

Deploying Secure Global Desktop roles

Secure Global Desktop uses roles to assign a specific task to one or more servers. The administrator first needs to add a server to the Secure Global Desktop team and then add the

relevant roles to the server. The roles an administrator can deploy from the Management Console are:

- Web Server Role
- Application Server Role
- Load Balancer Role
- Relay Server Role

Role requirements

Secure Global Desktop can push any role to any server in the team, but each server must already have the specific minimum hardware and software configuration required to operate each role received. Pentium III, 400 MHz, Windows 2000, or Windows 2003 servers generally have the software required for most roles, but to run the Application Server role, a server must be configured in Application mode.

NOTE

If the Console is running in secure mode (HTTPS), the Depot folder on the Web Server has to have plain HTTP access, even if the other folders are secured as HTTPS.

The configuration requirements for the various Secure Global Desktop roles follow, along with the MDAC, SQL server and browser requirements.

Secure Global Desktop Web Server role

The Secure Global Desktop Web Server role requires the following software:

- Windows 2000 Server or Advanced Server with Service Pack 3 or Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition or Windows Server 2003, Web Edition
- Internet Information Services (IIS)
- MDAC
- Browser

Secure Global Desktop Load Balancer role

The Secure Global Desktop Load Balancer role requires the following software:

- Windows 2000 Server or Advanced Server with Service Pack 3 or Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition
- MDAC

Secure Global Desktop Relay Server role

The Secure Global Desktop Load Balancer role requires the following software:

- Windows 2000 Server or Advanced Server with Service Pack 3 or Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition
- MDAC

Secure Global Desktop Application Server role

You must have a system with the following:

- Windows 2000 Server or Advanced Server with Service Pack 3 or Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition
- Windows Terminal Services installed in Application Server Mode with the service running.

- MDAC

SQL Server

The following versions are supported:

- MSDE with Service Pack 3

NOTE

Secure Global Desktop installation provides you the option of installing MSDE with Service Pack 3. Additionally, the CD provides you the software for upgrading to MSDE Service Pack 3 if you have an earlier version already installed. When you choose this option, ADO is also upgraded to MDAC 2.7 if the version of ADO on the server on which the administrator installs the MSDE is older than MDAC 2.7. The existing database applications on the server that depend on a particular version of ADO may no longer function properly after an MSDE install or upgrade. To avoid this, do not install MSDE on the Application Server, or verify that the database client applications will work with the MDAC version that MSDE would install.

- SQL Server 7 with Service Pack 3
- SQL Server 2000 with Service Pack 3

NOTE

The SQL Server should be installed with case insensitive collation settings.

MDAC

The following versions are supported:

- MDAC 2.5 (without multiple-instance SQL server installations)
- MDAC 2.6 (not MDAC 2.6 with SP1)
- MDAC 2.7

Browser

The following versions are supported:

- Internet Explorer 5.5, Internet Explorer 6 with Service Pack 1.

NOTE

Cookies should be enabled to logon to the Console. Netscape Browser is not supported by the Management Console.

Server Identification in Secure Global Desktop

The administrator needs to enter the name of the server while adding a server to the team. Further, the system also needs the internal IP address of the server and a published IP address of the server. This section explains the use of these in the system.

Server Name

Name of the server as shown in console. This value is read-only in console and Secure Global Desktop Engine detects the name of the server. Secure Global Desktop Engine can put either NetBIOS or FQDN name. Server name given in console while adding the server is used to connect to the server.

Internal IP

This IP address of the server is used by other Secure Global Desktop servers to communicate with this server. This value is also given to the clients if a published IP address is not specified. Secure Global Desktop Engine auto-detects the IP address of the server. Sometimes the administrator may want to disable auto-detect. For instance, when the server has multiple network cards, or one card has multiple IP addresses assigned. In such cases, the IP address selected by Secure Global Desktop Engine might not be the right one. The administrator can disable auto-detection in the Add Server or Update Server sequence from the **Manage>Servers** page. The administrator can then specify a NetBIOS name, FQDN name, or IP address to be used. Unless auto discovery is disabled, values entered by the administrator are overwritten by the Secure Global Desktop Engine. For more information, refer to "Add a server".

NOTE

The Secure Global Desktop system does not do any validation checks on the value entered here. Whatever is entered by the administrator, is used by Secure Global Desktop, so the administrator has to be very sure about this value. Otherwise, it may result in an unstable system where other servers in team might not be able to talk to this server.

Published Address

This IP address is given to the clients. Internal IP address might not be routable from client, so the administrator can put two network cards on the server, or have two IP addresses on the same card and make one of them externally routable. Published Address is used only when it is defined; otherwise, the clients always get the Internal IP address. The Administrator may enter the IP address or an FQDN name in this field.

Web Server role

The purpose of the Web Server role is to provide a front-end to Secure Global Desktop end users and Secure Global Desktop administrators.

Secure Global Desktop implements the Web Server role using Web pages (asp, xml, xsl) that are located in the following folder on the IIS server: `\inetpub\wwwroot`.

When Secure Global Desktop deploys a Web Server role, Secure Global Desktop creates Console, Depot, and Launch Pad folders.

- **Console folder**. This folder contains the pages and logic that create the interface that enables an administrator to configure and manage Secure Global Desktop.
- **Depot folder**. This folder contains the software that you need to install Secure Global Desktop to either a client or a server (for deploying additional roles). Following is the description of some of the more important files and folders in the Depot folder:
  - **SGD-TSE-Roles.msi file**. This contains the binaries used to deploy a role to another server.
  - **Versions folder**. This contains the individual installs for the Tarantella Connection Manager and the WTS client. These functions are separate to facilitate individual component upgrades and to simplify client deployments (via automatic version checking and upgrades).
  - **Icons folder**. This contains the icons of the applications that are available in the system.
- **Launch Pad**. This folder contains pages that the end users connect to in order to access their applications.

When Secure Global Desktop deploys a Web Server role, Secure Global Desktop also uses COM+ Applications. There are six COM+ applications:

- Secure Global Desktop Application Engine
- Secure Global Desktop Jobs Framework Engine
- Secure Global Desktop Domain Engine
- Secure Global Desktop License Engine
- Secure Global Desktop Management Engine
- Secure Global Desktop Database Access Engine

Load Balancer role

The purpose of the Load Balancer role is to improve the performance of the application delivery process by utilizing the available resources in an intelligent way. It distributes application delivery requests to the server that is best suited to handle the request. The Load Balancer uses an algorithm to determine which server, from those available to the requestor, has the largest amount of free resources.

By default, Secure Global Desktop installs the Load Balancer role in the folder `\program files\Tarantella\Load Balancer` on the server that is to be the Load Balancer Server, and

this Load Balancer Server can be any server in the team that has enough resources to handle the additional tasks associated with the Load Balancer role.

To provide redundancy for the Load Balancer Role, you should install the role on more than one server.

The Load Balancer scheme provides the concept of a Master Load Balancer and Peer Load Balancers. All the Application Servers in the system register with the Master Load Balancer.

The Peer Load Balancers choose one Load Balancer from amongst themselves to become the Master Load Balancer. Every other Load Balancer in the system keeps track of the health of this Master Load Balancer. If the Master Load Balancer fails, then the Peer Load Balancers cooperate to select a new Master Load Balancer and the Application Servers register with the new Master Load Balancer. This process creates a failover mechanism and ensures system continuity, if ever there is a Master Load Balancer failure.

When a Master Load Balancer goes down, it takes a maximum of thirty seconds to discover that the Load Balancer is offline. The new Master Load Balancer waits for all the Application Servers to register with it. This process takes a maximum of 2 minutes. No applications can be launched in that interval. However, the existing application sessions continue as usual.

If the Master Load Balancer goes down when promoting the Secondary Database Server, no other Load Balancer takes over as Master Load Balancer until the promotion is over.

The Load Balancer in Secure Global Desktop version 4.0 is scalable.

The Application Servers ping the Load Balancers once a minute. The Master Load Balancer discovers within 3 minutes if an Application Server goes down and does not send any more sessions to the Application Server.

Relay Server role

The purpose of the Relay Server role is to enhance security by opening only one port for communication with client computers. If you are not using port 443, you can deploy the Relay Server role to a Web Server.

Relay Server role is a non-essential role. By default, installation of Secure Global Desktop does not install the Relay Server role like other roles. In the Secure Global Desktop team, the Secure Global Desktop administrator can deploy the Relay Server role on a Windows 2000 Server or a Windows Server 2003.

Prerequisites

- Windows 2000 Server or Advanced Server with SP3, or Windows Server 2003, Standard Edition or Windows Server 2003, Enterprise Edition.
- The port configured for the single port relay should be available. The system does not allow pushing of the Relay Server role on a server on which the port configured for single port relay is not available.
- If the administrator has to add the Relay Server role on a server that is a Web Server, the administrator should disable the SSL port on the IIS or change the IIS port.

Deploying the entire system to run on a single port

The administrator needs to do the following:

- Distribute Relay Servers and Web Server on mutually exclusive servers. If both are installed on the same server, both will compete for the same port. Hence, in such a case, two ports are required.
- Set the same port on the Web Server and Relay Server for communication.
- Ensure there are enough roles of each kind to take care of the load.

Deploying multiple Single Port Relay Servers

The Secure Global Desktop administrator can configure multiple Relay Servers to balance the load on the servers in the Secure Global Desktop team depending on the number of users. Secure Global Desktop uses round-robin logic to balance the load among different Relay Servers.

For a session, a client uses the same Relay Server. When a team is configured with multiple Relay Servers, if one Relay Server is offline, another takes over. However, if a Relay Server that has an application launched from it goes offline, the session goes to a disconnect state, if enabled, or logs off.

Deployment scenarios

The administrator needs to take a calculated decision on which client computers should go through the Single Port Relay Server. Single port affects performance; hence, the use should be limited to where needed.

The administrator can configure the clients that should use Single Port Relay using:

Connection settings for

- Client Groups
- Applications
- Users
    - URL specification. For more information, refer to "Relay switch for Launch Pad".

Thus, to make different clients use or not use Single Port Relay Server, do any one of the following:

- Create two Client Groups based on IP addresses for internal and external users. For internal users, turn off Single Port Relay.
- Use the firewall / DNS to route the right clients to Single Port Relay on, by using the special URL property.

DMZ /Firewall /VPN and the Single Port Relay Server

Single Port Relay Server in the DMZ

The following diagram is a symbolic representation of the protocols and ports used by the Secure Global Desktop components when the Single Port Relay and the Web Server are placed in the DMZ.

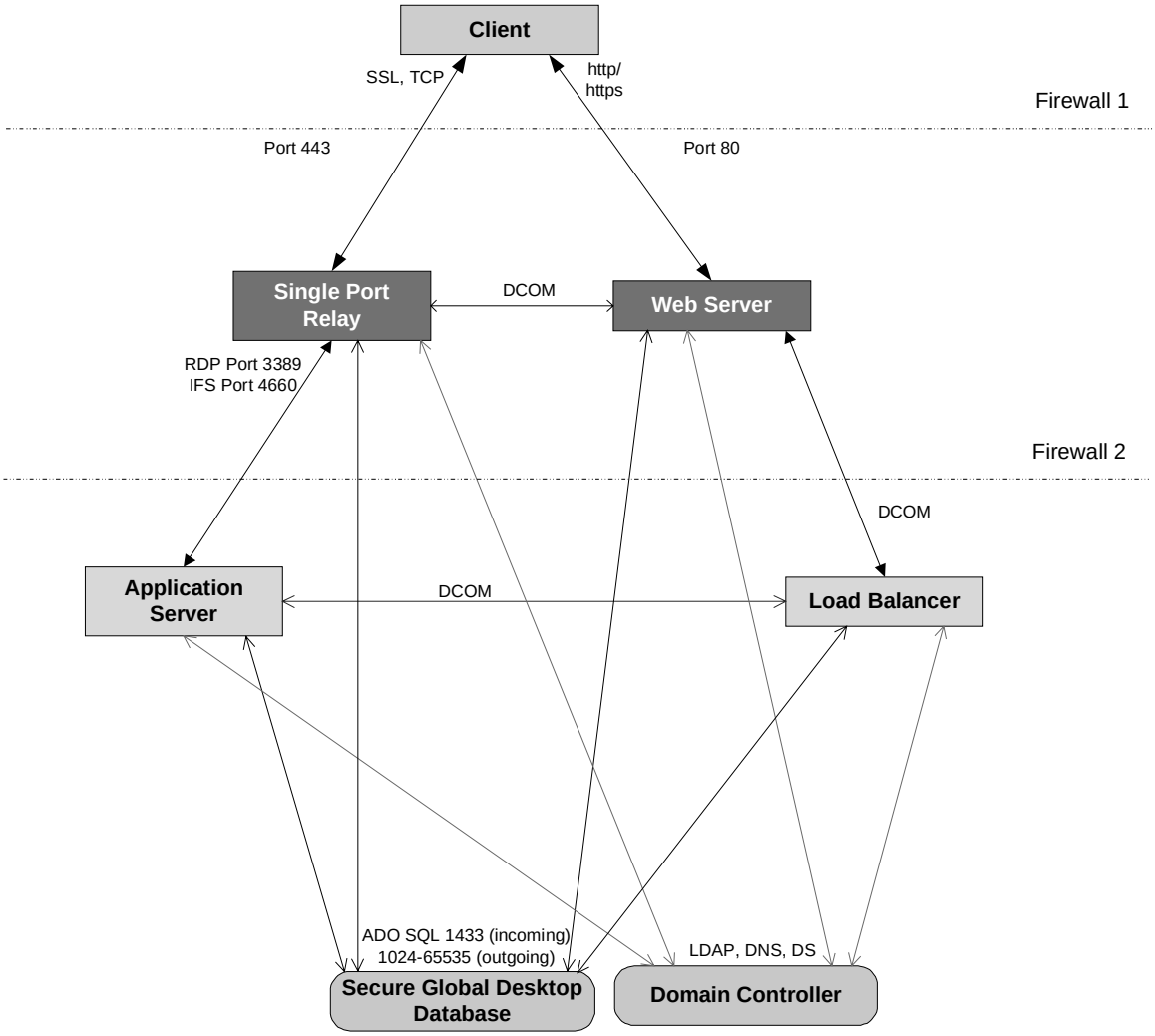


FIGURE 12. Single Port Relay Server in DMZ

Communication with Domain Controller uses:

- TCP/UDP protocol on MS-DS Traffic port 445
- TCP/UDP protocol on Kerberos port 88
- TCP/UDP protocol on LDAP port 389
- TCP/UDP protocol on DNS port 53

DCOM Calls use TCP protocol on port 135. Additionally, Microsoft recommends that you open a minimum of 15 to 20 ports from port 5000 and up. For more information, refer to http://support.microsoft.com/default.aspx?scid=kb;EN-US;250367.

SQL Server uses named pipes by default. You will have to configure a TCP provider on the Single Port Relay and the Web Server.

To specify TCP/IP as the transport append the following to the connection string using the CRK.

```
;network=DBMSSOCN;
```

To specify a port as well if SQL running on a port other than port 1433, use the following format

```
server=<servername>,<portnumber>
```

To summarize, following is an example of the connection string.

```
Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security
Info=False;Initial
Catalog=CanaveralDB;Server=192.168.9.55,2443;network=DBMSSOCN;
```

Alternatively, you can set the port and transport for the whole computer (from where ADO connection is being made). You may use the SQL Client Network utility to configure this. However, this is less useful if there are multiple applications running on the same computer.

Single Port Relay Server inside Firewall

The following diagram is a symbolic representation of the protocols and ports used by the Secure Global Desktop components when the Single Port Relay and the Web Server are placed inside the firewall.

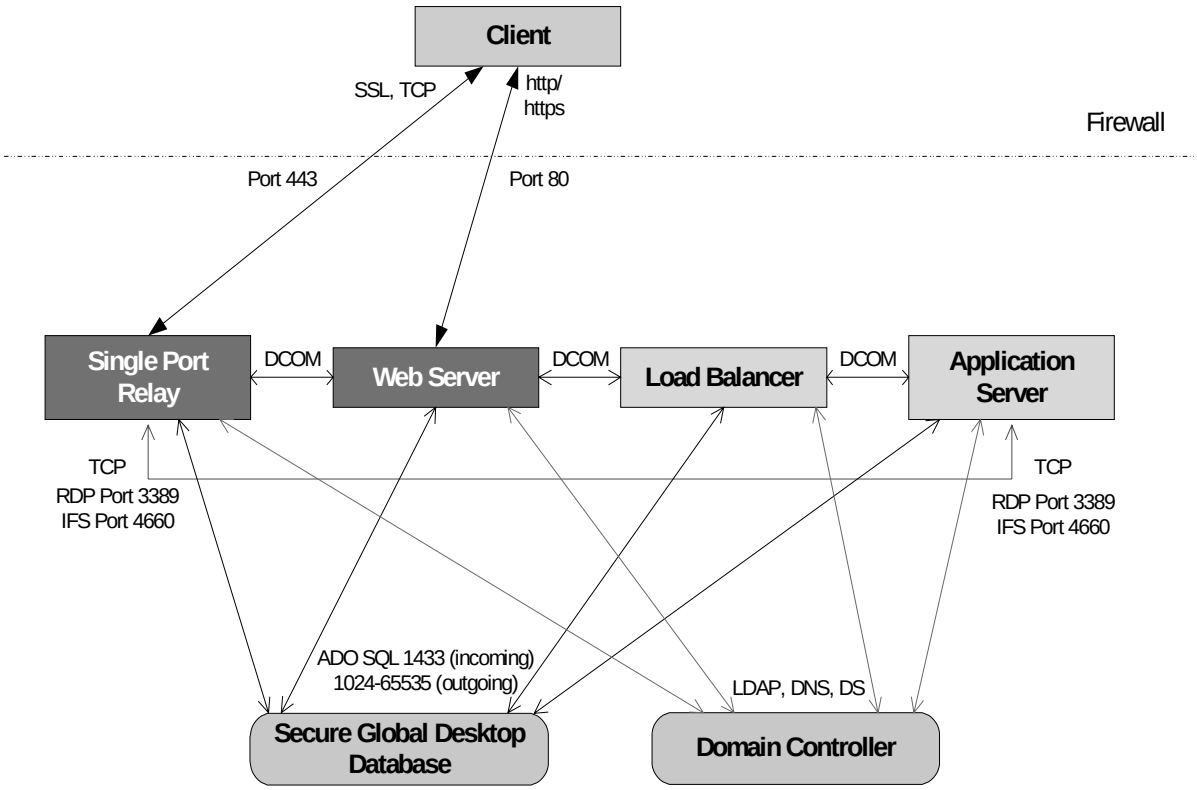


FIGURE 13. Single Port Relay Server inside Firewall

Communication with Domain Controller uses:

- TCP/UDP protocol on MS-DS Traffic port 445
- TCP/UDP protocol on Kerberos port 88
- TCP/UDP protocol on LDAP port 389
- TCP/UDP protocol on DNS port 53

DCOM Calls use TCP protocol on port 135. Additionally, Microsoft recommends that you open a minimum of 15 to 20 ports from port 5000 and up. For more information, refer to http://support.microsoft.com/default.aspx?scid=kb;EN-US;250367.

Application Server role

The purpose of the Application Server role is to enable Secure Global Desktop to control the terminal server, either Microsoft Windows 2000 Terminal Services (WTS) or Microsoft Windows Server 2003. Secure Global Desktop will manage the applications that have been installed on these Application Servers.

Local server install

Secure Global Desktop can function in two possible modes.

- Domain install mode, where domain resources (such as users, groups, and computers) are available.
- Local server install, where it is limited to local computer resources only.

In the second case, the local server may or may not be a part of a domain. Thus, for installations where a domain is not accessible, administrators are still able to use Secure Global Desktop using local user credentials.

Administrators and users

Secure Global Desktop administrators for the local server install have to be members of a local group. These administrators can then launch the Console, add applications on the server, and assign them to local users and groups.

Local users can launch the applications assigned to them when they logon locally. External users can connect to the Launch Pad and launch applications as long as they logon using a local user credentials.

In this case, only unibox install is supported. That is, all the roles have to be installed on a single server. Further, the database must also be on the same server. The software and hardware requirements for the servers are the same as those for any other Secure Global Desktop installation.

If the computer on which Secure Global Desktop is being installed is a part of a Domain, the Administrator has the choice to do a domain install or a local server install. If the computer is not in a domain, only a local server install is possible

Limitations

A local server install has the following limitations when compared to a domain install:

- The installation has to be a unibox installation
- An administrator cannot add another server to the team
- Since the default port for Single Port Relay is same as the SSL port for a Web Server, Single Port Relay cannot be used without changing the default port
- Since the install is limited to one computer only, backup of database is possible only when you use a named instance of SQL server/ MSDE (which might not make a lot of sense)
- Domain objects (such as OUs) are not available

Local server install and domain users

In a Secure Global Desktop team that has been installed for local users only, sometimes a local user cannot see the provisioned applications after logging on to the Launch Pad. This happens when the group to which the local user belongs also has some domain users as members of the group, and the server is no longer in the domain. In this case, the server is unable to resolve the user SIDs of the domain users.

The administrator should remove the users with unresolved user SIDs from the group and provision another application to the same group. Now, when the user refreshes the application list, the application icons are displayed on the Launch Pad. Alternatively, after the unresolved SIDs are removed, the administrator should delete the user from Console. The next time the user logs on, all the assigned applications are displayed.

To be able to logon to the Launch Pad or the Console in a local server install setup, the users should have a valid Logon Name and Password. Users with blank password cannot logon to the console and the Launch Pad.

It is not possible to do a local server install on a domain controller.

NOTE

If the computer is not in a domain, then only a local server install is possible. In case of local server install, Secure Global Desktop Administrator cannot change the Domain Name field (fixed to local server name) while changing the Secure Global Desktop Administrator group from Console.

Publishing a Windows Desktop

Whenever a user logs on to a server using Terminal Services, the shell is launched on the server. Accessing shell with Terminal Services means getting access to the desktop of the server.

The Publishing a Windows Desktop feature in Secure Global Desktop makes it easy for the Secure Global Desktop administrators to provision Shell (by default, explorer.exe) for the Application Servers. A Secure Global Desktop administrator can directly publish the desktop for users without having to put in the path of the shell manually as Secure Global Desktop puts in the path.

While publishing the desktop, the administrator can specify Connection Settings. We have provided “Shell” Connection Settings, which is an optimized set of connection settings for shell provisioning.

NOTE

If you provision a shell with connection settings that allow multiple application launches per session, and multiple applications are launched in a session, then logging off a published desktop closes all the applications in that session.

The user can access the Application Server desktop from the Launch Pad and use any application on the Application Server.

Publishing a Windows Desktop is particularly useful in case of CE clients. The administrator can install all the applications needed by a group or an OU on an Application Server and provision a shell for the required groups. The users can then logon to the Secure Global Desktop team using the Launch Pad and access the shell. The user gets the feel of having the Application Server desktop as own desktop.

NOTE

For this feature to work, v2.1 or later of the Tarantella Connection Manager should be installed on the Application Server.

Steps for publishing a Desktop

An administrator has to do the following for publishing a desktop:

1. Publish a desktop by choosing the Windows Desktop option from the Add Application page on the Console.
2. Add Application Servers.
3. Add groups, organizational units.
4. Install a client on the Application Server.

NOTE

We recommend that you choose the built-in set of optimum connection settings called "Shell" for publishing a desktop.

Behavior

When a user accesses the remote Windows Desktop from a client computer, the client has access to all the Secure Global Desktop shortcuts on the Application Server. Subsequent launches via these Secure Global Desktop shortcuts are metered by the system as if the launch came from the original client computer. This can be viewed from the **Monitor>Connections** page.

When the client launches an application, the desktop server is the preferred server as the first server to launch these applications. If the desktop server is not available, the Load Balancer directs the application to another available Application Server.

A single Secure Global Desktop license is used for the launch.

IFS

The client drives are redirected twice and the Application Server drives are redirected once if the application is launched from another Application Server. When you make a remote desktop connection, IFS maps the client drives on the remote Application Server. Any application launched from that remote desktop will launch in the same RDP session as the desktop if the application is available on that Application Server. If the application is not available on the same remote server, a new RDP session will be to an Application Server where the application is available. When connection is made to the new server, the client drives and the remote desktop drivers (which include the original client drivers) will be mapped on the new server. Thus doubling the client drives along with the original remote desktop drives.

Security implications

If the shell is the default windows shell (explorer.exe), then the user accessing the desktop is able to launch any application that is present on the Application Server. If the user has administrative rights on the Application Server, the user gets total control of the server.

Load balancing

Secure Global Desktop enables administrators to load balance terminal server application sessions based on the resources of the Application Servers. Secure Global Desktop supports resource based application-level load balancing as well as resource based connection-level load balancing.

The following figure shows the Load balancing architecture with clients, Secure Global Desktop severs, and Application delivery servers.

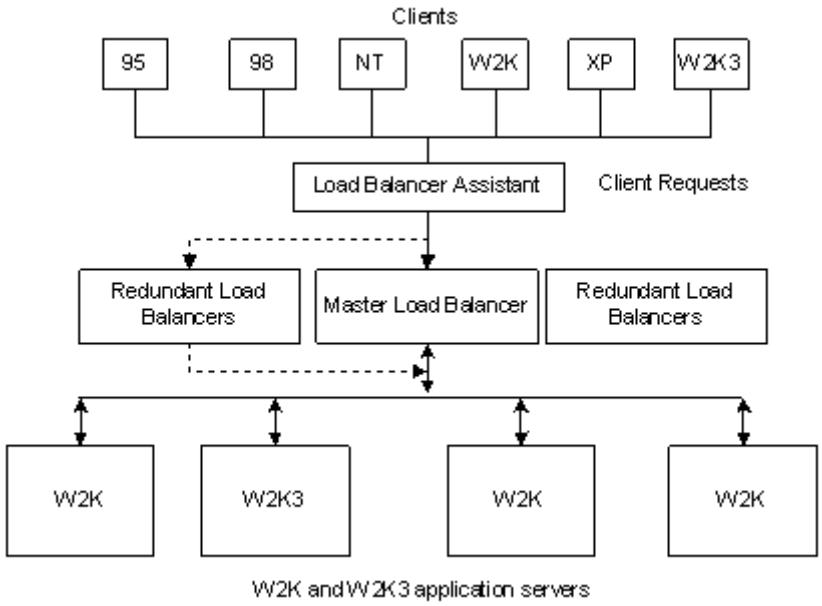


FIGURE 14. Load Balancing Architecture

Secure Global Desktop can have multiple servers designated to perform the job of load balancing by giving them the “Load Balancer” role. These servers could include the same server as the Application Server in small deployments, or could be a separate dedicated server for larger deployments.

For redundancy, there should be more than one Load Balancer in the system.

Once the Load Balancer service starts, it checks to see if a Master Load Balancer exists in the system. If one does not exist, then this load balancer service tries to declare itself the Master Load Balancer. All the Application Servers in the system register themselves with the Master Load Balancer. The Load Balancer Assistant also uses Master Load Balancer to forward the client requests. When Master Load Balancer goes down, other Load Balancers detect this and collaborate to select the new Master Load Balancer. All of the Application Servers and Load Balancer Assistants, who are in periodic contact with the Master Load Balancer, detect this change and begin communicating with this new Master Load Balancer, and Secure Global Desktop processing persists with data integrity.

Process flow:

1. Based on a few metrics, Secure Global Desktop elects the server that will function as the primary or the Master Load Balancer.
2. The Application Servers now register themselves with this primary load balancer.
3. The Load Balancer now talks to the database about this Application Server, gets the response concerning the applications provisioned to it, and replies back to the Application Server with all the application settings required to perform this task.

4. The Application Server now initiates itself with this response and waits for the next application session request.
5. On a regular basis, the Application Server reports its own perform metrics to the Load Balancer.

File associations

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

When a user double-clicks a file that is associated with an application on an Application Server, the file automatically opens in the application on the remote Application Server.

Associating file extensions with applications

The Secure Global Desktop Administrator can associate applications with file extensions from the console. Depending on the user settings made by the administrator, they may be binding for the user.

Making file associations from the Console

Secure Global Desktop Administrators can create file associations for each application that they provision on the Secure Global Desktop Application Servers. The administrator can make these associations while adding a new application to the Secure Global Desktop Team, or while updating file associations for an existing application.

When the administrator provisions an application and assigns it to multiple Application Servers, the administrator gets an intersection of all the current associations on all the selected servers for this application. These file associations on each server are taken from the HKLM registry hive.

NOTE

Like all other provisioned applications, the applications with file associations also launch in accordance with the licensing scheme.

The administrator then selects one or many of these extensions for file association. For example, consider the scenario where the administrator adds PaintShopPro as an application named PSPEastCoast, and assigns it to two Application Servers, AppEast1and AppEast2, out of the three available servers. The table that follows explains the concept.

TABLE 7. File Associations on Servers

Application Server	Extensions Available on Server	Extensions Available for Association
AppEast1	**.bmp, .gif, .jpeg**	**.bmp, .jpeg**
AppEast2	**.bmp, .jpeg, .tiff**	
AppEast3		

The administrator can now associate the application with .bmp and .jpeg extensions.

Further, for each application, the administrators can make these file associations binding for the users. Alternatively, they can give the users the choice to enable Secure Global Desktop file association for the each application. For more details on how to make file associations from the Console, refer to "Update file associations".

NOTE

If another application that hijacks the file associations is installed on top of an existing server, then this new application is launched even if the administrator has not provisioned it.

Enabling file associations from the Launch Pad

If the Administrator settings allow the user to enable file associations, the user can use the Launch Pad to select the desired applications for file association.

On the other hand, if the Administrator settings make the application settings binding on the user, the file associations made by the Administrator will be created on the client computer. For more information on how to enable file associations assigned by the administrator from the Launch Pad, refer to *Secure Global Desktop User Guide*.

File associations and the user's computer

Whenever the file associations are enabled, they are created on the user's computer whenever any 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 Link on the Launch Pad
- Right-clicks the Tarantella Connection Manager icon on the Task Manager and selects Refresh all shortcuts
- 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.

On a Windows 95 or Windows 98 computer, file associations modify the HKEY_LOCAL_MACHINE registry key. On a Windows 2000 or Windows 2003 computer, file associations modify the HKEY_CURRENT_USER registry key.

The following screenshot shows the file association for .doc added to HKEY_CURRENT_USER>Software>Classes for a Windows 2000 or a Windows 2003 client.

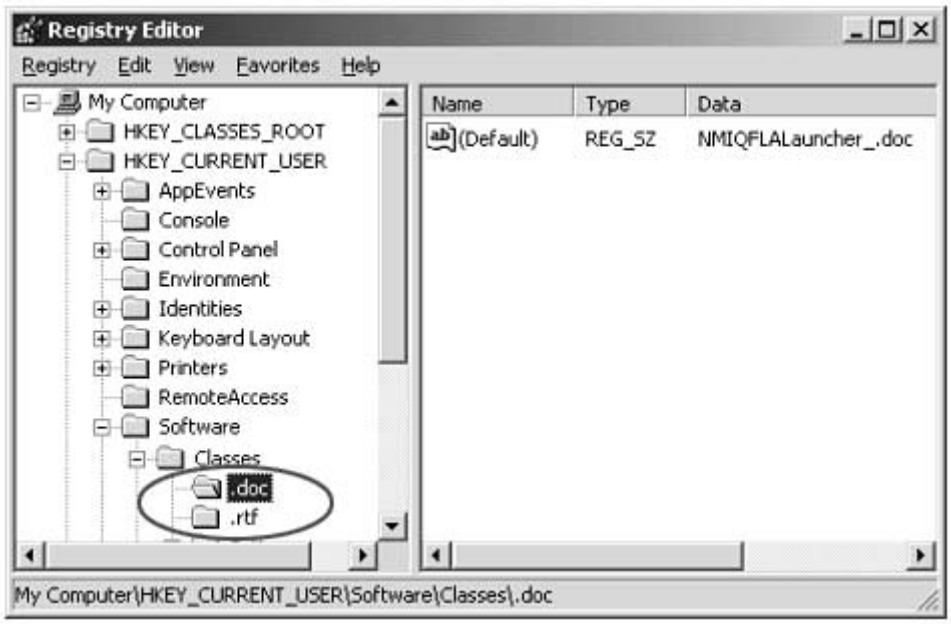


FIGURE 15. Registry Entries for File Associations

Interaction with other features

Client Group interaction

Client Group applications do not create file associations on the client's computer.

Connection Manager on Application Server

There are no issues. You can use file associations in conjunction with a published desktop. In other words, if a desktop is published to users, then with that desktop the users can use file associations.

Security implications

For any application, if the file association does not exist on the server, then the "Open With" dialog will appear and this might pose a security risk in some situations.

Overriding file associations

A local administrator can override the Secure Global Desktop file associations on a computer by reverting to the local file associations by:

- Right-clicking the **Tarantella Connection Manager** in the task bar and selecting **Delete all shortcuts** 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 next to the appropriate application name whose extensions are to be deleted.
- 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.

Launch Pad

The Secure Global Desktop Launch Pad gives users access to their Secure Global Desktop managed applications. Through this Web site, users can launch applications, adjust their Secure Global Desktop settings, and manage their connections. Users can also launch applications using items on their Windows Start Menu, desktop shortcuts, and Secure Global Desktop Connections on their Windows-Based Terminal, but they cannot perform these management functions from these places.

Launch Pad features

From the user's point of view, the Launch Pad is a simple Web site, focused on launching applications. The Launch Pad actually has two pages for launching applications: a Favorites page, which lists the applications a user has selected, and an Applications page, which lists all of the user's applications. The Favorites page is the home page for the site. The users can select the layout of their applications icons on each page.

From the Launch Pad, users can see all the connections that they have made to the Secure Global Desktop system, both from their current computer and other client computers and terminals. The Connections page lists both active and disconnected connections. From this page, the users can disconnect from active connections and reconnect to disconnected connections. The user can also connect to active connections on other client computers without first disconnecting those sessions on the other computers

The Launch Pad is one method for an administrator to distribute the Tarantella Client. When users log on to the site, client-side scripts will detect the presence of the Tarantella Client and prompt them to download the client if they do not have it.

From the Launch Pad, users can choose their favorite applications, start menu applications, desktop shortcuts, and file associations. They can also set the layouts of their favorites and applications pages, specify the reconnect option, and select the connection setting for application launches. Connection settings are collections of connection parameters that are setup by the administrator for the system.

Setting up the Launch Pad

Secure Global Desktop allows administrators to customize the Launch Pad from the **Options>User** page of the Management Console. The Secure Global Desktop administrator can remove end-user features, such as favorites or shortcuts and choose the style of the Launch Pad. The style affects the layout and graphics that appear in the Launch Pad. Secure Global Desktop provides styles that are useful in a stand-alone site or as a frame in another site.

TABLE 8. Secure Global Desktop Application Launch Pad styles

Name	Features	Graphics	Comments
Full	All	Full	Default stand-alone style
No Banner	All	Minimal	Useful for a stand alone style or a frame in another site
Minimal	Application/Logon	None	Useful for a frame in another site

The Secure Global Desktop Administrator sets the Launch Pad style for all members of a team. However, a user can change the appearance of his own or her own Launch Pad in terms of style. To do this, a user adds style=<style number> in the query string and the query string must begin with a question mark (?).

The first example below 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>\Launch Pad\

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

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 full launch style contains a banner.

The Secure Global Desktop administrator can choose to show the team name in the banner on the Launch Pad, customize the Secure Global Desktop team name, and change the support link for the user from the **Options>System>Update Options** page of the Management Console. The Secure Global Desktop administrator can also enable or disable certain features and specify the reconnect options. For more information, refer to "User options".

Client upgrade

To allow the Secure Global Desktop system to use all the features available in later versions, Tarantella Client upgrade from Secure Global Desktop version 2.1 to later versions of Secure Global Desktop is required on the Client computers, where the Secure Global Desktop users

logon. The client uninstalls the v2.1 client and then installs the new client. The computer does not have to be rebooted generally.

When you upgrade your team to later versions of Secure Global Desktop from Secure Global Desktop v2.1, if you have already upgraded to Tarantella Connection Manager v4.0, the Tarantella Connection Manager v2.1 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.

The user needs to be an administrator on the local computer to install the 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.

Forcing a download

An administrator can force an upgrade any time a user logs in by selecting the **Force Client Upgrade** check box in the **Options>User>Update User Options** page on the Console. In this case, every time the user launches the Launch Pad the Download Client page appears, depending on the Server and the Client versions.

NOTE

The user cannot proceed to any other page except the **About** *page on the Launch Pad without downloading the client if the force download is applicable as per Table 2.*

Thus,

- If Tarantella Client is not present on a computer and a user accesses the Launch Pad using the browser, the user is forced to download the Client, irrespective of the administrator's settings and the version of the Server.
- If the version of the Server is later than the version of the Client, the user is forced to download the Client only if the administrator has made this mandatory in the user settings. However, the user can go to the Download page and download the Client.
- If the version of the Server is not later than the version of the Client, the user is not forced to download the Client even if the administrator has made this mandatory in the user settings.

Pushing a client

For a Client upgrade, an administrator generally may want to push the client if:

- After a Server upgrade, there are multiple clients that need an upgrade
- There are multiple logons from such users that do not have administrator rights on Client computers

In such a case, the administrator can push a Client on each computer using a third party tool such as Windows 2000 IntelliMirror. For more information, refer to "Installing the client using an MSI push".

NOTE

We recommend that the administrator push the Client during install in a system account context and not to a user.

Client on a computer

Deploying the client software

There are two methods of deploying the Client software on a Client computer:

- User can download from a Web Server. For more information on downloading a client from a Web Server, refer to the *Secure Global Desktop User Guide*.
- Administrator can push to the Client computers using some third party tools in the system context.

Type of client

On a Client computer, in order to be able to use the Secure Global Desktop Team applications and shortcuts, Client software along with a Launch Pad ID is required for each user. The Client software manages the connections between the Servers and the Client computer and the Launch Pad ID manages the shortcuts and the file associations for a user.

A Client computer may have any one of the following types of Clients:

- Transformed Client
- Nascent Client

Transformed client

A transformed Client has the Launch Pad URL associated with it. This URL is stored in HKEY_LOCAL_MACHINE in the registry. When a Windows user logs on to a computer, the Launch Pad URL is combined with the user name and Launch Pad ID is generated. This Launch Pad ID is stored in HKEY_CURRENT_USER in the registry. The next time this user logs on to this Client computer, this registry entry in HKEY_CURRENT_USER is used to connect to the appropriate Web Server and provide the shortcuts, applications, file associations assigned to this user.

When another user logs on to the same computer, the same Launch Pad URL is combined with this user name and another Launch Pad ID is generated. This Launch Pad ID is also stored in HKEY_CURRENT_USER in the registry. The next time this user logs on to this Client computer, this registry entry in HKEY_CURRENT_USER is used to connect to the appropriate Web Server and provide the shortcuts, applications, file associations assigned to this user.

Thus, a Launch Pad ID is generated for every user, and an entry is created in HKEY_CURRENT_USER for every user. **Moreover, the Launch Pad URL that is used is the same for every user. This is the same URL that the administrator has used to transform the Client software**.

NOTE

A user who logs on to a computer having a transformed client has the shortcuts available after logon as the Launch Pad ID is created at logon.

Nascent client

A Nascent Client does not have a Launch Pad URL associated with it. A user has to logon to the Launch Pad using the Launch Pad URL provided by the administrator in the browser. The Launch Pad URL is combined with the user name and a Launch Pad ID is generated. This Launch Pad ID is stored in HKEY_CURRENT_USER in the registry. The next time this user logs on to this Client computer, this registry entry in HKEY_CURRENT_USER is used to connect to the appropriate Web Server and provide the shortcuts, applications, file associations assigned to this user.

When another user logs on to the same computer, the user can logon to the same Launch Pad URL or another Launch Pad URL provided by the administrator. This Launch Pad URL is combined with this user name and another Launch Pad ID is generated. This Launch Pad ID is also stored in HKEY_CURRENT_USER in the registry. The next time this user logs on to this Client computer, this registry entry in HKEY_CURRENT_USER is used to connect to the appropriate Web Server and provide the shortcuts, applications, file associations assigned to this user.

Thus, a Launch Pad ID is generated for every user, and an entry is created in HKEY_CURRENT_USER for every user. **However, the Launch Pad URL that is used may not be the same for every user**.

NOTE

A user who logs on to a computer having a nascent client has no shortcuts available after logon as the Launch Pad ID is created only after the user logs on to the Launch Pad using the browser.

Shortcuts

The purpose of the Secure Global Desktop shortcuts is to provide access to the Secure Global Desktop system from the client without requiring the user to use the Secure Global Desktop Launch Pad.

The user may have to enter a password when using a shortcut. First, a Secure Global Desktop administrator may specify that all users enter a password when using a shortcut. Second, the Secure Global Desktop administrator may permit users to omit using a password when launching an application using a shortcut. Third, if a Secure Global Desktop administrator permits a user to omit the password, the user still needs to select the check box on the Launch Pad Log On page to activate the option to use no password with shortcuts. Furthermore, although password saving affects shortcuts, it actually operates on all of a user's launch triggers whether they are shortcuts or regular Launch Pad triggers.

NOTE

If there are two or more applications in the Secure Global Desktop system with the same name, then shortcuts are created only for one application.

For a user to be able to run an application via Secure Global Desktop, Secure Global Desktop must install the Tarantella Client on the user's computer. This client software is a 5 MB file package.

The user can obtain the client software in one of two ways, by having the administrator pushed the software to the client device or by downloading the client software from the Launch Pad via a browser.

NOTE

Cookies should be enabled to logon to the Console or the Launch Pad.

What is the Tarantella Client?

The Tarantella Client is an MSI package that contains the following components

- Tarantella Connection Manager
- MS RDP 5.1 ActiveX control

The size of the whole package is approximately 5 MB

Installing the Tarantella Client and shortcuts

This section explains two ways of installing a Tarantella Client along with your personalized set of Secure Global Desktop shortcuts.

Installing the client using an MSI push

An administrator can push the client software to a user's client devices using any standard third party tool that supports .msi, such as Microsoft Intellimirror. Before you push the client install, you need to set the LAUNCH PADURL property in the SGD-TSE-Client400.msi to point to the URL of the appropriate Launch Pad. When you open the .msi this LAUNCH PADURL property may be set to http://shipit/someasppage. Change this to the value that is appropriate for your site. You can do this by editing the SGD-TSE-Client400.msi file or by applying a transform for the MSI (Intellimirror only). To edit the .msi file, you need a special application program. You cannot edit the .msi file using a program such as Notepad, but you can edit it using a program such as Wise for Windows Installer.

To read more about these operations:

- Refer to Windows Installer Service Help to find out more about editing MSI.
- Refer to Intellimirror and Windows Installer Service Help to learn more about applying transforms.
- Refer to your Intellimirror user guide to find out how you can push MSIs.

When a Secure Global Desktop administrator pushes a client install, it is best to push it on a per computer basis instead of a per user basis.

When the user logs into the computer with its corporate credentials, at logon, Secure Global Desktop evaluates the status of the shortcuts, and when necessary, pushes them, dynamically, to a user's Windows Start menu. Secure Global Desktop creates these shortcuts to reflect the applications accessible to this user from the groups or OUs to which the user belongs and through the direct assignment of applications.

When a user wants to update shortcuts for a Client that was set up using a push install, then the user must click **Start>Programs>Startup>Refresh Secure Global Desktop Shortcuts**.

Installing the client using a user-initiated download

A user can initiate a download of the client software to the user's client device using the Secure Global Desktop Launch Pad.

NOTE

The user needs to have local administrative privileges to install the client.

Under normal circumstances, a user goes to the Launch Pad URL using a browser, logs on to Secure Global Desktop using corporate network credentials, and when the Tarantella Client does not exist on the user's computer, Secure Global Desktop takes the user to the **Download Client** page. The user clicks Download Now to initiate the client download and install. The client install queries the user for the install location. At the end of the install, the client automatically contacts the Secure Global Desktop server, Secure Global Desktop populates the user's Windows Start menu with the appropriate Secure Global Desktop applications icons, and the browser page URL points to the Web page that lists this user's applications.

Any user who logs on to Secure Global Desktop from this computer will automatically have the personal shortcuts generated appropriately.

Configuring shortcuts

For administrators

Administrators can permit or deny the creation of shortcuts on the client devices. Administrators can allow certain users to override the system-wide shortcuts settings for their devices.

Location of shortcuts in the Start menu

Secure Global Desktop, by default, creates shortcuts in the program files folder that resides under a user's Windows Start menu. All shortcuts appear in a folder that has a name that reflects the Secure Global Desktop team name.

Location on a per application basis

An administrator can change the system-wide default-location for shortcuts files. An administrator does this on a per application basis, using the application's shortcut-location property. By placing a new value in this property, an administrator can change the location on the Windows Start menu where the Secure Global Desktop shortcuts appear.

For users

Users can launch their applications in one of several ways. They receive a preferred Launch Pad site, and they can choose to launch an application from that site or from the desktop or Start menu shortcuts.

If an administrator permits a user to have shortcuts, the user can decide on a per application basis, where to create application shortcuts. User can choose to create shortcuts on the desktop and or in the Windows Start menu. A user's permissions remain with the user's settings, so a user's shortcuts can appear on any client computers from which that the user connects. Therefore, a user could carry these settings to an internet café.

An Administrator can set one of the following shortcut options for Secure Global Desktop users:

None

This option prohibits the creation of shortcuts on the client computers.

All

This option creates shortcuts for all the applications in the Client, on Windows Start menu only

User choice

This option permits a user to choose specific applications to receive associated shortcuts. Then the user can choose to establish these shortcuts in the Start menu, on the Desktop, or in both locations.

Shortcut refresh

A refresh event deletes the old shortcuts and creates new ones in their place. It is important to understand that Secure Global Desktop updates only those shortcuts that Secure Global Desktop creates. If a user creates a shortcut using a method that is external to Secure Global Desktop then Secure Global Desktop does not update that shortcut. For example, a user could create a shortcut by using a standard Windows shortcut creation method, then the user might want to delete these shortcuts and then recreate them to match the Secure Global Desktop autogenerated shortcuts.

The following shortcut creation methods exist:

A user right-clicks the **Tarantella Connection Manager** on the task bar of the client computer, and then clicks **Refresh shortcuts and file associations**. The shortcuts will refresh if the user has previously logged on to the Secure Global Desktop Application Launch Pad, or if the administrator has placed the Launch Pad address in the SGD-TSE-Client400.msi install file.

A user logs on to a client computer. The logon event triggers a refresh. The shortcuts will refresh if the user has previously logged on to the Secure Global Desktop Application Launch Pad or if the administrator has placed the Launch Pad address in the SGD-TSE-Client400.msi install file.

A user clicks the **refresh application list** link that appears on the **Favorites** or **Applications** page of the Launch Pad to refresh the application list.

The user should refresh the shortcuts after changing the shortcut configuration from the **Launch Pad>Options>Update Options** page.

Security issues

All user-specific information is stored in the HKCU hive in the registry; therefore, other users using the same computer to access Secure Global Desktop applications cannot access another user's applications.

Each user's shortcuts exist on a per-user basis; consequently, shortcuts belonging to one user are not accessible to other users.

Printing

Secure Global Desktop printing

Secure Global Desktop provides multiple printing configuration options. Administrators need to find the best option for their environment based on the information provided.

Configuring Secure Global Desktop

After analyzing the system, the administrator can decide which option best suits the environment.

The following is a list of the printing options that an administrator can choose.

Option 1 - Disable Secure Global Desktop Printer Sharing

Use this option to enable server-side printing only.

We recommend this option if you want all printing to be from printers connected directly to the server or over the server-side network.

To enable this option from the Management Console, from the **Manage>Connection Settings** page, select the Connection Settings you want to update and click **Update Settings**. In the **Client Printer Sharing** area, from the **Windows 2000** and **Windows 2003** lists, select the **Off** option.

Option 2 - Enable Vendor Driver printing

Use this to enable users to print using the vendor driver of the printer.

For this option, the vendor driver must be installed on the server.

We recommend this option for most configurations. Secure Global Desktop Printing offers administrators the ability to select both the vendor driver and the Unidriver. In this way, Secure Global Desktop leverages any additional functionality that might be available with the vendor-specific printer drivers. If the vendor driver is not available, printing will use the UniDriver.

To enable this option from the Management Console, from the **Manage>Connection Settings** page, select the Connection Settings you want to update and click **Update Settings**. In the **Client Printer Sharing** area, from the **Unidriver** list, select the **If vendor driver not available** option.

Be sure to load all client-side drivers on the Application Server.

Option 3 – Enable UniDriver printing

Use this to enable the UniDriver, the proprietary generic printer driver, to print.

The proprietary Unidriver supports full quality printing, including color. By choosing this option, you may lose some functionality of the printer driver. For example, if your printer supports showing you ink levels of your printer, using the unidriver, you will not see that function.

We recommend this option if you do not want to install printer drivers on your server, and are satisfied with the full quality yet less functionality of your printers.

To enable this option from the Management Console, from the **Manage>Connection Settings** page, select the Connection Settings you want to update and click **Update Settings**. In the **Client Printer Sharing** area, from the **Unidriver** list, select the **Always** option.

NOTE

Printing data is always transmitted in encrypted form.

Option 4 - Printer Properties Remoted

You can retrieve the per-user DEVMODE properties and set them on the redirected client printers. A device driver's private data follows the public portion of the DEVMODE structure. Only those properties which are present in DEVMODE's public data can be remoted.

The properties that can be remoted are :

- Orientation
- Paper size
- Paper length
- Paper width
- Factor by which the printed output is to be scaled
- Number of copies to be printed
- Paper source
- Print quality(printer x-resolution)
- Color (monochrome or true color)
- Duplex printing
- Y-resolution of printer

- TrueType fonts option
- Whether collation should be used when printing multiple copies
- Name of the form to use
- Number of pixels per logical inch
- Color resolution
- Whether the NUP is done
- Frequency
- ICM method
- ICM color matching method
- Type of media being printed on
- How dithering is to be done.

How Secure Global Desktop Unidriver printing works

This section explains the Secure Global Desktop printing process.

This section addresses the operational differences between the Secure Global Desktop UniDriver and the Citirx MetaFrame Universal Printer Driver by reviewing the process flow of a print job. The following figure shows this flow.

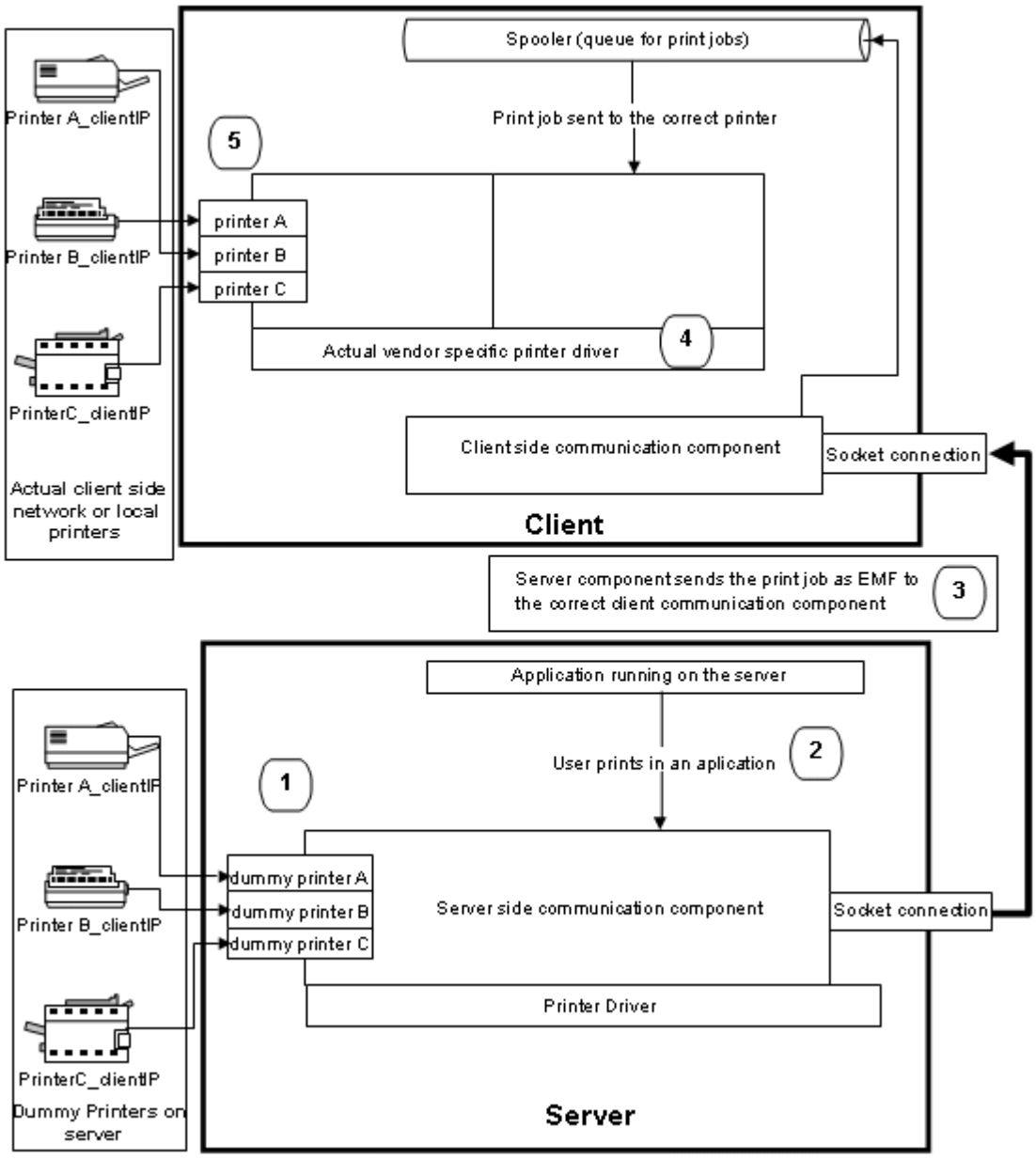


FIGURE 16. Secure Global Desktop Unidriver printer driver job flow

When the client connects to the Application Server, Secure Global Desktop maps all the client printers on the Application Server (network and local). Secure Global Desktop creates printers on the server using Windows Unidriver files. Since these drivers will not be used to process the print job it is not necessary to have the “real” printer driver on the server.

When the client prints via any of the active applications, Secure Global Desktop creates a print job on the server side.

When the print job is rerouted from the server to the client computer, it is routed in the form of an EMF (Enhanced Meta File), using the proprietary IFS (Internet File System) technology of Secure Global Desktop. The EMF format ensures that there is no noticeable loss in quality during the transmission of print files for the majority of cases.

NOTE

IFS and printing data is always transmitted in encrypted form.

When Secure Global Desktop processes the print job on the client side, it uses the actual vendor-supplied printer driver, and Secure Global Desktop converts the job to a format that the printer understands. Since Secure Global Desktop processes the job using the device-specific printer driver on the client, Secure Global Desktop fully supports printing features such as full color and high resolution.

When the print job is then finally sent to the printer, there is minimal loss in quality.

UniDriver printing

This section addresses Unidriver printing, network printing, and support of a default printer.

Secure Global Desktop UniDriver printing

The Secure Global Desktop UniDriver supports all types of printers (from basic, black and white, to high-resolution and high-color laser, PCL3, PCL4, and PostScript printers. The Secure Global Desktop UniDriver enables clients to print to any of their attached printers and to use all of their default printer's functionality. It does this without requiring server-side printer drivers and without compromising the quality of the print job.

Secure Global Desktop can print color output, support all printers that are used on the network, retain a reference to a client's original printer name, and print to a printer that is locally attached to a client's computer. As Secure Global Desktop does this, it eliminates printer driver conflict and improves printing reliability. It does not convert data transmitted from the server to the client to an interim format, because it avoids processes that can cause degraded printing quality.

Secure Global Desktop utilizes the superior Enhanced Meta File (EMF) redirection technology to achieve reliable, high quality, printing performance. The print process proceeds as follows: the client connects to the Application Server and Secure Global Desktop maps all the clients' printers to the Application Server (network and local). These printer drivers can exist on the Application Server along with the Secure Global Desktop UniDriver. However, the printer-specific server-side printer driver is not functioning to print the job, so if the required printer driver is missing on the Application Server host, Secure Global Desktop can still produce high-quality print jobs. It is not necessary to have the "real" printer driver on the server.

The Tarantella Client prints via an active application. Secure Global Desktop creates a print job on the server side, and Secure Global Desktop uses its own proprietary IFS technology to reroute this print job, in the form of an enhanced meta file (EMF), to the client's computer; additionally, the use of EMF ensures that there is no loss in quality during the transmission.

On the client side, a vendor-supplied, device-specific printer driver exists to process the print job, so the print job uses the full functionality of the printer. For example, Secure Global Desktop supports advanced-color and high-resolution printing.

Linking to printers

The Secure Global Desktop administrator should link to the printers that the Secure Global Desktop users will use. The administrator does this by using the Microsoft Printer Add utility (**Start>Settings>Control Panel>Printers>Add Printer**).

The Secure Global Desktop administrator should do this during the initial configuration of Secure Global Desktop and should update this configuration periodically. It is important to update as it can improve application launch speed.

When the Secure Global Desktop administrator does not perform this task, Secure Global Desktop creates transient printer links on a per user basis. This means, when a user launches an application, Secure Global Desktop launches the application and creates a transient link to the user's printer. When another user launches an application, Secure Global Desktop launches the application and creates a transient link to the user's printer (even if the user uses the same printer as the first user). When a user logs off from Secure Global Desktop, the printer link for that user disappears.

When the Secure Global Desktop administrator configures printers for each Application Server using the Microsoft utility, the configuration is static. This means that a specific printer used by a specific user will be available whenever that user wants to use the printer. The user will not have to wait for Secure Global Desktop to create the link, and this speeds the application launch process.

Jobs framework

Jobs framework feature in Secure Global Desktop ensures that jobs submitted by administrators, for example adding a group to an application, are completed without timing out. The system assigns a Job ID to the job and puts it in a queue from where the Jobs Framework picks up the job and completes it. The Job Framework feature displays a "Job in Progress" page, which checks in short intervals if the job is complete. Meanwhile, the administrator can go to any other page and carry on with the administrative tasks.

An administrator can monitor the jobs submitted to the system by all administrators. Additionally, the administrator can view the details of any job.

File handling

In the server-based computing world, all applications execute on central servers and not on user desktop. In an ideal world scenario, the users will save all their files on the servers too, which is not the case today. Users also need to access and save some of their files on their local hard drives. Secure Global Desktop adds this functionality to the RDP protocol. Secure Global Desktop permits users to save and access information from their local hard drives as well as their network drives mapped to their local PC.

Configuration

To map the client's drives on the server, there must be unique driver letter for each client drive. For instance if drive A, B, C are being used by the server operation system as server's floppy and hard drives then there must be a range of drive letters that must be set aside for client drive maps. Secure Global Desktop, by default, reserves drives I through Q on the server for the client-side drive mappings. These drive letters must not be used by the server. For smooth functioning, the administrator needs to ensure the following:

- The server is not using drive letters reserved for the client's drives, on the server.
- Drive letters reserved on the server are sufficient to map all client drives.

The administrator can change the letters to be used for client drive mapping from the **Options>System** page. The Secure Global Desktop Monitor service should be restarted for any change in the drive letter mapping to be effective.

You can turn off client drive sharing by specifying the first and last letter for drive sharing such that the last letter specified comes before the first letter specified in the alphabetical order. For example, you can specify the first letter as "Q" and the last letter as "M". In this case, none of the client drives will be available to the user in Secure Global Desktop.

Drive letter confusion on the client side

Because the client's drive letters change when using a server-side application, the administrator needs to explain this anomaly. It is possible for administrators to enable end users to retain their original drive letters by changing the drive letters on the server; for example, if the drives on the server are A, B, and C, the administrator can re-map these drives to U, V, and W. Then the administrator can reserve A, B, C to F, for the client drive mapping. You must re-map the drives before installing Secure Global Desktop or any other application software on the servers. There are numerous third-party tools available to do this job.

Security concern

Secure Global Desktop implements a SMB (Server Message Block) server on the client. This server allows secure access to client-side drives, within Secure Global Desktop applications, without exposing client drives to the whole network.

For certain secure environments, drive mapping may be a security concern. Administrators may want to prevent users from accessing local drives in Secure Global Desktop applications. Secure Global Desktop provides a global switch for turning off local drive access. To disable this option from the Management Console, from the **Manage>Connection Settings** page, select the Connection Settings you want to update and click **Update Settings**. In the **Client Drive Sharing** area, from the **Windows 2000** and **Windows 2003** lists, select the **Off** option.

System heartbeats

The system heartbeats and time-outs topic describes the heartbeat variables.

Heartbeat variables

Application attribute changes

If an administrator changes the properties of an application, such as the working directory path for the application, Secure Global Desktop instantaneously reflects the change, notifying all Application Servers that hold a copy of the amended application of the change. Next, the Application Servers register themselves with the Load Balancer. The Load Balancer queries the database gets the latest information and sends it to the Application Server. This process is roughly instantaneous, discounting any peripheral network-throughput issues.

Server-side application assignments to changes

If an administrator adds or deletes applications from Application Servers, Secure Global Desktop reacts by updating the Secure Global Desktop database and notifying the affected Application Server to refresh itself. This process is roughly instantaneous, discounting any peripheral network-throughput issues.

User-related application assignment change

Changes made to server-side application assignments affect users differently depending on their logon status.

If users are not using the Secure Global Desktop Applications Launch Pad then they receive the latest set of applications when they log on or when they refresh their shortcuts.

If users are using the Secure Global Desktop Applications Launch Pad then they need to perform an action, they must either refresh their browser to get a new set of applications or logon to Secure Global Desktop again.

Configuration changes

If an administrator changes the system's configuration, by altering one of the properties using the Management Console under the Options tab, the changes appear throughout Secure Global Desktop instantaneously. The Application Server's cache holds configuration information; therefore, in response to a configuration change, Secure Global Desktop, using the Secure Global Desktop Engine that runs on the Application Servers, forces each Application Server to refresh its cache. Incidentally, all components on an Application Server obtain configuration information from the Application Server's cache.

New role addition

If an administrator changes role assignments for a server on a Secure Global Desktop team, Secure Global Desktop reacts by marking these changes in the database and forcing the Secure Global Desktop Engine on the affected server to refresh itself. During this refresh, the server learns that it has a new role, and it takes appropriate actions to update itself. Secure Global Desktop reacts based on the conditions of the affected server. If either the Secure Global Desktop Engine or the server itself is down, then the refresh occurs when the server powers up. If the server is idle, the server automatically looks for changes, about every ten minutes, and it refreshes itself. This refresh process does not consume many resources.

Console monitor page

The monitor page in the Management Console refreshes itself every five seconds. This refresh updates the console with load balancer, database connections, relay server, jobs, and connection information. The administrator can change the page refresh interval from the **Options>Administrator page**. For more information, refer to "Administrator options".

Application Server load measurement

The Application Server reports its health (based on variables such as memory, CPU, and queue length) once every minute to the system. Secure Global Desktop samples five readings per minute, averages these five readings, and reports the averaged values to the system.

Application Server crash check

If the Load Balancer does not hear from the Application Server through three continuous refresh cycles (sixty seconds per cycle), the Load Balancer assumes that the Application Server is offline. Thus, if an Application Server becomes unavailable without notifying the system, Secure Global Desktop detects the condition anyway within three minutes.

The server crash check also operates to free application licenses that might otherwise be stuck with a failed session. This is how this works. If a user launches an application session, the Secure Global Desktop load balancer decrements that application's licenses-available count by one. Once the session starts on an Application Server, the Load Balancer knows that the session has started and Secure Global Desktop show a "launching" state in the Management Console, under the Monitor tab, and the connection's status. Once the sessions starts on the client, the Application Server the Load Balancer knows that the session has started.

Secure Global Desktop watches for the session to launch the application, and if the application session does not launch, after five minutes then Secure Global Desktop times out the application

session. This time-out must be of a sufficient duration to allow users to download a client, to obtain their profiles, and to launch their applications. After this amount of time, frequently five minutes, Secure Global Desktop increments that application's license-available count.

Diagnostics

Secure Global Desktop is a system that can use many computers and many configuration variables. Diagnostics helps you detect problems with the Secure Global Desktop servers' configuration or setup.

After selecting the servers to diagnose and the diagnostic tests to carry out, when the diagnose button is hit on the Management Console by the administrator then the servers selected asked to diagnose the roles on them. All the roles on the server get the diagnostic request, they are the ones who actually do the tests, and they report problems back to Secure Global Desktop and Secure Global Desktop displays this status information to the Secure Global Desktop administrator.

The architecture of the diagnostic flow appears in the following figure.

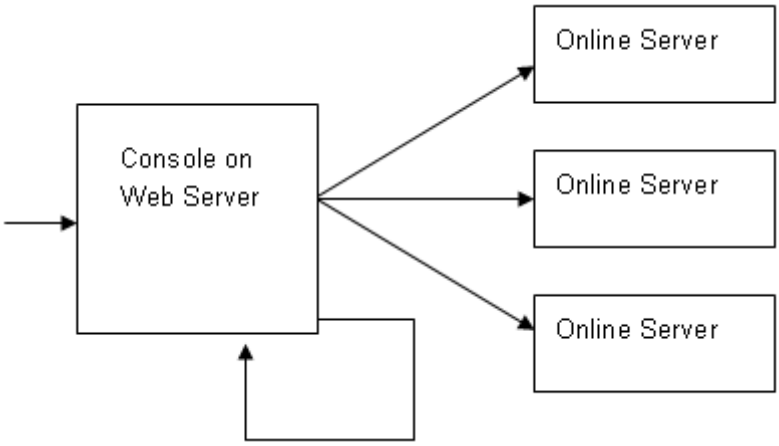


FIGURE 17. Flow of diagnostics

These are the Secure Global Desktop diagnostic tests and the table that follows explains each.

- Application Path test
- Printer Driver Path Test
- Services Status Test
- Settings Test

TABLE 9. Diagnostic tests

Diagnostic tests	Test Description
Application Path Test	This test checks the executable paths for the applications assigned to the Application Servers and reports if any application path is incorrect.
Printer Driver Path Test	This test checks the printer driver paths for each Application Server to verify that the printer driver paths actually exist on the server.

TABLE 9. Diagnostic tests

Diagnostic tests	Test Description
Services Status Test	This test checks the status of the required services on the Servers and reports if a service is missing or stopped.
Settings Test*	This test checks whether the Servers have the proper settings required for the Secure Global Desktop roles. The various settings that this process checks for the roles are: Web server role: Here Secure Global Desktop checks to see that the required virtual directories exist on the IIS server and if they do, it checks to see that the required properties are set correctly. Load balancer role: If the Load Balancer is the Master Load Balancer then here Secure Global Desktop checks to see that all of the online Application Servers have registered with it. If the Load Balancer is not the master then Secure Global Desktop checks to ensure that no Application Servers have registered with it. Application server role: Here Secure Global Desktop checks the Terminal Services settings to ensure that they are properly set, and it reports any problem detected. Relay server role: Here Secure Global Desktop checks if port is available and if the Relay server was able to grab it. It also checks if the Single Port Relay was able to load certificate correctly.

* If you receive a Settings Test failure, see "Settings Test failure" in this document.

The following table lists some of the messages displayed after running the diagnostic tests, along with the cause and remedy for each message.

TABLE 10. Diagnostic test error messages

Description	Cause	Remedy
The application was not found.	Application Path specified is incorrect.	Update the application path from the **Manage>Applications>Update Application** page. For more information, refer to "Update application properties".
Service not running.	Any one of the role Services is not running.	Select **Start>Programs>Administrative Tools>Services** and start the service.
The printer driver file was not found.	Printer File Path specified is incorrect.	Update the printer file path from the **Manage>Servers>Update Server** page. For more information, refer to "Update server profile".
Tarantella Client is unable to set the user settings correctly.	The Terminal Services connection is not configured to use the connection settings from user settings in the Terminal Services Extension to Local Users and Groups and Active Directory Users and Computers.	Follow the procedure in "Settings Test failure" to configure the Terminal Services connection correctly.
Secure Global Desktop is unable to set the idle timeout.	The Terminal Services connection is set to override the default user settings in the Terminal Services Extension to Local Users and Groups and Active Directory Users and Computers. This does not allow you to configure time-out settings for the connection.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Sessions** tab and then under the Connection area, clear the **Override user settings** check box. 4. Click **OK** to save your settings.

TABLE 10. Diagnostic test error messages

Description	Cause	Remedy
Secure Global Desktop is unable to set the disconnect timeout.	The Terminal Services connection is set to override the default user settings in the Terminal Services Extension to Local Users and Groups and Active Directory Users and Computers. This does not allow you to configure time-out settings for the connection.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Sessions** tab and clear the **Override user settings** check box. 4. Click **OK** to save your settings.
Secure Global Desktop is unable to remote control user sessions.	The Terminal Services connection is configured to disallow remote control of a user's session.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Remote Control** tab, and choose the **Use remote control with default user settings** option, or select the **Use remote control with the following settings** option, and then choose the appropriate options. 4. Click **OK** to save your settings.
Automatic logon needs to be allowed.	The Terminal Services connection is configured to prompt for password.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Logon Settings** tab, and clear the **Always prompt for password** check box. 4. Click **OK** to save your settings.
Secure Global Desktop is unable to launch the application requested by user.	The Terminal Services connection environment is not configured correctly.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Environment** tab, and clear the **Override settings from user profile and Client Connection Manager wizard** check box. 4. Click **OK** to save your settings.
Secure Global Desktop is unable to manage the number of connections to this terminal server based on load balancing information.	The maximum number of connections is not configured correctly for the terminal server.	1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**. 2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu. 3. Click the **Network Adapter** tab, and choose the **Unlimited connections** option, or choose the **Maximum connections** option and specify the number of maximum connections. 4. Click **OK** to save your settings.

TABLE 10. Diagnostic test error messages

Description	Cause	Remedy
Service not found	One of the services is not registered.	On the command prompt go to the directory where the service is installed. Type `LoadMgrService.exe -service` and press **Enter**.
The Read permissions are not set for the Console virtual directory (Console, Launch Pad, Depot)	IIS is not configured with read permission.	1. Click **Start>Settings>Control Panel>Administrative Tools>Internet Services Manager**. 2. Right click **Console** (or **Launch Pad** or **Depot**) and select **Properties** from the shortcut menu. 3. Click the **Virtual Directory** tab, and select the **Read** check box. 4. Click **OK** to save your settings.
The Enable Default Documents property is not set for the Console virtual directory (Console, Launch Pad, Depot)	IIS is not configured with the correct settings for documents.	1. Click **Start>Settings>Control Panel>Administrative Tools>Internet Services Manager**. 2. Right click **Console** (or **Launch Pad** or **Depot**) and select **Properties** from the shortcut menu. 3. Click the **Documents** tab, and select the **Enable Default Document** check box. 4. Click **OK** to save your settings.

Reporting

Secure Global Desktop provides many powerful system-status and management-information reports that are dynamically updated in real time. These reports are available from the Management Console. Additionally, Secure Global Desktop provides data manipulation features to support data sorting, to summarize data by properties, or to filter data object type or processing time. It also provides administrators with a simple way to download the Secure Global Desktop data, so the data can be input to other management information systems. These reports help administrators observe resource usage and project future resource requirements.

NOTE

If a report has a very large size, the download may time-out and an error may be displayed.

Secure Global Desktop creates session data reports and audit data reports.

Sessions data

When users launch applications through Secure Global Desktop, Secure Global Desktop monitors and stores information about each session. Secure Global Desktop stores information about both currently running and completed sessions.

Audit log data

When an administrator changes system data (by adding, changing, or deleting an object such as a user, an application, or a server) or when an administrator changes object options, Secure Global Desktop records the change in the Secure Global Desktop Audit Log.

Elements

Secure Global Desktop monitors and reports on these elements, many of which are domain objects:

Sessions

With this report, the administrator can view the currently active and completed sessions to see who launches sessions, the time and duration of sessions, and a session's exit status. The administrator has the option to truncate or to copy and truncate some or all of the session logs.

Applications

With this report, an administrator can view who uses an application from which client, to see the maximum current application license use for a designated period, and to determine if the site has too many or too few licenses. Additionally, the sessions report shows requestor and server information such as who requests applications from which client computers and which servers fulfill these requests.

Users

With this report, an administrator can see who launches sessions, number of sessions launched, and the aggregate duration of the sessions' use during the specified time. This report helps an administrator understand how heavily each user uses Secure Global Desktop for a given period and to ascertain whether demand is increasing or decreasing by providing data from different periods.

Clients

With this report, an administrator can see the client computer that launches sessions, number of sessions launched, and the aggregate duration of the sessions' use during the specified time. This report helps an administrator understand how heavily each client computer uses Secure Global Desktop for a given period and to ascertain whether demand is increasing or decreasing by providing data from different periods.

Servers

With this report, an administrator can see the Application Server that hosts sessions, number of sessions launched, and the aggregate duration of the sessions' use during the specified time. This report helps an administrator understand how heavily each client computer uses Secure Global Desktop for a given period and to ascertain whether demand is increasing or decreasing by providing data from different periods.

Audit log

With this report, the administrator can view changes made to the Secure Global Desktop database. The administrator can view who made which changes to what instances of which object, and when they made a change. This report encourages accountability for changes (adds, updates, or deletes) made to objects (user groups or organizational units, client computers, server computers, or applications). The administrator has the option to truncate or to copy and truncate some or all audit log.

Product keys

With this report, the administrator can see the number of Secure Global Desktop seats owned, which indicates the number of users who can use Secure Global Desktop concurrently; the maximum concurrent usage for a given period; and the number of times this maximum use occurred over the specified period. An administrator can determine, at a single glance, whether the Secure Global Desktop licensing is adequate or nearing its limit. If it is nearing its limit, an administrator can upgrade the Secure Global Desktop licensing agreement.

NOTE

The setting made by the administrator to purge the Secure Global Desktop logs under **System>Options** *affects the Peak Concurrent Usage report. For example, if the administrator sets purging for logs older than 30 days, and sets the find filter for the Peak Concurrent Usage to Last 90 Days, the report displays the result only for last 30 days. This is because all the logs older then 30 days are purged.*

Reports for business solutions

Over time, Secure Global Desktop gathers a lot of useful information about the behavior of the end users with respect to application usage. The following table shows some business problems that Secure Global Desktop addresses.

TABLE 11. Business problems and useful Secure Global Desktop reports

Business Problem	Related Secure Global Desktop Report
To learn about the activity on a particular server	Sessions
To learn about the usage of the Secure Global Desktop product license keys	Product Keys
To monitor application software license compliance	Applications The different kinds of licensing that can be monitored by the reports are: • Application Summary by Users – unique users licensing • Application Summary by Sessions – concurrent usage licensing • Application Summary by Clients – client access licensing
To monitor changes made to the Secure Global Desktop System	Audit Log

Active session management

An administrator can manage the active sessions by shadowing, disconnecting, reconnecting, or -off the sessions.

Session shadowing

The Session Shadowing feature permits Secure Global Desktop administrators to view and control, from the Management Console, a Secure Global Desktop session that is running on a user's desktop.

Administrators and qualified technical-support representatives use this type of session shadowing for user training and for trouble shooting. This feature can provide enormous cost-savings by reducing the need for system administrators and technical representatives to visit a user's site to resolve an application problem.

An administrator or support representative can activate shadowing, a session-level tool, for any *active* session (a disconnected session cannot be shadowed). To shadow a session, a Secure Global Desktop administrator or support representative selects the session to be shadowed from

the **Monitor>Connections** page, and clicks the **Shadow** action. This action generates a request to shadow the session to the owner of a session. The owner of the session may grant or disallow permission to shadow the session.

When an administrator monitors a session, both the administrator and the session owner can control input to and save output from the session. However, either can save the work from the session only on those drives that are available to the owner of the session.

Considerations

- A session cannot be shadowed more than once at the same time. If more than one administrator would like to view the same user session, one administrator must log off from the shadowing session to permit the next administrator to log on and shadow that same session.
- To close a shadowing session from the Console, the Secure Global Desktop Administrator should type the following keys together:

  <Ctrl> <*>

  where the * is taken from the numeric keypad.

  Do not use the * that is created from <Shift> <8> on the alphabetic/numeric area of the keyboard.

Session disconnect and reconnect

The Session Disconnect and Reconnect features permit the administrator or a user to detach a session from a user's computer temporarily. The user can later reattach to the disconnected Secure Global Desktop session.

The session disconnect option terminates a session on a user's computer, but maintains the session on the server. Whereas, a session *log off* terminates a session on both the user's computer and the Application Server.

The administrator can disconnect a session from the console. Additionally, a user can disconnect a session from the Tarantella Connection Manager or the Launch Pad.

Only a user can initiate a session reconnect. The user can do this from either the original user computer (the computer from which the user triggered the disconnect event) or from a different computer (maybe from a home computer). The user can resume work on the affected files at the point in the files where the disconnect event was triggered.

When a user logs on to Secure Global Desktop and launches an application that was a component of a disconnected session, Secure Global Desktop highlights all of that user's sessions that have a disconnected status. The user can select and launch a disconnected session, which will trigger the launch of all applications that were components of that session.

Users can also connect to their active sessions on other client computers. They need not first disconnect from one client and then go to the other client. This is useful, for example, if a user leaves a session running in the office, but forgets to save, and then wants to continue with the same session at home so that there is no loss of work.

When a network failure occurs, Secure Global Desktop attempts to *save* the session data, so a user can later continue work on a project at the point in the project where the error occurred.

Considerations

For a session disconnect/reconnect to operate, a Secure Global Desktop administrator must first permit session disconnects.

To enable the disconnect connections property, a Secure Global Desktop administrator the administrator selects the profile to be changed from the **Manage>Connection Settings** page of the console, clicks **Update Setting**, and selects the **Reconnect** check box.

Once the reconnect option is set, the user has the option to consider session disconnect and reconnect actions. The following items are true if the **Reconnect** check box is selected.

If there is a failure (a power outage on the client computer, a network-generated failure, or a Terminal Server failure), Secure Global Desktop automatically triggers a session disconnect.

- If the Reconnect option is enabled, the session disconnect executes, and data from all applications running under that session is saved.
- If the Reconnect option is not enabled, the session disconnect fails, a session log off occurs, and data from all the applications running under that session is not saved.

  If a user saves the files at some point prior to the failure, the user can later launch the affected files and see that data as it was during the last save. The data entered between the last file save and failure event is lost.

Procedures

A user uses the Launch Pad to view all active sessions and to disconnect from one or more sessions. Additionally, the user uses the Launch pad to reconnect to a disconnected session or connect to an active session on another client computer without first disconnecting the session from the other computer.

An Administrator uses the Console:

- To view all disconnected sessions from the **Monitor>Connections** page, by sorting active sessions on the Session State column.
- To disconnect a user’s session from the **Monitor>Connections** page, by using the Disconnect function.
- To control the duration between a session’s disconnect event and a subsequent automatic session log off event.
- To enable or disable the session disconnect/reconnect option.

Configuration

The session disconnect/reconnect option is available only when an administrator enables this feature. Some administrators may want to disable this feature.

Session log off

The Session Log Off feature permits the administrator to terminate a session that is running on a user's computer in an active or a session that is in a disconnected state. The administrator may need to log off sessions in extreme circumstances; for example, a server may be failing or a disk may appear corrupt and the administrator may want to remove the session from the server immediately.

The session log off option terminates the session on both the user's computer and on the Application Server. This action forcibly kills and permanently terminates the session. Consequently, it is a good idea to send a message to the owner of the session in question before executing a logoff event. To send a message to the owner of the session, use the **Send Message** action on the **Manage>Connection Settings** page.

Secure Global Desktop can initiate a session log-off event programmatically in conjunction with an inactivity timer, an administrator can initiate a log off from a Management Console, or a user can initiate a log off from the Tarantella Connection Manager or the Launch Pad. The Session report lists all logged off sessions along with a logoff event trigger (normal, forced, or time-out).

Procedures

An Administrator uses the Console:

- To view the event that triggered a session's logoff, from the **Report>Sessions** page, select the time duration and sort the sessions on the **Application Exit Status** column.
- To force a log off from the console, from the **Monitor>Connections** page, select the session to terminate, and click **Log Off**.
- To control the duration between a sessions' disconnect event and a subsequent automatic log off event, from the **Manage>Connection Settings** page, select the Connection setting target, and click **Update Settings**. Change the **Logoff Disconnected Connections** option under the Secure Global Desktop Features area, and click **Update**.
- To send a message to one or more active sessions, from the **Monitor>Connections** page, select the logon names that are the target of the message and click **Send Message**.

Configuration

The only configurable variable is the idle time-out parameter, which relates to the duration of inactivity between the client computer and a server. This is duration between the then current time and the prior last keyboard input or mouse click. This time-out parameter acts at the session level; however, it is set at the launch settings level, so all users (and their sessions) running under a specific Launch Settings profile are affected by the value of the idle time out setting. A Secure Global Desktop administrator who uses the Console sets this variable.

Achieving database redundancy

Secure Global Desktop provides a method for a fail-over Database Server so that application launches do not fail even if the Primary Database Server is offline.

An administrator can achieve database redundancy in the following ways:

- Use SQL tools to create a database cluster or use a redundancy mechanism
- Use Secure Global Desktop database redundancy feature

Secure Global Desktop allows the administrator to specify a Backup Database Server in addition to the Primary Database Server. After the administrator adds a backup database, the Secure Global Desktop system adds to the Console the interface to promote, remove, and synchronize the backup database.

The system automatically synchronizes the Backup Database Server periodically with the Primary Database Server. The administrator can specify the time interval for this synchronization. The Load Balancer decides which Web Server does the synchronization. The system requirements for the Backup Database Server are the same as those for the Primary Database Server.

The administrator can promote a Backup Database Server to make it a Primary Database Server. Additionally, the administrator can remove a Backup Database Server. The administrator can also view the status of the Database Server Connections.

Adding backup Database Server

An administrator can add a second Database Server to act as a backup in case the Primary Database Server goes offline. This server is called a Backup Database Server. When the Backup Database Server is added, the system:

- Creates the database
- Copies all the system, log, and session information from the database on the Primary to the Backup Database Server

In order to add a Backup Database Server, the administrator needs to:

- Specify the name of a Database Server and the synchronization interval.

- Specify the required user credentials. The account should have sufficient rights on the Database Server to create database.

NOTE

Incomplete jobs are not copied to the Backup Database as it is read-only and administrative changes cannot be updated to the Backup Database.

Uses of the Database redundancy feature

This section explains some of the ways for the administrator to use the database redundancy feature.

Primary Database Server fails or goes offline

When the Primary Database Server fails or goes offline, the system becomes read-only and application launches take place using the Backup Database Server. The administrator cannot make any updates to the system.

The Backup database contains information synchronized during the last synchronization. Changes made in the Primary database after the last synchronization will not be there in Backup database.

Existing users can launch applications from the existing client computers. However, a user who has never logged on to the Launch Pad will not be able to logon while the Secure Global Desktop team is running on the backup database. Additionally, any computer that never been used to logon to the Launch Pad cannot be used to logon to the Launch Pad while running on the backup database. Users cannot change their system option settings.

The administrator can do the following:

- Logon to Console/Launch Pad and navigate all tabs
- Diagnose servers
- All actions under Connections tab
- Monitor Load Balancer status
- Monitor database connections
- Monitor the Relay Server
- Review jobs history

NOTE

Only completed and failed jobs are copied to the backup database, so a job in started or submitted state is not displayed.

- Generate and download all types of reports.
- Promote backup database.

NOTE

It takes about two minutes to switch launches from the Primary Database Server to the Backup Database Server when the Primary Database Server fails or goes offline. All launches attempted in the switching period fail.

Promoting the Backup Database Server

When the Primary Database Server fails or goes offline, the administrator should do the following:

- Promote the Backup Database Server to make it the Primary Database Server. For more information, refer to "Promote Backup DB".

> **NOTE**
>
> *Since the Backup Database Server is synchronized periodically, it is possible that the backup database is not synchronized with the Primary Database Server when the Primary Database Server goes down. We recommend that if the Primary Database Server is online, the administrator should synchronize the Backup Database Server with the Primary Database Server before promoting the Backup Database Server.*

  While promoting the Backup Database Server, the administrator should ensure that all the servers in the system are online and can talk to the Backup Database Server. The administrator can verify this from the **Monitoring>Database Connections** page.
- Create a new Backup Database Server. For more information, refer to"Add Backup DB".

If the master Load Balancer goes offline when promoting the Backup Database Sever, no other Load Balancer takes over as master Load Balancer until promotion is over.

The administrator can decide not to promote the Backup Database Server and restore the Primary Database Server with some other mechanism, or correct a hardware problem on Primary Database Server and bring that back online. In this case, all the information the system writes to the log archive table while the Primary Database Server is offline is lost.

Using Secure Global Desktop Resource Kit to assign Database Server

If a server is offline when the administrator promotes a Backup Database Server, the administrator should wait for the server to come online, and then use the Secure Global Desktop Resource Kit to assign the new Primary Database Server, that is the promoted Backup Server to the server that has come online. For more information, refer to *"*Migrating to a new Secure Global Desktop Database server"*.*

Taking the Primary Database Server offline for maintenance

The administrator needs to do the following:

- Manually synchronize the Backup Database Server with the Primary Database Server.
- Take down the Primary Database Server, and do the maintenance. The system runs on the Backup Database Server in the read-only mode in this time.
- Bring up the Primary Database Server. All the information written in the log archive table while the Primary Database Server is taken off for maintenance is lost.

Moving the Primary Database Server to another server

To move the data from the Primary Database Server ‘A’ to another Database Server ‘C’, the administrator should:

- Create a Backup Database Server ‘C’.
- Promote ‘C’ to make it the Primary Database Server.

Synchronization of the Backup Database Server

The system synchronizes the Backup Database Server with the Primary Database Server in two ways:

Full copy of the database

Using the same database, the system recreates the tables and copies all the data again to the Backup Database Server. It is like recreating a new backup database minus “create database”. The administrator can set the synchronization interval from the Console. For more information, refer to "Change Sync Interval".

In addition to the automatic full copy of the database that occurs at the interval, the administrator can manually synchronize the backup database from the console. For more information, refer to "Synchronize DB".

Advantages of full synchronization are:

- Any failed 10-minute synchronizations are now reset.
- It resets the database.

Disadvantages of full synchronization are:

- It causes overhead on the Web Server.
- It increases the Network traffic.

We recommend full synchronization when:

- 10-minute synchronizations are failing.
- Log archive table information is to be synchronized.
- Administrator wants to take down the Primary Database Server for maintenance.

Incremental synchronization of the database

Every ten minutes, the system copies the incremental audit log operations to the backup database. All the essential Secure Global Desktop functioning data is copied from the primary database to the backup database.

The interval for this incremental synchronization is set in the registry of each Load Balancer server. We recommend that you do not edit the registry. Contact Tarantella support if you want to change the incremental synchronization interval.

Every 10 minutes, the Master Load Balancer finds the best Web Server that can connect to both the databases to perform this synchronization. The Web Server does the synchronization.

Seamless windows

The seamless windows feature integrates locally and remotely running application into a local Windows desktop removing the WTS shell. This allows a user to view a remotely hosted session without viewing the desktop frame from the server session that hosts the application.

The seamless windows feature provides a cleaner-looking, less-confusing interface and it enables a remotely launched application to mirror the look and feel of a locally launched application. Secure Global Desktop places a task bar button on the task bar for each top-level window in that Secure Global Desktop session.

To produce a seamless window on a user’s desktop, Secure Global Desktop removes the background of the remote desktop and adds a corresponding dummy task bar button to allow a user to minimize and then maximize an application. The dummy task bar button activity then synchronizes with the actual server-side window.

Launch setting configuration

Every Launch Pad portal, high-speed to low bandwidth, has at least one associated launch setting profile that supports the device and its configuration characteristics. Seamless windows is one of the parameters of the launch setting profile, so all applications launched under a specific Launch Settings profile will have the same seamless windows behavior.

Seamless window options

The administrator can set the value for the **Seamless Windows** option on the Secure Global Desktop Features area from the **Manage>Connection Settings** page by selecting the relevant Connection Settings and clicking **Update Setting**. The valid values are **Always**, **Never**, and **Except During Logon**.

The following text explains why many people select the **Except During Logon** option.

When the administrator permits users to use automatic logon and users are also using seamless windows, it generally works. In most cases, a user can successfully log on to the Terminal Server Computer (Application Server) without the user entering the password and username.

However, in some instances, the computer may prompt for some user response and the prompt may not be visible to the user. This might happen when the user's password expires or when some network-security-authentication message box pops up.

To negotiate these exception events, it is best to select the **Except During Logon** option for the Connection setting.

- If the Seamless Windows setting is set to **Always**, the prompt will not be visible on the client computer but some message box will be waiting for some user input. So the session may effectively appear like hung.
- If the Seamless Windows setting is set to **Except During Logon**, the prompt will be visible. Therefore, it is always advisable to set the Seamless Windows setting to Except During Logon. This setting permits the Window session to launch in one mode and to run in another mode. The session launches in a non-seamless window, and the user sees the Windows Logon Dialog box and any subsequent message boxes. Once the authentication completes and the session switches complete, the session runs in a seamless mode.

Procedures

An administrator uses the Application Management Console, **Manage>Connection Settings>Update Settings** page to affect Seamless Windows in the following ways:

- To enable or disable seamless windows mode for the relevant platform's launch profile.
- To enable select seamless window Always or Except During Logon.

This parameter affects all applications that use a particular launch setting.

Security

Server-based computing has many potential security benefits. Servers can be placed in a datacenter where administrators can safeguard them. If a user is using a thin-client computer, data will be stored in the datacenter, so the datacenter can protect that data, and software can audit, monitor, and control application access. Industries, such as health care and finance, are adopting server-based computing for these reasons.

Design principles and practices

The design of Secure Global Desktop reflects the following principles and practices.

Unsecured external components

Secure Global Desktop assumes the network that connects all of its servers is unsecured; therefore, it takes measures to protect Secure Global Desktop data, communication, and components on all of its servers, not just those exposed to clients. IFS and Secure Global Desktop printing data is always transmitted in encrypted form.

Redundant measures

Every Secure Global Desktop component, not just those dealing with clients or networks, has security measures. If one component were compromised, then the other components will prevent the system from becoming compromised. In this manner, the total damage to the system could be isolated if an attack were successful.

Least privilege

On Windows servers, every component runs under a security context with set of privileges. Privileges give the component permission to perform certain operations such as access a file or set a registry entry. Components that run with fewer privileges are safer, because if they were compromised, they would do less damage. The Secure Global Desktop designers made sure that every Secure Global Desktop component runs with the smallest set of privileges possible. All COM+ components run with privileges for a normal user. Secure Global Desktop services run under SYSTEM account.

Proven code

Rather than invent its own encryption algorithms and security techniques, Secure Global Desktop relies on proven security libraries. Code that as been heavily scrutinized and found to be secure is better than the code that has not been so challenged. In particular, Secure Global Desktop relies heavily on the Window's cryptography, authentication, and access control mechanisms for it security design.

Secure defaults

Secure Global Desktop ensures that every default setting of the system is the most secure setting for the system. The only exceptions to this principle are settings that might not run on most systems. A corollary to this principle is to warn the administrator when the administrator chooses settings that are not secure.

Features and security

Many features have security aspects to them. This section reviews the features with security considerations.

Logon

To perform any operation in Secure Global Desktop, an end-user or administrator must authenticate with Secure Global Desktop using their domain user name. Since the Management Console and Launch Pad portal are web applications, they use web authentication methods. Secure Global Desktop supports all the authentication mechanisms found on the Windows Internet Information Server (IIS). The table below summarizes the advantages and disadvantages of each.

TABLE 12. Web authentication methods

Type	Automatic Logon	SSL Required	Internet Explorer Required	Firewall Compatible	Special Setup
Anonymous	Yes, with cookies	Recommended	No	Yes	None
Basic	No	Yes	No	Yes	None

TABLE 12. Web authentication methods

Type	Automatic Logon	SSL Required	Internet Explorer Required	Firewall Compatible	Special Setup
Windows Integrated	Yes	No	Yes	No	None
Certificate	Yes	Yes	No	Yes	Yes

The administrators can choose the authentication that best suits their environment. They change their IIS authentication method directly using the IIS administration consoles. Secure Global Desktop dynamically detects the authentication method set up by an administrator.

By default, IIS uses anonymous authentication. With anonymous authentication, Secure Global Desktop will display a form in their web browser to query the user's name and password. To keep these credentials secure, we recommend that administrators configure their servers to have SSL available, so that the browser transmits these credentials to the Web Server in an encrypted form. The Management Console has an "SSL Available" setting to configure Secure Global Desktop to switch to SSL automatically for logon.

Certificates and Smart Cards

Many vendors provide Public Key Infrastructures that distribute certificates to users. Setting up a PKI system can be difficult. Administrators are encouraged to check the Tarantella Web site for more details on specific PKI vendors. As long as the PKI used is compatible with the Windows certificate cache and as well as the IIS Directory Service Mapper Secure Global Desktop will be able access certificates in the cache.

Since Secure Global Desktop supports Certificate based authentication, it easily supports authentication using Smart Cards. As long as the Smart Card vendor implements Window security providers that place certificates in the Windows certificate cache, Secure Global Desktop will be able use these certificates for authentication.

Launching applications

When a user launches an application, the user must logon to the Application Server that hosts the application. This is a fundamental feature of Windows Terminal Services. For this logon to be successful, the Application Server must verify the user's name, domain, and password. This verification requires a trust relationship between the domain containing the Application Server and the domain containing the user.

As a convenience to the user, Secure Global Desktop can cache the user name and password for Application Server logon on the client computer and use these stored credentials every time the user connects. Secure Global Desktop uses a strong encryption algorithm provided by the Windows CryptoAPI's protect the user's credentials. The administrator can configure the system to store the credentials in memory or on disk, or to disable the cache altogether.

Installation

Secure Global Desktop needs a domain user account and a domain group to operate. The domain user account is called the Secure Global Desktop System Identity. Secure Global Desktop components use this to authenticate to each other, so that malicious calls to the components are denied access. The Secure Global Desktop System Identity only needs normal user privileges, but it should be setup so that its password does not expire. This identity account should have access to the Secure Global Desktop Database. Additionally, this Secure Global Desktop Identity account should have read-only rights on all users that are likely to use the Secure Global Desktop system. For more information, refer to "Giving read permissions to Secure Global Desktop Identity account".

NOTE

For security reasons, it is recommended that the Secure Global Desktop Identity account should have low privileges in the domain and on the Database Server.

The domain group is called the Secure Global Desktop Administrators group. As the name implies, this group contains those users who have administrative access to the Secure Global Desktop system.

During initial installation of Secure Global Desktop, the installer prompts for the Secure Global Desktop System Identity and the Secure Global Desktop Administrator group. The administrator must provide the names of an existing user (whose password never expires) and a group for the accounts to manage Secure Global Desktop. During installation, the administrator who installs Secure Global Desktop must have software install privileges on the computers that will receive the installs.

When you add servers in Secure Global Desktop Team through Management Console, you must provide the name and the password of an account that has Administrative rights on the computer on which you are going to install the Secure Global Desktop software.

Server lock down

To help administrators protect their Application Servers, Secure Global Desktop contains a component that prevents RDP connections to the server that does not use Secure Global Desktop. Only Secure Global Desktop administrators and local administrators can logon to a locked down server through RDP. However, if the Primary Database Server is down, or if the Secure Global Desktop Database connectivity is lost due to some reason, only local administrators can logon to a locked down server through RDP.

Best practices

Secure Global Desktop has many security measures, but it is ultimately the administrator's responsibility to secure their datacenter.

Setup SSL

Perhaps the most important security precaution that the administrator can take is to install certificates on the Web Servers and Relay Servers so that Secure Global Desktop can use SSL for communications. SSL is required to make the basic authentication secure and to prevent tampering with the web traffic of the console. Once the certificate installation completes, the administrator should configure the Web Server to require SSL on the Console and Launch Pad Web sites.

Monitor audit logs

Secure Global Desktop keeps an audit trail of all the changes made to the system and the initiator. This audit can be very valuable to stop tampering with the system.

Update your operating system

Secure Global Desktop adapts to the operating system of the server that receives the install. Each release of Windows has new security features that Secure Global Desktop will exploit. In particular, Windows 2000, Windows 2003, and Windows XP contain security features that help Secure Global Desktop store user credentials.

Use the NTFS file system

The NTFS file system is an option of Windows 2000, Windows 2003, and Windows XP. Secure Global Desktop takes advantage of the access control feature of the NTFS file system to protect its files from tampering.

Place all Secure Global Desktop Servers in an Active Directory OU

It is a good management practice to place all the Secure Global Desktop servers in single Active Directory OU. From a security perspective, this configuration allows the administrator setup a Group Policy Object to govern the access settings and encryption levels of the servers.

Screen saver

We do not recommend setting screen savers for remote users' profiles and on the Application Servers.

File logging

Secure Global Desktop logs all warning, error, and information messages to a log file. The log file is called **SGDTSE.log** and it is created in the install directory. If the administrator accepted the default destination settings while installing Secure Global Desktop, the log file is created in **X:\Program Files\Tarantella** directory. A Secure Global Desktop administrator contacting the Tarantella Technical Support for some troubleshooting may be asked to send the log files as the log files contain a lot of information that can help the Technical Support in troubleshooting.

NOTE

File logging is not the same as tracing, whose options you can set from the **Options>System>Update System Options** *page.*

Configuration settings for log file

The error logging feature of Secure Global Desktop uses the **HKEY_LOCAL_MACHINE\SOFTWARE\New Moon Systems\Canaveral\<Secure Global Desktop version>\Config\Log** registry key. You can change the file logging settings by modifying the registry values. The following table lists the details of the Secure Global Desktop file logging registry keys.

TABLE 13. File Logging registry keys

Name	Default Value	Description
LoggingEnabled	1	Controls file logging. It can take one of the following values: • 1 - File logging enabled • 0 - File logging disabled
LogToFile	1	Controls where the logs go. It can take one of the following values: • 0 - Output debugger • 1 - File
MaxLogSizeMB	10	Controls the maximum file size for a log file before it is rolled over. The value specified is in MB. It can take any numeric value and is only limited by the amount of free space on the drive. It cannot be set to a value less than 1.

The changes made to the LoggingEnabled and LogToFile keys are effective immediately. For the changes made to MaxLogSizeMB key to be applicable, the administrator should restart the Secure Global Desktop Engine service.

Rollover of log file

When the SGDTSE.log file is full, that is, when it reaches the maximum log file size setting defined in registry, it is archived with the name SGDTSEOld.log. At each subsequent rollover, old SGDTSEOld.log file is replaced by new SGDTSE.log file and a new SGDTSE.log is created. Thus, the latest logs are always in SGDTSE.log file and the oldest logs are in SGDTSEOld.log.

Secure Global Desktop — Basic Configurations

This section addresses the ways you can configure Secure Global Desktop to support different operational demands. It also shows how you can scale Secure Global Desktop to accommodate more users over time.

You can use one of three basic configurations:

- Single Server Configuration: A Secure Global Desktop single-server configuration uses one Secure Global Desktop server.
- Multi-Server Configuration: A multi-server configuration distributes Secure Global Desktop across more than one server.
- Advanced-Server Configuration: An advanced configuration distributes roles across more than one server and creates redundant configuration elements.

In addition, you can install Secure Global Desktop on a local server, which may not be a part of a domain, for local users. For more information, refer to "Local server install".

Single server configuration

A small company or a site that is evaluating Secure Global Desktop can use the Secure Global Desktop single server configuration. An administrator can use this as an initial configuration, where there are plans to scale the Secure Global Desktop deployment in the future.

An administrator may want to choose the Secure Global Desktop single server configuration for a production site with up to 100 concurrent users.

A typical server configuration can use a Pentium III 500 MHz with 256 MB RAM and run on a Windows 2000 or a Windows 2003 server, and this might run a small site. To size a server to offer applications to these 100 concurrent users, the system might require a dual 1 GHz CPU with 4 GB of memory. The disk size will depend on the amount of storage the applications require.

Procedure

To set up a Secure Global Desktop single server configuration.

1. If you want the domain to be redundant, be sure that redundancy elements, such as RAID or clusters, exist.
2. Configure the Windows 2000 server in application delivery mode.
3. Add those applications that you will offer to your users to the Application Servers.
4. Set up the MSDE or Microsoft SQL Server.
5. Install Secure Global Desktop on a single box. This will set up the Web Server, Load Balancer, and Application Server roles on the same box.
6. Provision applications to those users who will use the Secure Global Desktop services.

This configuration provides some advantages. This configuration is very inexpensive to install, maintain, and backup. This configuration is easy to expand by adding new servers to the team.

This configuration also has some areas that you need to consider. Administrators are running Secure Global Desktop on a single server, so there is no built-in fault tolerance. Administrators cannot take advantage of load balancing in Secure Global Desktop, because there can be no load balancing when only one application server is used. Administrators can serve only a limited number of concurrent users.

If you plan to use a single server configuration, here are some tips.

- It is best to avoid using applications that consume large amounts of memory or CPU cycles.
- It is best to boost the number of processors on the server configuration.
- It is best to use a server that implements redundancy to reduce the opportunity for and consequences of failures. An administrator can implement redundancy by using technologies such as RAID, hot swap, dual power supplies, or cluster servers.
- It is best to keep Secure Global Desktop on a server other than the domain controller. However, if the domain controller must be on the same server, it is best to boost the amount of memory available on the server.

NOTE

Printing does not work when the Secure Global Desktop server resides on the domain controller.

Multi-server configuration

The multi-server configuration is generally appropriate for more mature sites or sites that have up to 1000 users. This configuration provides the ability to perform load balancing of applications in the Secure Global Desktop environment.

An administrator might use this type of configuration for a site that has more than 1000 concurrent users. Typically, the Application Servers should be at least dual Pentium III 600 MHz CPUs with 700 MB of memory. The Web Server/Load Balancer should be at least a dual Pentium III 500 MHz with 1GB of memory. The disk size will depend on the amount of storage the applications require.

The environment, as noted above, requires one Web Server/Load Balancer and one SQL server. The number of application servers typically used ranges between 15 and 25. If an administrator uses more powerful Application Servers, the site requires fewer Application Servers.

In order to set up Secure Global Desktop on several servers, administrators generally install Secure Global Desktop on a central server and then use the Secure Global Desktop Administrative Console to join other servers to the team. An administrator would add servers to a team, and then plan and push roles to the appropriate Application Servers. An administrator can push the following four roles: Web Server Role, Load Balancer Role, Application Server Role, and Relay Server Role.

NOTE

If the Console is running in secure mode (HTTPS), the Depot folder on the Web Server has to have plain HTTP access, even if the other folders are secured as HTTPS.

For a simple multi-server configuration, the administrator would most likely push many application server roles because Application Servers hold and manage applications that users use. The administrator would then provision applications to the Application Servers and to users (users, groups, and OUs) to Secure Global Desktop. Finally, the administrator would arrange for backups. An administrator might want to consider performing frequent incremental backups and less frequent full backups on the Secure Global Desktop database.

This configuration provides some advantages.

- It uses the load balancing capabilities of Secure Global Desktop.
- It can enhance security by using a single port relay server.
- It can accommodate server maintenance during business hours.

  It can do this because the Load Balancer has the ability to exclude a server from a team dynamically and to redirect application requests to the servers that remain in the team. This configuration allows an administrator to set CPU, memory, and queue resource limits for application servers to ensure better performance.
- It distributes processing load across the available resources so there is no concentration of load on a single server. This configuration is robust in that if one server fails, other servers can still accept new application requests.

This configuration also has some areas that you need to consider. Administrators are still working with a system that has a single point of failure because neither the SQL server nor the Web/Load Balancer server has redundancy features. Additionally, an administrator will see the entire Secure Global Desktop operation fail when the domain controller fails.

If you plan to use a multi-server configuration, here are some tips.

- When copies of the same application are stored on different Application Servers in a team, the instances of these applications need to be stored on the same absolute path on each server, so the Secure Global Desktop load balancer can use load balancing to accommodate a request for an application.
- Ensure an even distribution of the application load across all the servers. To do this, configure the servers to have similar characteristics in terms of storage, speed, and RAM. If some of the servers are more powerful than others then the Load Balancer will send those powerful servers a greater number of the application requests. This is the benefit of resource-based load balancing: the server with the most resources available receives the request.
- Consider placing servers that are involved in critical tasks in a redundant configuration. The administrator should implement one or more of the various technologies that the industry makes available to increase uptime. These technologies include RAID for hard disks, hot swap for power supplies, and fault tolerant NICs for communications.

Advanced-server configuration

The advanced configuration is generally appropriate for larger, complex sites. An administrator can use this configuration for sites that serve 1000 to 3000 users concurrently. This configuration has multiple web servers and load balancers and there is no single point of failure.

The hardware requirements for the advanced environment are similar to the requirements for the multi-server configuration. Yet this configuration is different in that it uses redundant hardware resources for the Web Server, Load Balancer, and Relay Server roles.

In order to set up Secure Global Desktop on several servers, administrators generally install Secure Global Desktop on a central server and then use the Secure Global Desktop Administrative Console to join other servers to the team. To set up Secure Global Desktop on several servers, an administrator would need to verify that a virtual IP server is available for the Web Server, and if only a round robin domain name system were available, this would suffice. However, it would not provide guaranteed system availability due to the implementation of round robin DNS. That administrator would also verify that a site management system is running in the Secure Global Desktop environment, as this type of software can warn administrators of critical events. Next, an administrator would set up applications on several application servers and the administrator would use an imaging technology to replicate the setup; in this way, an administrator could be sure that the software installs applications on the same absolute path for all servers. The administrator would distribute Secure Global Desktop roles to different servers to ensure that those servers that

have a unique role also have at least one companion server. This arrangement provides a nonstop configuration for the Web Server, the Load Balancer Server, and the SQL server. Of course, the Application Servers would be numerous. To enhance security, the administrator would distribute the Relay Server role to at least on server. Finally, the administrator would arrange for backups. An administrator might want to consider performing frequent incremental backups and less frequent full backups on the Secure Global Desktop database.

This configuration provides some advantages. This configuration provides a fully redundant environment, so there is no single point of failure, it accommodates a high number of simultaneous users, it accommodates best-of-breed technologies for virtual IP (VIP) and SQL Clustering, and it can use a network load balancer or a round robin domain name system to perform load balancing on the Web Servers.

This configuration also has some areas that you need to consider. Administrators are working in a more complex environment, the virtual IP server that is part of this configuration adds hardware expense, and to accommodate multiple sites, an administrator must make special preparations.

If you plan to use an advanced server configuration, here are some tips.

- It is recommended that an administrator install Microsoft Cluster Server (MSCS) on cluster nodes to encourage high-availability, scalability, and manageability for the Microsoft SQL Server. A SQL server in a clustered configuration requires a minimum of two servers and a shared disk storage device.
- The environment as noted above is suitable for many Application Servers. The ideal number of Application Servers that an administrator can manage range between 20 and 60. When an administrator uses more powerful application servers, fewer servers are required. Therefore, there is an inverse relationship between the number of servers required and the power of servers used.

Using the Console

What's in this chapter?

This chapter provides step-by-step procedures for using the Management Console to administer the Secure Global Desktop system.

Management Console overview

This section provides an introduction to the Management Console

Management Console tabs

Home

The Home tab provides access to the Secure Global Desktop Summary, Getting Started, Log On, Download, Product Keys, and About (Secure Global Desktop) pages. Additionally, it provides information about issues that require the Secure Global Desktop administrator's attention.

Manage

The Manage tab contains links to Applications, Servers, Groups, OUs, Users, Domains, Client Groups, Connection Settings, and Admin Roles pages. The manage function helps you work with objects. You can add, remove, or update object properties, and you can identify those objects that you want to use for Secure Global Desktop from those that exist in your existing domain.

Monitor

The Monitor tab contains links to Connections, Load Balancer, Database Connections, Relay Servers, and Jobs pages.

Report

The Report tab offers links to reports for sessions, applications, users, clients, servers, audit logs, and product keys.

Options

The Options tab provides links to objects that interface with or control the Secure Global Desktop environment. These objects include users, administrators, load balancers, relay servers, database servers, and system.

Common operations

This topic explains how to navigate through the Secure Global Desktop Administrative Console. Not all navigation elements appear on all pages, but you can learn about all navigation here.

Features

To help you work with multiple objects, Secure Global Desktop offers you the ability to:

Select multiple objects for an operation

This **select all** feature permits you to select the check box at the top of a column to select all of the objects that appear in that column.

Sort objects

View data in sequence by sorting on any of the columns in the report table. To do this, click the column heading that is to represent the new sort key. Secure Global Desktop immediately displays the re-sequenced data.

Filter objects

Choose a filter by selecting a property from the drop-down list box. Enter a corresponding value in the text field and click **Find**. Secure Global Desktop displays the items that meet the selection criteria.

Cancel button

The multi-page user input sequences have a **Cancel** button on page two and beyond. Click this button to cancel the in-progress action and go back to the starting page of the multi-page sequence.

What is application publishing?

Application publishing permits you to control application access to users, groups, and/or organizational units.

Once you have added an application into the system, you can provision this application to your users. Using Secure Global Desktop, you are able to provision applications to Domain Groups, Domain Organizational Units, and/or Domain Users. Additionally, you are able to provision applications to Client Groups.

Management Console Home tab

This Home tab has five objects, which this section considers.

"Summary page"

"Getting Started page"

"Log On page"

"Download page"

"Product Keys page"

"About page"

Summary page

This page notifies you when you have issues that require attention. If you need to take an action, this page indicates both the problem and the solution. It also provides a summary of the objects that Secure Global Desktop is managing. Additionally, it provides information about connections, Secure Global Desktop licenses in use, product keys limit, and audit logs.

NOTE

For a delegated administrator who has been assigned the monitoring task, the Summary page displays the total number of licenses currently consumed and not the number of licenses consumed by only the users that the delegated administrator can monitor.

Getting Started page

This page provides a quick overview of the activities associated with each of the other console tabs (Manage, Monitor, Reports, and Options). The tasks listed on this Getting Started page do not represent a comprehensive list of tasks available.

Log On page

From this page, a member of an administrator group or a delegated administrator can log on to the Management Console. Only some of the tabs of the Console are available when a delegated administrator logs on, depending on the tasks that have been delegated. For more information, refer to "Delegated administrator tasks".

The administrator group is set during the Secure Global Desktop install, and you can modify it from **Options>Administrator** page.

Procedure

To log on to the Management Console:

1. Access the management console from a Web browser using a URL of the following format:

   ```
   http://<webserver identification>/console
   ```

   NOTE

   Cookies should be enabled to log on to the Console.

2. In the **Logon Name** and **Password** fields, enter the user name and password you use to logon to the domain.

   NOTE

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

3. From the **Log on to** list, select the domain and click **Log On**.

Download page

From this page, you can download software for the Tarantella Client or the Secure Global Desktop Server.

Download for clients

You may download a Tarantella Client for a Windows-based client platform. This Tarantella Client allows users to launch applications, and it allows administrators to shadow a user’s session.

Secure Global Desktop offers you two versions of the client software:

- Tarantella Connection Manager (.exe): Secure Global Desktop requires Windows Installer version 1.0 on the client to run the client software. This package includes the Windows installer 1.1, checks for the installer on the client system, and if it is not there, it installs the software. Use this package if you will be directing users to an ftp site or a URL.
- Tarantella Connection Manager (.msi): This package does not include the Windows installer 1.1. Use this package if you will be pushing clients to the desktops via a third-party tool.

Download for servers

You may download the Secure Global Desktop server software for Secure Global Desktop servers.

To create a Secure Global Desktop team, you need to install the Secure Global Desktop Server software on the Web Server. After this, you can bring other servers into the Secure Global Desktop team. Under normal circumstances, you can push the join team software over the net using the **Manage>Server>Add Server** operation.

Under unusual circumstances, you can download this server software to the server that needs to join the team. To do this, you can hand-carry the Secure Global Desktop CD to each server that should join the team. Alternatively, you can log on to the console from the server, download Secure Global Desktop (.msi), and run the software on a server to join an existing team or to create a new team. This package does not include the Windows installer 1.1.

Product Keys page

From this page, you can view, add, or remove a Secure Global Desktop Product Key, or activate the system. In addition, you can view the Secure Global Desktop license usage.

Your product key type may be one of the following: beta key, evaluation key, base key, activation key, or user-level upgrade key. The product key regulates the number of users who can access your Secure Global Desktop system concurrently. You may notice that you have one product key, called a base key, and you may have several add-on or supplemental product keys. You will be unable to remove your base key, but you will be able to remove other product keys. The base key expires 60 days after installation. You need to activate the system with the activation key within 60 days of installing the base key.

For more information, see "Types of product keys".

Add Key

To add a product key:

1. On the **Product Keys** page, click the **Add Key** link to open the **Add Key** page.
2. In the **Product Key** field, enter the product key and click **Add**.

Remove Key

To remove an upgrade key from the Secure Global Desktop system:

1. On the **Product Keys** page, select the upgrade keys you want to delete, and click the **Remove Key** link to open the **Remove Key** page.
2. Click **Remove** to confirm that you want to remove the displayed keys.

NOTE

You can only remove Upgrade Keys from a Secure Global Desktop system.

Activate System

You have to activate your system within 60 days from the time you install the base key.

To activate the Secure Global Desktop system:

1. On the **Product Keys** page, click **Activate System**. The **Activate System** link is available only after the base key has been added to the Secure Global Desktop system. Once a system is activated, the **Activate System** link is not displayed on the Console.
2. From the **Activate System** page, copy the **Activation Request Code** and click http://www.tarantella.com/support/registration/activate.html to open a web form. Paste the Activation Request Code in the web form to get the activation key.
3. Follow the steps in "Add Key" to add the activation key and activate your system.

NOTE

The activation key of one Secure Global Desktop team installation cannot be used on another installation.

View License Usage

You can view the names of the users that are consuming the Secure Global Desktop licenses at any time and know the number of licenses that are already in use.

To view the Secure Global Desktop user licenses currently being used, on the **Product Keys** page, click **View License Usage**.

T the Concurrent User Licenses page opens, displaying the User Name of the users that are currently logged on, along with the Client Name of the computer they have logged on from.

About page

Use the **About** page to know more about your version of the Secure Global Desktop software. You can view the registered owner, the version number, and the build number. You can also locate phone numbers for contacting Tarantella Inc. and the URL for accessing the Tarantella Web site.

Management Console Manage tab

This Manage tab addresses the objects you can manage.

Manage summary

This **Manage>Summary** page identifies the types of objects that you can manage and it provides links to the pages that manage each object type, as follows:

"Manage applications"

"Manage servers"

"Manage groups"

"Manage OUs"

"Manage users"

"Manage domains"

"Manage Client Groups"

"Manage connection settings"

"Manage Admin Roles"

Manage applications

Use the **Manage>Applications** page to view or change application properties. This page displays the name, path, description, and the connection settings for all the applications that you add to the Secure Global Desktop system.

This page enables you to do the following:

"Add application to Secure Global Desktop"

"Update application properties"

"Remove applications"

"Update file associations"

"Add applications to servers"

"Remove applications from servers"

"Add applications to groups"

"Remove applications from groups"

"Add applications to OUs"

"Remove applications from OUs"

"Add applications to users"

"Remove applications from users"

You must install an application on an Application Server before you can add that application to Secure Global Desktop using the **Manage > Applications** functions.

Add application to Secure Global Desktop

To add an application:

1. On the **Manage>Applications** page, click **Add Application**.
2. The **Add Application** page opens. While adding an application you need to:
   - "Add application details"
   - "Select servers"
   - "File associations"
   - "Select groups"
   - "Select OUs"

After adding the application, you can make it available to individual users from the **Manage>Applications>Add Users** page. If a domain user does not exist in the Secure Global Desktop system, you can add the user from the **Manage>Users>Add User** page.

The sections that follow explain each step in detail. Select/Enter the relevant information on each page.

Add application details

The **Add Application** page allows you to add application information, the launch settings, and the application defaults for shortcuts.

Application Type

You can choose to add the following:

- **Windows Desktop**, to provision the desktop of an Application Server
- **Application**, to add an application on an Application Server

You can add the applications to Secure Global Desktop by using the **Start** button on the Add Application page along with the server's name, which you select from the drop-down list. To use this function, first select the name of the Application Server that holds the application you want, and then click the **Start** button. This causes Secure Global Desktop to retrieve a list of applications that appear on the Windows Start menu of the Application Server you select.

- If the application you want appears under the Application Server's Start menu, you can see the application on the Start list and you can select it. Secure Global Desktop automatically places the configuration data that Secure Global Desktop requires onto this Add Application page. Some applications such as Microsoft FrontPage, Microsoft Project, and some Microsoft Office Tools are not displayed on the Start list even if they are installed on the selected Application Server. You need to enter the application information for these applications manually.
- If the application you want does not appear under the Application Server's Start menu, but is located on the server in a different directory, then you must manually enter the application information on this Add Application page.

NOTE

If you are planning to use copies of this application on more than one Application Server in the Secure Global Desktop team, all instances of this application must reside on the same absolute path on each specific server. For example, if a program appears under C:\Program Files\Microsoft Office\<anything>.exe on one computer in a team, it must appear under this same path for all computers in that team.

The following text explains the other fields that appear on this page. The fields marked with an asterisk (*) are mandatory fields.

Application Information

Application Name*

This application name will display on the Management Console. You may want to browse the applications on a specific server using the navigation tools on this page to select the starting information for this application's name. Once the application data appears on this page, you may customize the name that appears in this field. You do not have to use the name that the program provides.

Description

This is a free-form description of the application. You may want to add identifying information such as who uses this application.

Application Path*

This element must be a fully qualified path with the .exe file extension. When the browse utility completes this name, you *must not* change the application path. Furthermore, if more than one server in the same team will run this application, then the application *must* be loaded on all of the affected servers on this specific path. All instances of one application on all members of one team must appear on one consistent path.

Working Directory

Secure Global Desktop generally selects a working directory name, however, if this property is blank, then Secure Global Desktop assigns a default working directory path.

Command Line Parameters

This field has no effect when the field is blank. If you enter a command line, Secure Global Desktop will launch the application using the information on that command line.

Start Menu Location

This field can hold two types of values, a blank value, and a literal value.

- The literal value (folder path name), places the shortcut folder at the location of the literal path on the Windows Start menu on a client. When you select this option, if an administrator changes the team's name, Secure Global Desktop does *not* manage the path's modification. For example, if you specify the path as **Secure Global Desktop Team\Marketing** in this field, the shortcuts are created in the **Start>Programs>Secure Global Desktop Team>Marketing** folder.
- A blank value permits Secure Global Desktop to manage the location of the folder and Secure Global Desktop places the folder under the Secure Global Desktop Team's name on the user's Windows Start menu. When you select this option, if an administrator changes the team's name, Secure Global Desktop automatically manages the path's modification. For example, if the team name is **Secure Global Desktop Team Marketing**, and this field is left bank, the shortcuts are created in **Start>Programs>Secure Global Desktop Team Marketing** folder.

NOTE

To disable shortcuts, select **Options>User>Update Options** *and from the* **Shortcuts** *list, choose* **None***.*

Launch Settings

Connection Setting

This parameter governs the way an application connects to Secure Global Desktop. Refer to "Connection settings", for more information on this concept. You can specify the Connection Settings as:

- Unspecified
- Default
- Any other Connection Settings defined in the system

Limit Total Concurrent Sessions

This places a maximum limit on the number of sessions of this application that can run concurrently, on this Secure Global Desktop **team**. This is particularly useful for applications where you are using specific application licenses rather than site licenses.

Limit Concurrent Sessions per Server

This places a maximum boundary on the number of sessions of this application that can run concurrently, on any one Secure Global Desktop application server. This is particularly useful for applications that exhibit high overhead or high resource-utilization profiles.

Application Defaults

This area sets the default location for shortcuts. Secure Global Desktop uses the default location an administrator sets here. However, an administrator can permit users to change these defaults individually, for their own user name.

Favorites

This parameter places a shortcut to this application on the Favorites page on the user's Secure Global Desktop Application Launch Pad.

Start Menu Shortcut

This parameter places a shortcut to this application on the user's Windows Start menu.

Desktop Shortcut

This parameter places a shortcut to this application on the user's Desktop.

File Association

This parameter enables file associations for this application.

Click **Next** to proceed to the **Select Servers** page

Select servers

The **Select Servers** page allows you to select the Application Servers that will host the application. Select the Application Servers and click **Next** to proceed to the **File Associations** page.

NOTE

You can also add applications to Application Servers later from **Manage>Applications>Add Servers** *page.*

File associations

The **File Associations** page retrieves all the possible extensions that can be associated with the application based on the servers that will host the application. You can associate the application with one or more of these file extensions. When file associations are enabled, a user can open a document in an application on an Application Server by double-clicking the file. Select the file extensions you want to associate with the application and click **Next** to proceed to the **Select Groups** page.

NOTE

You can also make file associations later from **Manage>Applications>Update File Associations** *page.*

Select groups

The **Select Groups** page retrieves a list of the domain groups in the Secure Global Desktop system and allows you to select the groups that will be able to access the application. You may add a group to the system from the **Manage>Groups>Add Group** page. Select the groups and click **Next** to proceed to the **Select OUs** page.

NOTE

You can also add applications to domain groups later from **Manage>Applications>Add Groups** *page.*

Select OUs

The **Select OUs** page retrieves a list of the OUs in the Secure Global Desktop system and allows you to select the OUs that will be able to access the application. You may add an OU to the system from the **Manage>OUs>Add OU** page. Select the OUs and click **Next**.

NOTE

You can also add applications to OUs later from **Manage>Applications>Add OUs** *page.*

The **Add Application** page displays the choices you make in the sequence. Review the information and click **Add** to add the application to the Secure Global Desktop system.

Update application properties

You can change properties such as that of the Limit Total Concurrent Sessions, Application Path, Command Line Parameters, or any other property. When you select one application to update, all of the currently assigned properties appear for editing.

You can update multiple applications by selecting multiple applications and clicking **Update Application** on the **Manage>Applications** page. Select the properties you want to update, fill in the appropriate information, and click **Update**. Secure Global Desktop updates all selected properties for all selected applications. For a complete list of property definitions, see "Add application to Secure Global Desktop".

Remove applications

This removes the application from use on the selected Secure Global Desktop Application Servers. The application remains installed on the Application Server; it is simply unavailable to the Secure Global Desktop users.

To remove applications:

1. From the **Manage>Applications** page, select the applications you want to remove and click **Remove Application**.
2. Verify that the applications listed are the ones you want to remove and click **Remove.**

Update file associations

You can associate applications with file extensions. When file associations are enabled, a user can open a document in an application on an Application Server by double-clicking the file. You can update the file associations made with an application.

To update the file associations for an application:

1. On the **Manage>Applications** page, select an application, click **Update File Associations**, and then click **Next**. The system retrieves all the extensions you can associate with the application from the Application Servers.
2. Select the extensions you want to associate with the application and click **Update**.

Add applications to servers

You can add applications to servers that exist within a Secure Global Desktop team.

To add applications to servers:

1. From the **Manage>Applications** page, select an application, and then click **Add Servers**.
2. Select the servers that are to host this application, and click **Add**. The application will now become available from these selected servers.

NOTE

You can add multiple applications to multiple servers at one time by selecting multiple applications to add and selecting multiple servers to receive.

Remove applications from servers

To stop an application from being hosted by servers:

1. From the **Manage>Applications** page, select an application, and then click **Remove Servers**.
2. Select the servers and click **Remove**. The application remains installed on the Application Server; it is simply unavailable, on the selected servers, to the Secure Global Desktop users.

Add applications to groups

You can add applications to groups that exist within Secure Global Desktop.

To add an application to groups:

1. From the **Manage>Applications** page, select an application and click **Add Groups**.
2. Select the groups that are to receive access to the applications, and click **Add**. This provisions applications to the selected groups.

NOTE

If you want to add applications to groups that are not on this list, you must add these groups to Secure Global Desktop from the existing domain from **Manage>Groups>Add Groups** *page. After you add a group to Secure Global Desktop, you can add applications to it.*

Remove applications from groups

You can add remove application availability to groups that have been assigned an application.

To remove an application from groups:

1. From the **Manage>Applications** page, select an application and click **Remove Groups**.
2. Select the groups that should no longer use this application, and then click **Remove**. Secure Global Desktop will no longer provision the application to those selected groups.

Add applications to OUs

You can add applications to OUs that exist within Secure Global Desktop.

To add an application to an OU:

1. From the **Manage>Applications** page, select an application and click **Add OUs**.
2. Select the OUs that are to receive access to the applications, and click **Add**. This provisions applications to the selected OUs.

NOTE

If you want to add applications to OUs that are not on this list, you must add these OUs to Secure Global Desktop from the existing domain from **Manage>OUs>Add OUs page***. After you add an OU to Secure Global Desktop, you can add applications to it.*

Remove applications from OUs

You can remove application availability to OUs that have been assigned an application.

To remove an application from an OU:

1. From the **Manage>Applications** page, select an application and click **Remove OUs**.
2. Select the OUs that should no longer use this application and click **Remove**. Secure Global Desktop will no longer provision the application to those selected OUs.

Add applications to users

You can directly provision existing applications to existing users in the Secure Global Desktop system.

To provision applications to a user that exists within Secure Global Desktop:

1. From the **Manage>Applications** page, select an application and click **Add Users**.
2. Select the **Logon Name** of the users that are to receive access to the application and click **Add**.

NOTE

If you want to provision applications to users that are not on the list, you must first add the users to Secure Global Desktop and then add applications to the users. For more information, refer to Add a user.

Remove applications from users

You can remove application availability to users that have been assigned an application.

To remove applications from existing users in the Secure Global Desktop system:

1. From the **Manage>Applications** page, select an application and click **Remove Users**.
2. Select the **Logon Name** of the users that should no longer use this application and click **Remove**.

Manage servers

You access the **Manage>Servers** page to know about the servers, change server properties, run diagnostics on a server, remove a server from a Secure Global Desktop team, add or remove roles to or from a server, or add or remove applications to or from a server.

The summary page displays all of the servers of the Secure Global Desktop team. You can use this page to see which servers are operating, what roles they hold, and whether they exist online, installed, and enabled.

In all cases, you can add, update, and remove properties for one object. In many cases, you can add, update, or remove properties for many or for all of the instances of an object. For example, for servers, you may want to update or delete a property for all servers at one time.

This section provides step-by-step procedures to do the following:

"Add a server"

"Update server profile"

"Change server status"

"Diagnose server condition"

"Remove a server"

"Add roles to a server"

"Remove roles from a server"

"Add applications"

"Remove applications"

Add a server

The **Add Server** page allows you to add a remote server to the Secure Global Desktop Team. Secure Global Desktop tries to install software remotely on the server you want to add, so you must have administrative rights on the remote server. When you add a server, you need to enter server information and the server administrator information required to add the server.

NOTE

If the Console is running in secure mode (HTTPS), the Depot folder on the Web Server has to have plain HTTP access, even if the other folders are secured as HTTPS.

These are the properties for the Add function. Where a field name holds an asterisk, the associated property is mandator y.

Server Information

Server name*

This name is used to connect to the server.

This can be the distinguished name for the server (also known as the DNS name, interchangeably written as FQDN name), or it is the IP address, or it is the NetBIOS name. If you use multiple domains, it is important that you use the FQDN name format, serverX.domain.com. A NetBIOS name such as <serverX> may not resolve correctly in a Secure Global Desktop environment that serves multiple domains.

Description

This provides free-form text that identifies the server or clarifies other information.

Published Address

When you specify a server IP address or fully qualified domain name (FQDN) in this field, a client will use this address to connect to this server. If you do not specify an address in this field, Secure Global Desktop routes the client connections to the Internal IP Address.

NOTE

If you specify a published address, be sure to specify an address that is available to a client because a server may have several IP addresses and some of these addresses may be unavailable for client connections.

Disable Best Internal Address Discovery

By default, Secure Global Desktop will discover the best address to use for its internal communication. If you wish to specify a particular address, clear this check box to disable the discovery mechanism and enter an Internal IP Address or DNS name in the **Internal Address to use** field.

Internal Address to use

Members of the Secure Global Desktop Team use this address to communicate with each other. Enter the internal IP address, NetBIOS name, or FQDN name in this field. If you do not specify an Internal Address, Secure Global Desktop will use the address that best communicates with your database server.

For more information, see "Add server fails".

Install Directory

This is the directory where Secure Global Desktop will place this server's Secure Global Desktop role software. If you place no value here, Secure Global Desktop places the software in the Program Files directory.

Click **Next** to provide server administrator information.

Server Administrator Information

Logon Name*

To add a server to a Secure Global Desktop Team, Secure Global Desktop remotely installs software on the server you are adding. To do that, it needs Administrative privileges on the remote computer. Specify the Logon name that Secure Global Desktop should use to connect to the remote server

Password

Specify the Password for the Logon Name specified above.

Domain Name*

Specify the name of the Domain for the Logon Name specified above.

The information entered here should be correct for Secure Global Desktop to be able to connect to the remote server.

Click **Next**. The **Add Server** page displays the information you enter. Review the information and click **Add** to add the server to the Secure Global Desktop team.

Join Team Download

If you do not want to do a remote install on the server, you can add a server to the Secure Global Desktop team in one of several ways.

- Take the Secure Global Desktop install CD to the server that is to join the team and run an install.
- Log on to the Management Console from the server that is to join the team, and click **Home>Download**. Then click the Secure Global Desktop (msi) link to download the software to local disk.

Update server profile

Use the **Update Server** action to update a server's properties. All of the properties that appear on this page also appear on the **Add Server** page, for more information on these variables, refer to "Add a server".

Change server status

Use the **Change Status** action to enable or disable a server. A server with an Enabled status is ready and available. A server with a Disabled status is not available. You may want to disable a server for maintenance.

TABLE 14. Enable/disable servers with server-specific behaviors

Role	Enable	Disable when safe	Disable forcefully
Application Server	Accepts new application launches	Does not accept new launches and gets disabled when existing sessions are closed	Kills all active sessions and stops accepting new application sessions
Load Balancer	Used as master or redundant load balancer	Does not accept new load balancing requests	Does not accept new load balancing requests
Web Server	Enabled	User cannot access Launch Pad	User cannot access Launch Pad
Relay server	Accepts new application launches	Does not accept new launches and gets disabled when existing sessions are closed	Kills all active sessions and stops accepting new application sessions

As soon as you choose the **Disable when safe** option, the server stops accepting any new connections of

- Applications
- Single Port Relay
- Load Balancer election

Nevertheless, all lights on the **Manage>Servers** summary page stay green. As each session gets over from the disabled server, within two minutes, that role is disabled and the lights go red, indicating that the server is disabled.

Diagnose server condition

Use the **Diagnose Server** action to run diagnostics. Secure Global Desktop provides several one-click diagnostics that check the configuration of servers. It is good to run these tests after you

make server configuration changes. In this way, you can determine that the server is stable and ready to run correctly. If the server is not stable, you can address any issues before you attempt to move on to other tasks. From the **Manage>Servers** page, select the servers and click **Diagnose Server**. From the **Diagnose Server** page, select the diagnostic tests you want to run on the selected servers and click **Diagnose**.

If you receive a Settings Test failure, see "Settings Test failure".

For a complete explanation of diagnostics, see "Diagnostics".

Remove a server

Use the **Remove Server** action to remove a server from the Secure Global Desktop team. All software installed by Secure Global Desktop is removed and the server no longer remains a part of the Secure Global Desktop Team. The application software you installed on that server remains on that server. Secure Global Desktop removes only the software that it installed.

Some methods for removing a server are a little safer and others are a little quicker. You can choose from the following options:

When safe

This indicates that you want Secure Global Desktop to manage the role/server removal in a way that has no adverse impact on your environment. For example, you may want to remove an Application Server role only when all connections are closed.

Now

This indicates that you are confident that an immediate update to roles/servers will have no adverse impact on your environment; or, that you do not care if there is an adverse impact on your environment. For example, you want to remove an Application Server, with this selection, Secure Global Desktop drops any open client connections, and your users lose any data that is in process on the Application Server at that time.

Only from database

This indicates that you want to remove this role/server from the database only. You might want to do this when you cannot uninstall a role or the computer has crashed. This option removes the role from the database but Secure Global Desktop does not attempt to uninstall the role from the server.

Add roles to a server

Use the **Add Roles** action to add additional roles to one server, and you can use this to create redundant configurations (by placing the same role on more than one server). You must set up the required roles within the server team to run Secure Global Desktop, but once the team holds an instance of each required role, you can begin to create redundant roles. Before you do this, see "Secure Global Desktop — Basic Configurations".

When you are adding a Load Balancer role, or a Web Server role to a server, you will see no properties. If you are adding a Relay Server role, you can view the Relay Server information such as the relay port, whether SSL handshake is enabled or not, and the Server Certificate. You can change these options from the **Options>Relay Servers** page.

NOTE

If you change the relay port, the existing connections are disconnected. However, the user can reconnect the disconnected sessions from the Launch Pad **Connections** *page, depending on the connection settings.*

The port configured as **Relay Port** in the Secure Global Desktop system should be available. The system does not allow pushing of the Relay Server role on a server on which the port configured for single port relay is not available. If the port is not available on a server, the **Relay Server Role** check box is disabled when you select the server to push a role on it.

NOTE

If the Console is running in secure mode (HTTPS), the Depot folder on the Web Server has to have plain HTTP access, even if the other folders are secured as HTTPS.

However, if you are adding an Application Server role to a server, you will see the following server information properties.

Server Type

This identifies the function of the server. For example, for an Application Delivery Server, the type may be WTS for Windows 2000 Server or Windows Server 2003.

Printer INF path

If the vendor supplied printer drivers reside in the INF directory, then use this location as the list of supported printers and manufacturers. The default location is C:\WINNT\inf\ntprint.inf

Additional driver path

If the vendor-supplied printer drivers reside in a different directory, specify the other directories here; for example, C:\ i386, or use this field to specify the network share where the printer drivers exist. If you use a network share, the network share must have read rights set to All Users.

For more information, see "Web Server role", "Load Balancer role", "Relay Server role", "Application Server role", and "Understanding feature considerations".

Remove roles from a server

Use the **Remove Roles** action to remove roles from a server.

Removing required roles

If you attempt to remove a required role that has only one instance on this team, you will receive a warning such as:

One of the selected roles is the last role in the Team. If you remove this role, your system may become unusable.

NOTE

If you click **Remove** *at this point, the server may reboot.*

Checking the location of roles

Before you remove any roles, click **Manage>Servers** to see where the roles are installed. Secure Global Desktop runs when all of the required roles are present. If some of the required roles are

not present, Secure Global Desktop will not operate fully until you reinstall the missing, required roles.

NOTE

If you remove the last Web Server role, your Secure Global Desktop installation will be out of commission. After such an event, you must reinstall Secure Global Desktop using the Secure Global Desktop CD. When you run the new install, select the **Create New Team** *option and provide the Secure Global Desktop database server's name. Do not Overwrite the database. The database is the key to recreating the Secure Global Desktop team. When an install rejoins your server to the database using the Create New Team option, Secure Global Desktop can reconstruct your team.*

Removing roles incorrectly

If you remove roles from a Secure Global Desktop team incorrectly, which could be by using the Windows Add/Remove program, you will **not** remove the role from the Secure Global Desktop database; consequently, when Secure Global Desktop lists roles installed at a later time, it will continue to show the incorrectly removed role as installed. Therefore, to preserve the integrity and consistency of your data, it is important to remove roles correctly, using **Manage>Servers>Remove Roles**.

Add applications

You can add applications to servers that exist within Secure Global Desktop. When you use this action, from the **Manage>Servers** page, select a server and click **Add Application**. The application will now be available from your selected servers. You can add multiple applications to servers in one operation too. To do this, choose multiple servers and click **Add Application**. Select the applications that you want to add to these servers and click **Add**. All selected applications will be available from the selected servers.

NOTE

With this function, Secure Global Desktop will overwrite any previous application chosen to run on these servers. Only the newly selected set of applications will remain.

Remove applications

When you use this action, from the **Manage>Servers** page, select the servers and click **Remove Applications**. Select the applications you want to remove, and click **Remove**. Secure Global Desktop will configure these servers to make these applications unavailable from the selected servers. Secure Global Desktop does not remove the application from the servers; it simply makes the application unavailable through the selected servers.

Manage groups

Use the **Manage>Groups** page to know about domain Groups, to add or remove Groups to or from Secure Global Desktop; to synchronize the Secure Global Desktop domain Groups with the corporate domain's Groups; or to add or remove applications to or from the purview of a Group.

The summary page displays all of the groups that are set up to use Secure Global Desktop. You can use this page to see the subset of groups, from among *all* groups in the existing domain, that can use Secure Global Desktop.

In all instances, you can add, update, and remove properties for one object. In many instances, you can add, update, or remove properties for many or for all of the instances of an object. For example, for groups, you may want to update or delete all groups at one time. You may also want to synchronize several groups with the existing domain.

This section provides step-by-step procedures to do the following:

"Add a group"

"Remove a group"

"Synchronize a group"

"Add applications to a group"

"Remove applications from a group"

Add a group

Use the **Add Group** action to add a group to Secure Global Desktop. You would do this if you wanted to provision an application to a group of users. To perform this add event, from the **Manage>Groups** page, click **Add Group**. Secure Global Desktop reads all of the groups in your selected domain and displays them in ascending order. Select groups you would like to provision applications to, and click **Next**. Select the applications you would like to provision to the selected groups and click **Next**. Verify that the displayed information is correct and click **Add**. All the selected groups will have access to the applications you have selected. To add more applications to a group, see "Add applications to groups".

Remove a group

Use the **Remove Group** action to remove a group from Secure Global Desktop. To perform this, from the **Manage>Groups** page, select the group that you want to remove and click **Remove Group**. Verify that the displayed information is correct and click **Remove**. When you remove a group, anyone from that group who is using Secure Global Desktop can continue and complete their current session. However, they will be unable to launch a new session.

Synchronize a group

The **Synchronize Group** action ensures that the group information in the Secure Global Desktop domain remains synchronized with the group information in the corporate domain. This ensures that any addition or removal of users to or from a corporate domain group also appears in the corresponding Secure Global Desktop group. It is important that information concerning these two groups remains synchronized. To perform this, from the **Manage>Groups** page, select the group that you want to synchronize and click **Synchronize Group**. Verify that the displayed information is correct and click **Synchronize**.

Add applications to a group

You can add applications to groups that exist within Secure Global Desktop. When you use this action, from the **Manage>Groups** page, select a group and click **Add Applications**. You can add multiple applications to groups in one operation too. To do this, choose multiple groups and click **Add Applications**. Select the applications that should be added to these groups and click **Add**. Afterwards, the selected applications will be available from the selected groups.

NOTE

Secure Global Desktop will overwrite any previous selection of applications for these groups with this newly selected set of applications.

Remove applications from a group

You can take applications away from groups that exist within Secure Global Desktop. When you use this action, from the **Manage>Groups** page, select a group and click **Remove Applications**. Select the applications to remove and click **Remove**. The selected applications will no longer be available to users in that group.

Manage OUs

Use the **Manage>OUs** page to know about the domain's OUs, to add or remove OUs to or from Secure Global Desktop; to synchronize the Secure Global Desktop domain OU with the corporate domain's OU; or to add or remove applications to or from the purview of an OU.

The summary page displays all of the OUs that are set up to use Secure Global Desktop. You can use this page to see the subset of OUs, from among *all* domain OUs, which can use Secure Global Desktop.

In all instances, you can add, update, and remove properties for one object. In many instances, you can add, update, or remove properties for many or for all of the instances of an object. For example, for OUs, you may want to update or delete all OUs at one time. You may also want to synchronize several OUs with the existing domain.

This section provides step-by-step procedures for the following:

"Add an OU"

"Remove an OU"

"Synchronize an OU"

"Add applications to an OU"

"Remove applications from an OU"

Add an OU

Use the **Add OU** action to add an OU to Secure Global Desktop. You would do this if you wanted to provision an application to an OU. To perform this function, from the **Manage>OUs** page, click **Add OU**. Secure Global Desktop reads all of the OUs in your selected domain and displays them in ascending order. Select all the OUs to which you would like to provision applications. Click **Next**. Select applications you would like to provision to those OUs, and click **Next**. Verify that the information is correct, and click **Add**. Now all the selected OUs will have access to the applications you have selected. To add more applications to an OU, see "Add applications to OUs".

Remove an OU

Use the **Remove OU** action to remove an OU from Secure Global Desktop. To perform this action, from the **Manage>OUs** page, select the OU that you want to remove and click **Remove OU**. Next, you verify that the OU you selected is the one you want to remove, and then you click **Remove**. When you remove an OU, anyone from that OU who is using Secure Global Desktop can continue and complete their current session. However, they will not be able to launch a new session.

Synchronize an OU

The **Synchronize OU** feature ensures that the OUs in Secure Global Desktop are synchronized with the OU information in the existing domain. This means that any addition or removal of users to or from a corporate domain OU is reflected in the Secure Global Desktop OU. It is important that you keep the Secure Global Desktop OUs in sync with the existing domain OUs for proper functioning of Secure Global Desktop. To perform this, from the **Manage>OUs** page, select the OU that you want to synchronize and click **Synchronize OU**. Verify that the displayed information is correct and click **Synchronize**.

Add applications to an OU

You can add applications to servers that exist within Secure Global Desktop. When you use this action, from the **Manage>OUs** page, select an OU and click **Add Application**. The application will now be available from your selected OUs. You can add multiple applications to OUs in one operation too. To do this, choose multiple OUs, click **Add Application**, and select the applications to add to these OUs, and click **Add**. Afterwards, the selected applications will be available from the selected OUs.

NOTE

Secure Global Desktop will overwrite any previous selection of applications for these OUs with this newly selected set of applications.

Remove applications from an OU

You can take applications away from OUs that exist within Secure Global Desktop. When you use this action, from the **Manage>OUs** page, select an OU and click **Remove Applications**. Select the applications to remove, and click **Remove**. Afterwards, the selected applications will no longer be available to users in that OU.

Manage users

You access this page to know about the domain's Users of Secure Global Desktop; to add or remove Users to or from Secure Global Desktop; or to add or remove applications to or from the purview of User.

The summary page displays all of the users that are set up to use Secure Global Desktop. You can use this page to see the subset of users, from among *all* domain users, who can use Secure Global Desktop.

In all instances, you can add, update, and remove properties for one object. In many instances, you can add, update, or remove properties for many or for all of the instances of an object. For example, for users, you may want to update or delete many users at one time.

This section provides step-by-step procedures to do the following:

"Add a user"

"Remove a user"

"Add applications to a user"

"Remove applications from a user"

Add a user

Use this option to add a user to Secure Global Desktop. You would do this if you wanted to provision an application to a specific user or users. To perform this function, from the **Manage>Users** page, click **Add User**. Secure Global Desktop reads all of the users in your selected domain and displays the full name and logon name of each user in ascending order. Select all the users you would like to provision applications to and click **Next**. Select applications you would like to provision to those users and click **Next**. Verify that the information is correct, and click **Add**. Now all those users will have access to the applications you have selected. To add more applications to a user, see "Add applications to users".

NOTE

You cannot add a user, whose First Name or Last Name has more than 60 characters, to the Secure Global Desktop system.

Remove a user

Use this option to remove a user from Secure Global Desktop. To perform this remove, from the **Manage>Users** page, select the user that you want to remove and click **Remove User**. Verify that the information is correct, and click **Remove**. When you remove a user, if that user is using Secure Global Desktop, that user can continue and complete the current session. However, that user will not be able to launch a new session.

Add applications to a user

You can provision applications to users that exist within Secure Global Desktop. When you use this action, from the **Manage>Users** page, select the user that will receive additional applications and click **Add Applications**. Select the applications that you want to provision and click **Add**. The selected applications will now be available to the user.

NOTE

You can provision application to individual users; however, you should generally provision applications at the Group or OU level. In this way, you can provision, with only one action, to all users who belong to a Group or OU.

If you have one user in a group or OU who needs access to one additional program, a program that the others users should not use, that would be a perfect opportunity to use this function to provision that one application to that one user.

Remove applications from a user

You can take one or more applications away from users that exist within Secure Global Desktop. When you use this action, from the **Manage>Users** page, select a user and click **Remove Applications**. Select the applications you want to remove and click **Remove**. Afterwards, the selected applications will no longer be available to that user through provisioning at a user level.

Meanwhile, if the user inherits use of the same applications from a group or OU, then that user will continue to have use of that application until you remove the application from that Group or OU or until you remove the User from the Group or OU that inherits these applications.

Manage domains

Use the **Manage>Domains** page to add or remove Domains to or from Secure Global Desktop, or to synchronize the Secure Global Desktop Domains with the corporate Domain.

In all instances, you can add, update, and remove properties for one object. In many instances, you can add, update, or remove properties for many or for all of the instances of an object. For example, for domain, you may want to update or delete several domains at one time. You may also want to synchronize several Secure Global Desktop domains with the existing domains.

This section provides step-by-step procedures to do the following:

"Add a domain"

"Remove a domain"

"Synchronize a domain"

Add a domain

Use this option to add a domain to Secure Global Desktop. To perform this addition, from the **Manage>Domains** page, click **Add Domain**. Type the name of the domain you wish to add, and click **Next**. Review the domain information and click **Add**. After you add a new domain to your system, you must add OUs, groups, and users from that domain to Secure Global Desktop and provision applications to these entities.

NOTE

If you want to add an Active Directory domain running on Windows Server 2003 to a Secure Global Desktop team, make sure that the computer where Secure Global Desktop Web Server role is installed is a part of the same an Active Directory domain running on Windows Server 2003, or is a part of one of the domains in the same Windows Server 2003 forest. You cannot add a trusted an Active Directory domain running on Windows Server 2003 to a Secure Global Desktop team in an Active Directory domain when the two domains are in different forests.

For Active Directory synchronization to take place for users at logon, you need to give the required permissions to the Secure Global Desktop Identity account to access information from the Active Directory in the new domain. For information on how to do this, refer to "Prerequisites".

Remove a domain

Use this option to remove a domain from Secure Global Desktop. To perform this function, from the **Manage>Domains** page, select the domain that you want to remove and click **Remove Domain**. Verify that the domain listed is the one you want to remove and click **Remove**.

Synchronize a domain

Use this option to synchronize a domain that resides in Secure Global Desktop with the current view of the corporate domain. This will synchronize all users, OUs, and groups from that domain. This synchronization may result in application assignment changes because of users moving from one department or division to another, which might result in a user appearing in a different domain group or OU; one which uses different applications. To perform this synchronization function, from the **Manage>Domains** page, click **Synchronize Domain**, verify that you selected the domain you intended to select and click **Synchronize**.

Manage Client Groups

Use the **Manage>Client Groups** page to add, remove, or update a Client Group; to update filter criteria; or to add or remove applications, printer, or clients to existing Client Groups.

This section provides step-by-step procedures to do the following:

"Add Client Group"

"Update Client Group"

"Update filters"

"Remove Client Group"

"Add applications to a Client Group"

"Remove applications from a Client Group"

"Add printers"

"Set default printer"

"Remove printers"

"Add clients"

"Remove clients"

Add Client Group

To add a Client Group:

1. On the **Manage> Client Groups** page, click **Add Client Group**.
2. The **Add Client Group** page opens. While adding a Client Group you need to:
   - "Add Client Group information"
   - "Add filters"
   - "Select applications"
   - "Select printers"
   - "Select clients"

The sections that follow explain each of these in detail. Select/Enter the relevant information on each page.

Add Client Group information

The **Add Client Group** page allows you to specify the Client Group information, launch settings, and restrictions on clients.

Client Group Information

Name*

This Client Group name appears on the Secure Global Desktop reports. You should specify a meaningful name for a Client Group.

Description

This provides free-form text that identifies or clarifies other information.

Launch Settings

Connection Setting

The connection setting object determines the properties of the connection between the client computer and the Secure Global Desktop application server. It contains a number of parameters that affect the security of the connection. For more information, see "Manage connection settings" and "Connection settings".

Restrictions on Clients

Do Not Allow Save Password

Select this check box to prohibit the users from saving their passwords. If you do not select this option, then the users will see the **Automatically Log On From This Computer** check box on the Secure Global Desktop Application Launch Pad.

Do Not Allow Creation Of User Shortcuts

Select this check box to prohibit users from adding shortcuts to their Start Menu or to their desktops. If you do not select this check box, users can use the Options page on their Launch Pad to configure shortcuts. If you select this option, then the users will not see this option on their Secure Global Desktop Application Launch Pad.

Disable Secure Global Desktop File Associations

Select this check box to disable file associations on the clients for the Client Group applications that belong to this Client Group.

Hide Tarantella Connection Manager Tray Icon

Select this option to hide the Tarantella Connection Manager Tray Icon. In this case, the users will be able to launch applications only from the user shortcuts if the administrator has not disabled shortcuts, or from the Launch Pad.

Click **Next** to go to the **Add Filters** page.

Add filters

The system sorts clients into Client Groups based on the Client Group filters. The **Add Filters** pages allow you to specify filters based on many criteria such as client IP address, NetBIOS name, operating system, or OU.

Client IP Range

In the **IP From** and **To** fields, enter the start and end of the client IP address range to be sorted to this Client Group. The client IP range filter allows you to specify up to ten IP ranges for each Client Group.

Client NetBIOS Name

In the **Starts With, Contains**, and **Ends With** fields, enter the relevant strings for the criteria based on the letters in the NetBIOS name of the client. The client NetBIOS name filter allows you to specify up to ten criteria for each Client Group.

Client OS

Select the relevant operating systems.

Click **Next** to specify the OU filter.

OU Name

Select the OUs you want to add to the Client Group.

Click **Next** to proceed to the **Select Applications** page.

Select applications

The **Select Applications** page allows you to select applications that will be available to the clients that are sorted to the Client Group. The page displays all the applications in the Secure Global Desktop system. When a user launches a Client Group application, the authentication dialog box opens and the user has to enter valid credentials to launch the application.

Select the applications and click **Next** to proceed to the **Select Printers** page.

Select printers

The **Select Printers** page allows you to select printers that will be available to the clients that are sorted to the Client Group. All the members of the Client Group can print on the Client Group printers in addition to the client printers and the Application Server printers. By default, the page does not display any printers. Click **Find** to display all the printers in all the domains in Secure Global Desktop. Select the printers that you want to add and click **Next** to proceed to the **Select Clients** page.

Select clients

The **Select Clients** page allows you to add existing clients to the Client Group. The client is removed from the Default Client Group and is sorted to the selected Client Group. Dynamic Sorting should be OFF for this. The page displays all the clients from the Default Client Group. Select the clients you want to add to the selected Client Group, and click **Next**.

The **Add Client Group** page displays the choices you make in the Add Client Group sequence. Review the information and click **Add** to add the Client Group to the system.

Update Client Group

Use the **Update Client Group** page to update Client Group information, connection settings, and restrictions on the client group. To update a Client group, from the **Manage>Client Group** page, select a Client Group and click **Update Client Group**. Change the relevant information and click **Update**. All of the properties that appear on this page also appear on the **Add Client Group** page; for more information on these variables, refer to "Add Client Group".

Update filters

You can sort the clients into Client Groups based on many criteria such as client IP address, NetBIOS name, operating system, or OU. Any client that satisfies even one of these conditions can be sorted to the Client Group. You can even add individual clients from any other Client Group to the selected Client Group. The selected clients are removed from the earlier Client Group and moved to the selected Client Group. Dynamic Sorting has to be OFF for this. For more information on sorting to Client Groups, refer to "Use case analysis".

To update filters for a Client Group, on the **Manage>Client Groups** page, select the Client Group you want to modify, and click **Update Filters**. Enter information in the following fields:

Client IP Range

In the **IP From** and **To** fields, enter the start and end of the client IP address range. The client IP range filter allows you to specify up to ten IP ranges for each Client Group.

Client NetBIOS Name

In the **Starts With**, **Contains**, and **Ends With** fields, enter the relevant strings for the criteria based on the letters in the NetBIOS name of the client. The client NetBIOS name filter allows you to specify up to ten criteria for each Client Group.

Client OS

Select the relevant operating systems.

Click **Next** to set the OU Name filter.

OU Name

Select the OUs you want to add to the Client Group.

Click **Next** to set the Client Name filter.

Client Name

Select the Client Names from Default Client Group you want to add to the Client Group.

Click **Next**. Verify the displayed information and click **Update**.

Remove Client Group

Use this option to remove a Client Group from Secure Global Desktop. To perform this function, from the **Manage>Client Groups** page, select the Client Groups you want to remove and click **Remove Client Group**. Verify that the client groups listed are the ones you want to remove and click **Remove**.

Add applications to a Client Group

You can provision applications to Client Groups that exist within Secure Global Desktop. From the **Manage>Client Groups** page, select the Client Groups that will receive additional applications and click **Add Applications**. Select the applications that you want to add and click **Add**. Those applications will now be available to the selected Client Groups.

Remove applications from a Client Group

You can take one or more applications away from client groups that exist within Secure Global Desktop. When you use this action, from the **Manage>Client Groups** page, select the Client Groups and click **Remove Applications**. Select the applications you want to remove and click **Remove**. Afterwards, the selected applications will no longer be available to the Client Groups through provisioning at a Client Group level.

Meanwhile, if the user inherits use of the same applications from a group or OU, then that user will continue to have use of that application until you remove the application from that Group or OU or until you remove the User from the Group or OU that inherits these applications.

Add printers

You can add printers to a Client Group. All the members of a Client Group can print on the Client Group printers in addition to the client printers and the Application Server printers. To add printers to Client Groups, from the **Manage>Client Groups** page, select the Client Groups and click **Add Printers**. By default, the page does not display any printers. Click **Find** to display all the printers in all the domains in Secure Global Desktop. Select the printers that you want to add and click **Add**. The selected printers will now be available to the selected Client Groups.

Set default printer

You can set the default printer for a client group. The default Client Group printer overrides the default printer set on the client for applications launched through Secure Global Desktop. To set

the default printer for a Client Group, from the **Manage>Client Groups** page, select the Client Group and click **Set Default Printer**. The page displays all the printers that have been added to the Client Group. Select the printer that you want to set as default and click **Update**.

Remove printers

You can remove the printers assigned to a Client Group. The removed printer will then not be available to the members of the Client Group through the Client Group assignment. To remove printers assigned to Client Groups, from the **Manage>Client Groups** page, select the Client Groups and click **Remove Printers**. The page displays all the printers that have been assigned to the Client Groups. Select the printers that you want to remove, and click **Remove**.

Add clients

You can add existing clients to a Client Group. The client is removed from its current Client Group and is sorted to the selected Client group. Dynamic Sorting should be OFF for this. To add clients to a Client Group, from the **Manage>Client Groups** page, select the Client Group and click **Add Client**. The page displays all the clients that exist in the Secure Global Desktop system. Select the clients you want to add to the selected Client Group, and click **Add**.

Remove clients

You can either move clients sorted to a Client Group to the default Client Group or you can remove them from Secure Global Desktop. Dynamic Sorting should be OFF for this. To remove clients from a Client Group, from the **Manage>Client Groups** page, select the Client Group and click **Remove Client**. From the **Remove Clients Option** list, select one of the following and click **Next**:

- Move to Default Client Group
- Remove from Secure Global Desktop

The page displays all the clients that are sorted to the selected Client Group. Select the clients you want to remove from the Client Group and click **Remove**.

Manage connection settings

Connection Settings define the manner in which applications are launched in Secure Global Desktop. An administrator can update properties of a connection setting or create new connection settings and apply them to applications. If the administrator permits, the end user (using the Secure Global Desktop Launch Pad) can choose a connection setting to use from among any predefined connection settings.

In all instances, you can add, update, and remove properties for one object. In many instances, you can add, update, or remove properties for many or for all of the instances of an object. For example, for connection settings, you may want to update all connection settings or to delete several connection settings at one time.

This section provides step-by-step procedures to do the following:

"Add setting"

"Update setting"

"Remove setting"

"Select default"

Add setting

The **Add Setting** action allows you to add a new connection setting to the Secure Global Desktop system. To add connection settings, you first need to choose a template, and then specify the settings. For detailed information on templates, refer to "Connection settings templates".

To add a set of connection settings:

1. From the **Manage>Connection Settings** page, click **Add Settings**.
2. Choose a template and click **Next**.
3. Select/Enter the relevant terminal service settings and click **Next**.
4. Select the Secure Global Desktop feature settings and click **Next**.
5. The **Add Setting** page displays the choices you make in Steps 3 and 4. Review the information, and click **Add**.

Following are the fields you need to specify while adding connection settings.

Information

Name

This name identifies this profile.

Description

This description is a free-form field where you can enter information about who requested this profile or who will use this profile.

Allow Users to Select This Connection Setting

Select this check box to make this connection setting available to users. When you select this check box, the users can use the Launch Pad **Options** page to choose this setting for launching applications.

Display

Screen Size

This is the size of the WTS screen in pixels.

Launch Full Screen

This mode launches a Secure Global Desktop application session using the full area of a display screen.

Color Depth

This is the number of distinct colors that Secure Global Desktop displays for applications running under Secure Global Desktop. Color depth is associated with bit depth as it relates the number of bits used for each pixel.

The color depth of an 8-bit setting is 2^8, that is, 256 colors. Secure Global Desktop offers these color depth settings: 8 bit, 15 bit, 16 bit, 24 bit.

Experience

Bitmap Caching

This enables an area in the memory of a user's computer where bitmaps can be temporarily stored.

Enable Compression

This enables you to turn off or to turn on a second level of compression, final bit stream compression. RDP provides the first level of compression. This second level compression does not affect the fundamental RDP compression algorithm.

Secure Global Desktop Features

Seamless Windows

This enables the seamless window feature, which hides the Terminal Server Frame from around your remote applications.

Launch in Existing Connections

This indicates preference to launch new applications in existing connections. Since each terminal connection has a certain amount of overhead associated with it, enabling this feature reduces the amount of resources consumed on the server. It also significantly reduces the application launch time due to the elimination of a second logon.

Reconnect

This allows users to launch new sessions in the same application's disconnected sessions.

Enable Single Port Relay

This enables you to turn off or to turn on the use of a Single Port Relay server for communication.

Logoff Disconnected Connections

This time determines the amount of time a session is allowed to stay in disconnected mode before being logged off.

Logoff Idle Connections

This time determines the amount of time a session is allowed to stay idle (no keyboard or mouse movements) before being logged off.

Client Drive Sharing

Windows 2000

This enables you to turn on or to turn off client drive mapping, which permits an instance of Secure Global Desktop that is running on a Windows 2000 server to operate with a user's local drive.

Windows 2003

This enables you to turn on or to turn off client drive mapping, which permits an instance of Secure Global Desktop that is running on a Windows 2003 server to operate with a user's local drive.

NOTE

IFS data is always transmitted in encrypted form.

Encryption

This enables encryption of data during transmission.

Secure Global Desktop Printer Sharing

Windows 2000

This enables you to turn on or to turn off printer sharing, which permits an instance of Secure Global Desktop that is running on a Windows 2000 server, to print to a user's local or network printer.

Windows 2003

This enables you to turn on or to turn off printer sharing, which permits an instance of Secure Global Desktop that is running on a Windows 2003 server, to print to a user's local or network printer.

NOTE

For Windows 2003 servers, client drive sharing and printer sharing work on CE clients when you select **Native** *as the option in connection settings, otherwise they are off. Windows 2000 settings have no effect on CE client; and client drive sharing and printer sharing are always off for Windows 2000 servers.*

UniDriver (for Secure Global Desktop printing only)

We recommend that you set this feature to "If vendor driver not available" except in certain special circumstances. Refer to the "Secure Global Desktop printing" for a complete explanation of this feature.

NOTE

Printing data is always transmitted in encrypted form.

Encryption (for Secure Global Desktop printing only)

This enables encryption of data during transmission.

Windows 2003 Specific

Enable Serial Ports

This enables you to make your local serial port available in a session. Depending on the policies of your network, local serial port mapping might be disabled for some or all remote connections.

Enable Sound

Audio redirection enables the client to receive locally any sounds that a remote session generates.

Desktop Background

This enables encryption of data during transmission.

Show Contents of Windows While Dragging

This allows you to enable a window to show its entire contents even while you are dragging it across the desktop.

Smooth Scroll

This toggles between smooth scroll, which shows a continuous page of information, and paging, which provides a page-by-page view.

Menu and Windows Animation

This allows you to turn on or turn off menu and Windows animation.

Themes

This enables you to turn on or turn off a feature that influences the appearance of a desktop by providing components that support a specific theme such as a nature theme or a space theme. The components that may reflect this theme include desktop images, screen savers, cursors, icons, or sounds.

Update setting

The **Update Setting** action permits you to change individual values of the properties associated with connection settings.

To update connection settings:

1. From the **Manage>Connection Settings** page, select a connection setting and click **Update Settings**.
2. Change the relevant fields and click **Update**.
3. If you change the Secure Global Desktop Drive Sharing property by enabling or disabling it, you must restart the Secure Global Desktop Monitor services manually. To do this, select **Start>Settings>Control Panel>Administrative Tools>Services>Secure Global Desktop Monitor,** and then select **Action>Start**.

For a description of the fields that appear on this page, refer to "Add setting".

Remove setting

The **Remove Setting** action permits you to delete existing connection settings. If you remove the existing connection settings associated with a user or application, Secure Global Desktop changes the connection settings back to the Secure Global Desktop default settings. You can delete more than one connection settings at a time.

To remove connection settings:

1. From the **Manage>Connection Settings** page, select the Connection Setting you want to remove and click **Remove Settings**.
2. The **Remove Settings** page displays the settings you choose. Click **Remove** to remove the displayed settings.

NOTE

You cannot remove the default connection settings. To remove a connection setting that has been set as default, you must first set another connection setting as default.

Select default

The **Set as Default** action permits you to choose the default connection settings.

To set the default connection settings:

1. From the **Manage>Connection Settings** page, select a connection setting and click **Set As Default**.
2. The **Set As Default** page displays the connection setting you choose. Click **Update**.

Manage Admin Roles

Administrative Roles define the scope of Secure Global Desktop functions and the scope of active directory domains, OUs, or groups that are within the purview of members of the named Admin Role.

In all instances, you can add, update, or remove Admin Roles. In many instances, you can add, update, or remove properties for many or for all of the instances of an admin role. You can also change delegation to alter the group or users who are delegated an admin role. You can also change the groups and OUs the members can control.

This section provides step-by-step procedures to do the following:

"Add role"

"Remove role"

"Update role"

"Update delegated admin group"

"Add delegated admin users"

"Remove delegated admin users"

"Add groups to be controlled"

"Remove groups to be controlled"

"Add OUs to be controlled"

"Remove OUs to be controlled"

Add role

To add an Admin Role:

1. On the **Manage>Admin Role** page, click **Add Role**.
2. The **Add Role** page opens. While adding an Admin Role you need to:
   - "Add role information"
   - "Add delegated admin group"
   - "Add delegated admin users"
   - "Add groups to be controlled"
   - "Add OUs to be controlled"

The sections that follow explain each of these in detail. Select/Enter the relevant information on each page.

Add role information

The **Add Admin Role** page permits you to add individual values of the properties associated with an Admin Role.

Select/Enter the relevant information.

Role Information

These are the role information properties.

Name

This name identifies this Admin Role. Try to make this name descriptive of its responsibilities.

Description

This free-form field permits you to describe information such as the responsibilities or organizational duties of members of this role.

Tasks to Delegate

These are the tasks that you can delegate to an Admin Role.

Monitor Sessions and Servers

Select this check box to assign the monitoring task to the Admin Role.

Provision applications

Select this check box to assign the application-provisioning task to the Admin Role.

Click **Next** to proceed to the **Add Delegated Admin Group** page.

Add delegated admin group

The **Add Delegated Admin Group** page displays the names of all the groups that exist in Secure Global Desktop system and the names of the domains to which these groups belong. You can delegate an Admin Role to only one group. However, you can delegate an Admin Role to many users.

To add a delegated group, select the group and click **Next**. To add a user instead of a group, click **Next** to proceed to the **Add Delegated Admin User** page.

Add delegated admin users

The **Add Delegated Admin Users** page displays the logon name, domain name, and other details of the users that exist in Secure Global Desktop system. To add users, select the users and click **Next** to proceed to the **Add Groups to be Controlled** page.

Add groups to be controlled

This page displays the names of all the groups that exist in Secure Global Desktop system and the names of the domains to which these groups belong. Select the groups you want the members of this Admin Role to control and click **Next** to proceed to the **Add OUs to be Controlled** page.

Add OUs to be controlled

This page displays the names of all the OUs that exist in Secure Global Desktop system and the names of the domains to which these groups belong.

NOTE

The Add OUs To be Controlled page is skipped if no OUs exist in the Secure Global Desktop system.

Select the OUs you want the members of this Admin Role to control and click **Next** to proceed to the **Add Admin Role** page.

The **Add Admin Role** page displays the choices you have made in the Add Admin Role sequence. Review the information and click **Add** to add the Admin Role to the system.

Remove role

The **Remove Role** action allows you to remove existing Admin Roles from the Secure Global Desktop system.

To remove Admin Roles:

1. From the **Manage>Admin Roles** page, select the roles you want to remove and click **Next**.
2. The **Remove Role** page lists the roles you choose. Review the information and click **Remove**.

Update role

The **Update Role** action allows you to change role information and the tasks assigned to a role.

To update an Admin Role:

1. From the **Manage>Admin Roles** page, select the role you want to update and click **Next**.
2. Change the relevant fields and click **Update**. For more information on the fields on this page, refer to "Add role information".

Update delegated admin group

The **Update Group** action allows you to delegate an Admin Role to a different group. The page lists all the groups in the Secure Global Desktop system and the group that is a member is selected by default.

To update delegated admin group:

1. From the **Manage>Admin Roles** page, select an admin role and click **Update Group**.
2. From the **Update Delegated Admin Group** page, choose a group and click **Change**.

NOTE

To remove a group without delegating the admin role to any other group, choose **No Member Group** *in Step 2.*

Add delegated admin users

The **Add Users** action allows you to make existing Secure Global Desktop users, members of an Admin role.

To add delegated admin users:

1. From the **Manage>Admin Roles** page, select an admin role and click **Add Users**.
2. From the **Add Delegated Admin Users** page, select the users and click **Add**.

Remove delegated admin users

The **Remove Users** action allows you to take away control from delegated admin users.

To remove delegated admin users:

1. From the **Manage>Admin Roles** page, select an admin role and click **Remove Users**.
2. From the **Remove Delegated Admin Users** page, choose the users and click **Remove**.

Add groups to be controlled

The **Add Groups** action allows you to add groups that will be controlled by the members of an Admin Role.

To add groups to be managed by an Admin Role:

1. From the **Manage>Admin Roles** page, select an admin role and click **Add Groups**.
2. From the **Add Groups to be Controlled** page, select the groups and click **Add**.

Remove groups to be controlled

The **Remove Groups** action allows you to remove the groups that are managed by an Admin Role.

To remove groups to be managed by an Admin Role:

1. From the **Manage>Admin Roles** page, select an admin role and click **Remove Groups**.
2. From the **Remove Groups to be Controlled** page, select the groups and click **Remove**.

Add OUs to be controlled

The **Add OUs** action allows you to add OUs that will be managed by the members of an Admin Role.

To add OUs to be managed by an Admin Role:

1. From the **Manage>Admin Roles** page, select an admin role and click **Add OUs**.
2. From the **Add OUs to be Controlled** page, select the OUs and click **Add**.

Remove OUs to be controlled

The **Remove OUs** action allows you to remove the OUs that are managed by an Admin Role.

To remove OUs to be managed by an Admin Role:

1. From the **Manage>Admin Roles** page, select an admin role and click **Remove OUs**.
2. From the **Remove OUs to be Controlled** page, select the OUs and click **Remove**.

Management Console Monitor tab

This Monitor tab has a some objects and the overview page, which the section considers.

Overview page

You view this page when you click the **Monitor** tab. This page identifies the types of objects that you can monitor and it provides links to the following pages that monitor each object type.

"Connections"

"Load Balancer"

"Database Connections"

"Relay Server"

"Job Status"

Connections

You access this page to monitor the active RDP connections. From this page, you can trigger four actions.

Disconnect

When you disconnect a connection, the session persists on a server in an active state even though it is no longer active on a client. A user can reconnect to a disconnected session, continue with the session, and the session will appear as if there were no interruptions.

NOTE

A disconnected session continues to use server resources including one Secure Global Desktop license.

For more information, see "Session disconnect and reconnect".

Logoff

When you log off from a session, the session terminates on both the server and the client. This type of session termination is immediate, so any work in progress that has not been saved is lost. You may want to attempt to use the send message function to encourage users to log off before you perform a forced logoff.

Shadow

When you shadow a session, you can view a user's session and share control of the session with the user. You can do this from a remote location. You do this by watching an image of the session from your Web-based Management Console. Session shadowing is a useful troubleshooting tool.

Send message

Use this to send a message to active users.

Load Balancer

You access this page to view the status of servers that are members of the Secure Global Desktop team.

NOTE

You can change the Load Balancer settings from the **Options>Load Balancer** *page.*

The **Load Balancer** page displays the following information.

Application Server

This is the server name.

Running Status

This indicates whether the Application Server is operating. A True value indicates that the Application Server is running.

Server Ranking

This reflects the availability of an Application Server to accept new session loads from the Load Balancer. The ranking value relates to the amount of CPU and memory available, the ranking values are natural numbers, and the Load Balancer prefers to place new sessions on those servers that have the *best* server ratings, where a server with server ranking of 1 is considered the best. Two or more servers can have the same rating. If all the criteria for ranking servers are cleared from the **Options>Load Balancer>Update Options** page, the Server Ranking of each server becomes 1.

Load Balancer Server

This is the Master Load Balancer.

Available Memory in MB

This shows the difference between the total memory and the memory in use by active processes.

Total Memory in MB

This field shows the total memory on the server.

Available CPU Cycles in MHz

This shows the difference between the total CPU cycles and the cycles in use by active processes.

Total CPU Cycles in MHz

This shows the total CPU cycles available on the server.

Server Version

This shows the Operating System.

Number of processors

This shows the number of processors used by the Application Server.

Free Page Table Entries (PTEs)

This shows the availability of the memory page table entries (PTEs). PTEs identify pages of memory called pageframes and the number of PTEs in a system is typically a fixed number. An average PTE count would be in the range of 150,000, so if you see a count that is near 1,000 or near 1,000,000, then you are viewing counts that are out of the expected range.

Page Swaps per Second

This shows the number of memory pages that swap in and out of virtual memory to physical memory. In general, it is positive to swap fewer pages out of the pagefile.

Context Switches per Second

This measures the number of context switches that occur when the kernel or core of the operating system, switches the processor from one thread to another. It is better to have fewer context switches. ISS 5.0 sets the default value for switches per processor and the number of switches can scale proportionately to the number of processors; so, if the ratio of context switches between a single and dual processor were 1:2, this is an acceptable ratio. This does not rule out the possibility of both values being too high.

Processor Queue Length

This measures the length of a processor queue in units of threads, and it helps you identify any bottlenecks. In general, faster CPUs can handle longer queue lengths than slower CPUs.

Database Connections

You access this page to view the status of the database connections with all the servers in the Secure Global Desktop team.

NOTE

You can change your database server settings from the **Options>Database Server** *page.*

The **Database Connections** page displays the following information.

Server Name

This shows the name of the servers in the Secure Global Desktop team.

Primary Database Status

This reflects success or failure for a server in connecting to the Primary Database Server. If there is failure in connecting to the Primary Database Server, you can promote the Secondary Database Server from the **Options>Database Server>Promote Backup DB** page.

Secondary Database Status

This reflects success or failure for a server in connecting to the Secondary Database Server. The page displays this field only if a Secondary Database Server exists in the Secure Global Desktop system.

Relay Server

You access this page to view the load on the Relay Servers in the Secure Global Desktop team. This is an optional role, so you may see no information if you have no Relay Server.

NOTE

You can change your Relay Server settings from the **Options>Relay Server** *page.*

You can view the current load in the following ways

- "View By Server"
- "View By Client"

View By Server

This is the default view. This displays the following information:

Relay Server

This displays the name of the Relay Server.

Number of Connections

This reflects the number of connections made through this port.

Relay Speed (BPS)

This reflects total throughput from all the clients to the Application Servers through the Relay Server. The throughput speed has an inverse relation to the Number Of Connections value. The value appears as bytes per second (BPS).

Available Memory (MB)

This shows the difference between the total memory and the memory in use by active processes. When the Available Memory becomes low on a continuous basis, you may want to consider adding another Relay Server role to one of the servers on your Secure Global Desktop team.

Available CPU Cycles (MHz)

This shows the difference between the total CPU capacity and the capacity in use by active processes.

View By Client

This is the alternate view and it displays the following information:

Client Name

This shows the NetBIOS name of the client computer.

Client IP Address

This shows the IP address of the client computer.

Source Address

This shows the NAT IP address. If there is no NAT, this displays the client IP address.

Relay Server

This shows the name of the Relay Server.

Connection Speed

This reflects throughput from each client to the Application Server. The throughput speed has an inverse relation to the Number Of Connections value. The value appears as bytes per second (BPS).

Job Status

The **Jobs** page shows the status of jobs submitted. For each Job, the page displays the job ID, the object and the corresponding action, the time when the job was submitted, and the status of the job. You can click a **Job ID** to view the details of the job.

Management Console Reports tab

This Reports tab shows several objects on the overview page. You access this page to view the status of these objects in Secure Global Desktop. To access reports on any one of these objects, use the hyperlink.

Most of the reports that you will review have similar operational attributes. For example, a time parameter defines the search period for your query, and to define the search period, you use the **Completed** drop-down list box to select pre-defined time intervals to view. While most of the time intervals concern past sessions, you have one option to query **Still Active** sessions.

NOTE

When you try to download a large-sized report, the download may time-out and an error may be displayed.

On many of these reports, you have an option to filter the reports based on predefined periods. Examples of these options follow:

- Still active: Use this to retrieve information on sessions that are running. This is the only classification that shows active sessions. All other options show completed sessions.
- Last xx hour: Use this to retrieve information on sessions that completed during that interval. For example, use the Last 12 Hours option to see those sessions that completed during the last 12 hours.
- Last xx days: Use this to retrieve information on sessions that completed during the last specified number of days.
- Last week: Use this to retrieve information on sessions that completed during the week. By default, the week is defined as Sunday through Saturday. Alternatively, you can reset this value using the SQL Server Week option.

- Last quarter: Use this to retrieve information on sessions that completed during the last quarter. By default, the quarter is defined by standard calendar quarters such as January through March, April through June, July through September, and October through December.

Overview page

You view this page when you click the **Reports** tab and this summary page provides links to the various report pages.

"Sessions report"

"Applications report"

"Users report"

"Clients report"

"Servers report"

"Audit Log report"

"Product Key report"

Sessions report

This report shows current sessions and past sessions.

All sessions

You can summarize session data by object property (server name, server address, client address, application name, logon name, time started or stopped, and application exit status). An administrator can create and use these views to see data and to reveal information to answer object-specific questions. You can download the Secure Global Desktop data to one of many management information systems where you can perform customized data analysis.

Duration

From this page, you can analyze the duration of sessions. You can answer many interesting questions by sorting, filtering, and selecting on the presented properties.

To use this page, you *must* first complete the boxes on the top of the page to indicate a Minimum (session) Duration, a Maximum (session) Duration, and the time interval to search (for example, during the last week).

To identify applications that are not being used, set the Minimum Duration and the Maximum Duration value to zero, set the time interval to an appropriate period (such as last 24 hours or last 90 days), and click Find.

To determine which applications are used most during a single session, set the Minimum Duration variable to an arbitrarily high value and set the Maximum Duration to another arbitrary but higher value, insert the time interval to search, and click Find. Next, you can sort the table data to aggregate information by entity; for example, you can sort this data by client computer to see how frequently one specific client used a Secure Global Desktop sessions of this duration. Such information might reveal that the longest sessions used over the last 24 hours were X number of minutes each, and it might further indicate that Jane Z and Sumita Y are the only users who regularly use sessions of this duration.

Applications report

This report shows application usage data. You can use the **Completed** drop-down list box to select different time intervals to view, and while most of the time intervals concern past sessions, Secure Global Desktop offers one option to query **Still Active** sessions.

Total time

You can analyze the demand for an application using this report by viewing the number of sessions and the total session time. Because each instance of an application must have a unique name, this report provides information on instances of an application one-by-one. For example, you may have three copies of Microsoft Word (called Word1, Word2, and Word3), so you can see each of these instances individually and assess the discrepancy in the ways they are used. It is important to know that if you see different use profiles it is probably because different user groups or OUs use each instance when the same users are using the same applications

Users

You can see how many users use a specific application. This is meaningful when used with the Total Time report, as you can see a profile where 332 sessions were operated for 10 hours by *1* person, or maybe you would see that 332 sessions were operated for 10 hours by *300* persons. This can help you determine the application usage profiles of the users, and it can help you determine ways to distribute applications that will improve system performance.

Client computers

You can see how many client computers use a specific application. This is meaningful when you use this with the Total Time report, as you can see a profile where 332 sessions were operated for 10 hours by 1 person from *30* different terminals, or maybe you might see a profile where 332 sessions were operated for 10 hours by 300 persons from *1* terminal. This report can help you spot application usage by specific clients.

Peak Usage

This report shows you, during a set amount of time, how many concurrent sessions of the application have run. It also tells you how many times that the application hit that peak number.

The Average Daily Session Count actually displays the mean of the daily peak session counts in the chosen period. This number varies with the size of the period. If you choose a long duration, such as 90 days, then the rounded average number produced could be very small, but it could still be mathematically correct.

Users report

This report shows the number of sessions run by each user during the selected period. It also displays the total time used on Secure Global Desktop Application servers by all the sessions running in that specified period for each user. You can use the **Completed** drop-down list box to select different time intervals to view, and while most of the time intervals concern past sessions, you have one option to query **Still Active** sessions.

Clients report

This report shows the number of sessions run by each client that connected to Secure Global Desktop during the selected period. It also displays the total time used on Secure Global Desktop Application servers by all the sessions running in that specified period for each client. You can use the **Completed** drop-down list box to select different time intervals to view, and while most of the time intervals concern past sessions, you have one option to query **Still Active** sessions.

Servers report

This report shows the number of sessions each server hosted during the selected period. It also displays the total time used by all the sessions running on each server. You can use the **Completed** drop-down list box to select different time intervals to view, and while most of the time intervals concern past sessions, you have one option to query **Still Active** sessions.

Audit Log report

This report displays all the changes/updates made to the Secure Global Desktop system.

Overview

The overview page, the one you see when you select **Reports>Audit Log** permits you to sort columns to find data patterns and it permits you to do a direct access search where you select a time interval, the object type, and the instance's identity. This page displays the audit ID, change type, object type, object name, parameters, logon name, and the log date for each audit log. The audit ID is a unique number that identifies an audit transaction.

Change Type

Use this page to see how the Secure Global Desktop database is changing. During initial deployment, you might expect to see many Add actions and fewer Update and Delete actions.

If a change type displays and you want more information, select **Reports>Audit Log** to display the Audit Log overview page. From the **In** list, select **Change Type**; in the **Look for** field, type the appropriate change value; from the **Completed** list, select a time period and click **Find**.

Object Type

Use this page to see a list of changed object types. If Secure Global Desktop displays a change record for an object that concerns you and you want more information, select **Reports>Audit Log** to display the Audit Log overview page. From the **In** list, select **Object Type**; in the **Look for** field, type the appropriate object type; from the **Completed** list, select a time period; and click **Find**.

Object Name

Use this page to see a list of changed objects. If Secure Global Desktop displays a change record for an object that concerns you and you want more information, select **Reports>Audit Log** to display the Audit Log overview page. From the **In** list, select **Object Name**; in the **Look for** field, type the appropriate object name; from the **Completed** list, select a time period; and click **Find**.

Made By

Use this page to see if a specific user has made a change to the database during the selected time interval. If Secure Global Desktop displays a change record and you want more information, select **Reports>Audit Log** to display the Audit Log overview page. From the **In** list, select **Made By**; in the **Look for** field, type the appropriate user name; from the **Completed** list, select a time period; and click **Find**.

Product Key report

This report identifies the maximum number of people who use Secure Global Desktop concurrently over the time interval you specify. The Peak Reached Count reflects the number of times the Secure Global Desktop users reached the Peak Concurrent Usage value. The Concurrent User Limit reflects the existing Secure Global Desktop concurrent user licenses.

Sometimes, on the product keys report, the Daily Peak Usage appears as 0 and the Peak Reached Count appears as 1. This means that there were no application launches in the specified

period. The minimum number that Secure Global Desktop displays in the peak reached count filter is 1.

The setting made by the administrator to purge the Secure Global Desktop affects the Peak Concurrent Usage report displayed on the **Reports>Product Key** page. For example, if the administrator sets purging for logs older than 30 days, and sets the find filter for the Peak Concurrent Usage on the **Reports>Product Key** page to Last 90 Days, the report displays the result only for last 30 days. This is because all the logs older than 30 days are purged.

Management Console Options tab

Two actions govern all these settings except Database Servers settings, reset options and update options. Use the reset option to set the object properties back to the software manufacturer's default values. These default values reflect a generically optimized value set. This reset capability is important because it allows you to adjust some parameters *without* placing you in a position where you might irrevocably impair your system. Use the update option to customize and tune your system.

Overview page

You view this page when you click the **Options** tab. This is a navigation page, with the following links:

"User options"

"Administrator options"

"Load Balancer options"

"Database Servers options"

"Relay Servers options"

"System options"

User options

Use this page to customize the user interface with Secure Global Desktop.

Launch Pad Web Site

Style

This field governs the way the Secure Global Desktop Application Launch Pad will appear on a user's desktop. This simply affects the initial look of the Secure Global Desktop Application Launch Pad. Choose an option depending on the required look of the Launch Pad.

For more information about styles, see "Launch Pad".

Show Team Name in Banner

Select this check box to display the Secure Global Desktop Team name in the banner on the Secure Global Desktop Application Launch Pad. You can change the team name. To do this, select **Options>System>Update Options** and type the new name in the **Name** field in **Secure Global Desktop Team**.

Support URL

Enter the Tarantella support URL in this field. The **Support** link on the Launch Pad links to this URL. Users use this URL to obtain technical support.

Session Timeout

This property is for the Secure Global Desktop Application Launch Pad and it is used to automatically time out a browser session that has been without keyboard or mouse input from the user for the time specified. The default value is 24 hours. In Internet Explorer 5.5 and higher, after a session times-out, the browser window, the Help window, and the support window (if those are open), close automatically. For other browsers, the user receives a prompt to continue.

SSL Available

Select this check box if you have an SSL certificate. When you set the URL for the Secure Global Desktop Secure Global Desktop Application Launch Pad, you can use either an HTTP or an HTTPS address, but the latter works only when you have an SSL certificate. If you have an SSL certificate and you provide a URL of HTTP, Secure Global Desktop will still use the HTTPS protocol to process passwords. If **SSL Available** is not selected, Secure Global Desktop assumes your site has no security certificate. If you choose HTTPS, Secure Global Desktop processes everything using HTTPS.

Features

Favorites Page

Use this to permit users to use, or to prohibit users from using the Favorites feature of the Secure Global Desktop Application Launch Pad. The Favorites feature permits users to aggregate applications that they use frequently in one special area, which is separate from the area where they store a list of all applications available to them.

Connections Page

Use this to permit Launch Pad users to view the connection page. From the connection page, a user can disconnect or logoff from or reconnect to a session.

Shortcuts

Use this to permit users to use, or to prohibit users from using shortcuts on their desktop.

File Associations

Use this to permit users to use, or to prohibit users from using file associations for their files.

Connections Settings

Use this to permit the users to change Connection Settings through the Launch Pad Web site, Options page.

Re-sort Client into Client Group on each connect

Select this check box to turn Dynamic Sorting ON. When you select this check box, every time the user connects to the Secure Global Desktop system, the user is sorted into a Client Group based on the filters on the current Client Groups.

Client Upgrade

Select this check box to force the client to download the latest version of Tarantella Connection Manager if there is an older version on the client computer. If you select this check box, when the client connects to the Secure Global Desktop system, the client is not allowed to access any page of the Launch Pad, other than the Download page, without client upgrade.

Log on

Allow save password on Client Computers

Select this check box to permit users to use the password save function. If you do not select this check box, then the users will not see the **Automatically Log On From This Computer** check

box on the Secure Global Desktop Application Launch Pad Log On page and on the authentication dialog box.

Reconnect on Launch

Reconnect on launch

Use this to permit users to reconnect to a disconnected session during an application's launch. The disconnect function leaves the session running on the Application Server and terminates it on the client's computer. This behavior permits a user to stop working on a session for a while. If you choose the **Always** option, then the user will be automatically reconnected to the disconnected session, the next time the user launches that application.

Allow user to change this option

Select this check box to give the user the control to set the reconnect on launch preference.

Administrator options

Use this page to customize the Secure Global Desktop administrator interface with Secure Global Desktop.

Console Web Site

Session Timeout

Use this to automatically time-out a console session that has been without data or mouse input from the console for the time specified. Valid values appear in the drop-down list box. The default value is 24 hours. After a session times out, the browser window and help and support windows (if those are open), will close automatically in IE 5.5 and above. For other browsers, the administrator receives a prompt to continue. Secure Global Desktop uses this security feature to shut down a terminal session when it appears that no one is using this session.

Page Row Count

Use this to designate the maximum number of data rows that appear on the Management Console. Valid values appear in the drop-down menu. The default value is 20 rows.

Page Refresh (in seconds)

Use this to specify the interval between updates to real-time data. This feature permits you to view changes to data, automatically, as the changes occur without clicking some sort of update/refresh button. The default value is 30 seconds.

SSL Available

Select this check box if you have an SSL certificate. When you set the URL for the Application Management Console, you can use either an HTTP or an HTTPS address, but the latter works only when you have an SSL certificate. If you have an SSL certificate and you provide a URL of HTTP, Secure Global Desktop will still use the HTTPS protocol to process the user's password processing. If **SSL Available** is not selected, Secure Global Desktop assumes that your site has no security certificate. If you choose HTTPS, Secure Global Desktop performs all processing using HTTPS protocol.

Secure Global Desktop Administrator Group

Secure Global Desktop Administrator Group

This specifies the group of users that are Secure Global Desktop Administrators. This could be any regular domain group. Only the users of this group can log on to the Management Console.

Domain

This identifies the domain in which the administrator group resides.

Domain Type

This identifies a domain as either Active Directory or NT Domain. This value is automatically displayed by Secure Global Desktop system based on the name of the Domain of the administrator group.

Load Balancer options

Use this page to:

- Set thresholds for the Application Server properties.
- Specify which properties you want Secure Global Desktop to consider when Secure Global Desktop computes the availability rating of different servers.

The Load Balancer first considers the threshold limits to eliminate the Application Servers that do not meet the lower limits. Then the Load Balancer calculates the availability rating of the short-listed Application Servers based on the criteria you select.

Performance Counter

You can set lower limits on each of the properties. Additionally, you can indicate if Secure Global Desktop should consider each of these properties in the availability rating calculation for the Application Servers.

Available CPU Cycles

Use this to specify the CPU capacity that must be available for additional tasks. CPU capacity is equal to the total capacity minus the capacity used by active processes. This value appears in MHz.

Available Memory (MB)

Use this to specify the difference between the total memory and the memory in use by active processes that must be available for additional tasks. When the available memory falls to that threshold, Secure Global Desktop adds no more new sessions to that server until more memory becomes available.

Memory Page Table Entries Available

Use this to specify the minimum number of page table entries (PTEs) that must be available for additional tasks. PTEs identify pages of memory called pageframes; and the number of PTEs in a system is typically a fixed number.

Memory Page Swaps

Use this to specify the minimum number of memory pages that swap in and out of virtual memory to physical memory. In general, it is positive to swap fewer pages out of the pagefile.

Processor Queue Length

Use this to specify the minimum length of a processor queue in units of threads. In general, faster CPUs can handle longer queue lengths than slower CPUs. Additionally, identifying an acceptable queue length is a subjective judgment that may vary significantly with variations in the Secure Global Desktop environment.

Processor Context Switches

Use this to specify the minimum number of context switches that occur when the kernel or core of the operating system, switches the processor from one thread to another. It is better to have fewer context switches. ISS 5.0 sets the default value for switches per processor and the number of switches can scale proportionately to the number of processors; so, if the ratio of context switches between a single and dual processor were 1:2, this is an acceptable ratio. This does not rule out the possibility of both values being too high.

Database Servers options

Use this page to add or remove a Backup Database Server, and synchronize or promote it when required. If the Primary Database Server goes down, the system continues to function in read-only mode. Existing users can still launch applications, though you cannot update the Secure Global Desktop system. You can let the system continue in read-only mode or promote the Backup Database to make it the Primary Database and restore normal functionality. For more information, refer to "Achieving database redundancy".

The page displays the Database Server Name and the Database Type. Other properties include a database synchronization trigger, a synchronization interval, and a remove backup database trigger.

Add Backup DB

You can add a backup database to the Secure Global Desktop system to achieve database redundancy.

To add a backup database:

1. From the **Options>Database Servers** page, click **Add Backup DB**.
2. In the **Server Name** field, enter the name of the database server.
3. From the **Session Table Sync Time** list, choose an interval for synchronization and click **Next**.
4. Enter the account details to access the database server and click **Next**.
5. The **Add Backup Database Server** page displays the choices you make. Review the information and click **Add.**

Promote Backup DB

This page displays the name of the Backup Database Server and offers you the option to promote it to the status of primary database. If the Primary Database is online, we recommend that you first synchronize the Backup Database before you promote the backup database. In addition, all the servers in the Secure Global Desktop system should be online when you promote the backup database. For more information, refer to "Promoting the Backup Database Server".

Synchronize DB

The backup database is automatically synchronized periodically with the primary database depending on the synchronization interval. This page allows you to synchronize the backup database with the primary database dynamically. For more information, refer to "Synchronization of the Backup Database Server".

Change Sync Interval

This page allows you to change the database synchronization interval that governs the automatic database synchronization process. For more information, refer to "Synchronization of the Backup Database Server".

Remove Backup DB

This page allows you to remove the current backup database server from the Secure Global Desktop team. This removes the Backup Database Server information from the Primary Database Server.

Relay Servers options

Use this page to customize the Relay Server properties. To add the Relay Server role on a server that is a Web Server, you should disable the SSL port on the IIS or change the IIS port.

Additionally, you may want to place the Relay Server role on more than one server. For more information on adding roles to servers, refer to "Add roles to a server".

Relay Port

This is where you assign the relay port. In general, you might want to use port 443 (SSL) if you have no specific objection to using it as it is generally open for communication in most server-client environments. However, if you cannot use port 443, this port assignment is configurable.

NOTE

If you change the relay port, the existing connections are disconnected. However, the user can reconnect the disconnected sessions from the Launch Pad **Connections** *page, depending on the connection settings.*

Enable SSL Handshake

The SSL protocol generally begins with a handshake phase that negotiates an encryption algorithm, checks the keys (public and private), and authenticates the server to the client.

NOTE

If you reset options, the relay port is set to 443 and SSL handshake is enabled.

System options

Use this page to customize the system configuration values in Secure Global Desktop.

Secure Global Desktop team

Name

This is the name of the Secure Global Desktop Team. This field must not have any special characters. Secure Global Desktop uses this field as the Start menu folder on user desktops. If you delete the Secure Global Desktop Team name, a user cannot launch any applications from the Tarantella Connection Manager tray icon. You can do this to prevent the users on public terminals from using the Launch Pad.

Description

This is a free-form description of the team.

Application Servers

Server Lock Down

You use this feature to prevent any non-Secure Global Desktop based RDP connection from connecting to a Secure Global Desktop Terminal Server unless the user of that connection is a Secure Global Desktop Administrator. Only Secure Global Desktop administrators and local administrators can logon through RDP on a locked down server.

First Letter for Drive Sharing

This shows the first letter, for a list of sequential alphabetical letters, that Secure Global Desktop should use for mapping additional drives. Ensure that these drives are not being used by the Application Servers or for logon scripts.

If you change the First Letter for Drive Sharing property, you must restart the Secure Global Desktop Monitor service manually or reboot the Application Servers. To Secure Global Desktop

Monitor service, select **Start>Settings>Control Panel>Administrative Tools>Services>Secure Global Desktop Monitor,** and then select **Action>Start**.

Last Letter for Drive Sharing

This shows the last letter, for a list of sequential alphabetical letters, that Secure Global Desktop should use for mapping additional drives. Ensure that these drives are not being used by the Application severs or for logon scripts.

If you change the Last Letter for Drive Sharing property, you must restart the Secure Global Desktop Monitor service manually or reboot the Application Servers. To Secure Global Desktop Monitor service, select **Start>Settings>Control Panel>Administrative Tools>Services>Secure Global Desktop Monitor,** and then select **Action>Start**.

NOTE

You can turn off client drive sharing by specifying the first and last letter for drive sharing such that the last letter specified comes before the first letter specified in the alphabetical order. For example, you can specify the first letter as "Q" and the last letter as "M". In this case, none of the client drives will be available to the user in Secure Global Desktop.

Tracing

Log To

Secure Global Desktop can write error, warning, and information messages. This identifies the destination of the message tracing output. You can send the trace messages to the output debugger or the application event log. By default, the trace messages are written to the application event log, and your selection is exclusive. If you use an application event log and you are having a problem, you might want to truncate your application event logs to make room for the output. To view output from output debugger, use a debugger such as Debug View. To view output from Secure Global Desktop to the application event log, you must go to **Start>Settings>Control Panel>Administrative Tools>Event View>Application Log.**

Level

This identifies the type of the logged output. You can choose to log information, warnings, or errors. Each of these parameters will operate correctly with either the output debugger or the application event logs.

Purge Logs

This identifies the destination of the Secure Global Desktop database add, change, and delete actions. You can set up a scheduled event to purge old Secure Global Desktop database logs automatically. Secure Global Desktop can automatically accommodate your log retention requests. The data from these logs appears in reports; therefore, the longer you retain logs, the more information you can collect in reports. However, the data you keep stays in the database; hence, more data occupies more space.

NOTE

The setting made by the administrator to purge the Secure Global Desktop affects the Peak Concurrent Usage report displayed on the **Reports>Product Key** *page. For example, if you set purging for logs older than 30 days, and set the find filter for the Peak Concurrent Usage on the* **Reports>Product Key** *page to Last 90 Days, the report displays the result only for last 30 days. This is because all the logs older than 30 days are purged.*

Sessions Log

These logs track session-level events such as adds, changes, and deletes. Specify a time option for deleting old logs.

Audit Log

These logs track system-level events such as adds, changes, and deletes. Specify a time option for deleting old logs.

Usage Log

These logs track user-, client-, server-, and Secure Global Desktop-level events such as adds, changes, and deletes. Specify a time option for deleting old logs.

Job Records

These logs track the outcome of events that cause a job to run. Other logs show the trigger for these jobs, but the outcome of the jobs appears here. Specify a time option for deleting old logs.

Troubleshooting

What's in this chapter?

This chapter presents information about situations you may encounter and it also explains how to work with any related issues.

Troubleshooting Secure Global Desktop

This section deals with issues related to the following.

"Application-specific issues"

"User-specific issues"

"SSL enabled"

"Secure Global Desktop version"

"Client download"

"Client problems"

"Configuration"

"Diagnostics"

"Disconnect"

"Installation"

"“Join Team” installation fails"

"Domain-specific issues"

"Ports"

"Product keys"

"Local file saving and printing"

"Seamless windows"

"Server problems"

"Server roles"

"Shadowing"

"Shortcuts"

"File associations"

"Windows Terminal Services settings and seamless windows"

"Launch Pad"

"Event Log"

Application-specific issues

This section addresses application-specific issues.

Office XP application remains running after closing it

Issue

You cannot exit your Secure Global Desktop Applications Manager after exiting from an XP application.

Symptom

If you run certain Microsoft Office XP applications through Secure Global Desktop in seamless mode, the application session may not exit after you close the application.

Cause

This is because the Ctfmon.exe program stays running in the session (Ctfmon.exe monitors the active windows and provides text input service support for speech recognition, handwriting recognition, keyboard, translation, and other alternative user input technologies).

Resolution

Microsoft provides an article on how to prevent Ctfmon.exe from running. Excerpts from this article appear below, and you can read the original article on http://support.microsoft.com/support/kb/articles/Q282/5/99.ASP.

To prevent Ctfmon.exe from running, follow these steps.

Step 1. Uninstall Alternative User Input

To uninstall the alternative user input feature, set the installation state to Not Available in Office XP Setup.

For Microsoft Windows Millennium Edition (Me), Microsoft Windows 98, or Microsoft Windows NT 4.0:

1. Quit all Office programs.
2. Select **Start>Settings>Control Panel>Add/Remove Programs**.
3. On the **Install/Uninstall** tab, click to select the Microsoft Office XP product, where Office XP product is the name of the specific Office product that is in use. If you are using a standalone version of one of the Office programs, click to select the appropriate product in the list. Click **Add/Remove**.
4. In the **Maintenance Mode Options** dialog box, select **Add or Remove Features**, and then click **Next**. This displays the **Choose installation options for all Office applications and tools** dialog box.
5. Expand **Office Shared Features**.
6. Click the icon next to **Alternative User Input**, and then select **Not Available**.
7. Click **Update**.

NOTE

If you have multiple Office XP products installed, for example, Office XP Professional and Publisher 2002, you must repeat the preceding steps for each installed product.

For Microsoft Windows 2000 or Windows 2003:

1. Quit all Office programs.
2. Select **Start>Settings>Control Panel>Add/Remove Programs**.
3. In the **Currently installed programs** list, click to select the Microsoft Office XP product, where Office XP product is the name of the specific Office product in use. If you are using a standalone version of one of the Office programs, click to select the appropriate product in the list. Click **Change**.
4. In the **Maintenance Mode Options** dialog box, select **Add or Remove Features**, and then click **Next**. This displays the **Choose installation options for all Office applications and tools** dialog box.
5. Expand **Office Shared Features**.
6. Click the icon next to **Alternative User Input**, and then select **Not Available**.
7. Click **Update**.

NOTE

If you have multiple Office XP products installed, for example, Office XP Professional and Publisher 2002, you must repeat the preceding steps for each installed product.

Step 2. Remove alternative user input services from Text Services

1. Select **Start>Settings>Control Panel>Text Services**.
2. Go to the Installed Services section, and, one by one, select each input item listed, and then click **Remove** to remove the item. Remove most items, all items except the following input service:

   English (United States)- default Keyboard United States 101

Step 3. Run Regsvr32 /U on the Msimtf.dll and Msctf.dll files

1. Select **Start>Run**.
2. In the **Run** dialog box, type the following command:

   ```
   Regsvr32.exe /u msimtf.dll
   ```

3. Click **OK**.
4. Repeat Steps 1 to 3 for the `Msctf.dll` file.

Alternatively, you can perform one of the following procedures:

- You can end the session explicitly using the Log Off option in the Tarantella Connection Manager.
- You can enable Office XP applications in non-seamless mode.

User-specific issues

Add user fails

Issue

Add user with long names fails.

Symptom

On the Console, when you try to add to the Secure Global Desktop system, a user with First Name or Last Name longer than 60 characters, the operation fails and the Console displays an error.

Cause

This is due to the Secure Global Desktop database design.

Resolution

Limit the length of First Name and Last Name of users to 60 characters each in the Active Directory.

User logon fails with “null” error

Issue

Logon to Launch Pad fails with “null” error.

Symptom

The Launch Pad displays “null” error when a user tries to logon to the Launch Pad.

Cause

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

Resolution

Do one of the following:

- Synchronize the domain
- Delete the appropriate user from the console

NOTE

Synchronizing the domain may take a considerable amount of time, so we recommend the second option.

Logon fails

Issue

Logon fails for users with long names.

Symptom

A user with First Name or Last Name longer than 60 characters is unable to logon to the Console and the Launch Pad.

Cause

This is due to the Secure Global Desktop database design.

Resolution

Limit the length of First Name and Last Name of users to 60 characters each in the Active Directory.

SSL enabled

Internet Explorer on Windows 95 client

Issue

If SSL is enabled, Internet Explorer on Windows 95 client fails.

Symptom

When SSL is enabled and a user tries to access the Launch Pad from Internet Explorer on Windows 95 computer, “Launch Pad ID is missing” error is displayed.

Cause

This is because of the way Internet Explorer handles the certificate.

Resolution

1. After enabling SSL on server and adding proper certificate on server, when you try to visit the Launch Pad in browser on the client you will get a dialog box asking for certificate authority.
2. Click **View Certificate**.
3. On the **Certificate** dialog box you will have the option for adding this certificate to the Root authority. By selecting that add certificate to the root authority.
4. Access the Launch Pad after adding the certificate to the root authority.

Secure Global Desktop version

Locating the version number for the Secure Global Desktop software

Issue

A user would like to find the version number for his Secure Global Desktop software.

Symptom

N/A

Cause

N/A

Resolution

When the user places the cursor on the Tarantella Connection Manager tray icon and there are no active connections, the tool tip displays the version next to the program name.

Within the browser interface to Secure Global Desktop, there is an “About” link. This link is available on both the Secure Global Desktop Application Launch Pad and the Management Console. The resulting page contains the following information:

- Company name for which the product is registered
- Product Key
- Build
- Version
- Technical Support contact number
- Sales Support Center contact number

NOTE

In the event that you need the product version information and the browser interface to Secure Global Desktop is not available, you may retrieve the version information from Secure Global Desktop’s SQL Database.

---

1. From your SQL server, launch the SQL Enterprise Manager.
2. Expand the view so you can see the list of databases.
3. Expand the view for the CanaveralDb database.
4. Select **Tables**.
5. Right-click the table named **GBLConfiguration**.
6. Select **Open Table**, and then the option to **Return all rows**.
7. Scroll down, and look at the Value for the record labeled VersionNumber.

Locating the server-side Tarantella Connection Manager version

Issue

The systems administrator would like to determine the Tarantella Connection Manager version that his Secure Global Desktop system is delivering to the end user.

Symptom

N/A

Cause

N/A

Resolution

1. From the SQL server, launch the SQL Enterprise Manager.
2. Expand the view to see the list of Databases.
3. Expand the view for the CanaveralDb database.
4. Select **Tables**.
5. Right-click the table named **GBLConfiguration**, select **Open Table**, and select **Return all rows**.
6. Scroll down, and look at the Value for the record labeled “ClientManagerSetupVersion”

Active directory

Application list refresh based on group membership

Issue

Application list not refreshed correctly on Launch Pad after change in group membership across domains.

Symptom

If a user's group membership is changed across domains and the **refresh application list** link is clicked, the application list does not display the correct application list according to the changed membership.

Cause

This is due to the AD Replication latency across domains. Universal Groups are updated first in Global Catalog (GC) and then the changes replicated to each domain. The time to replicate depends on topology as well as the replication schedule set by the system administrator. Typically, the time taken would be about 15 minutes.

Resolution

Due to the AD architecture, the updated application list will be displayed after replication takes place as per the replication schedule set by the system administrator and the topology. The system administrator can also do manual synchronization. The change in group membership is then reflected immediately.

Client download

Considering administrative rights for the client computer

Issue

Does a user need to have administrator privileges on the client computer in order to launch Secure Global Desktop applications?

Symptom

N/A

Cause

N/A

Resolution

No, to launch applications a user need not have administrative rights on the client computer.

A user must have administrative rights on the client computer to *install* Secure Global Desktop's client software. However, after the installation is complete, no user operations require administrative rights.

Understanding the contents of the client computer's download

Issue

What files will a user download to a Tarantella Client computer?

Symptom

N/A

Cause

N/A

Resolution

The user downloads SGD-TSE-Client400.exe. It shows up as Tarantella Connection Manager in the Add\Remove programs.

Understanding the size of Client components

Issue

How large is the Tarantella Client?

Symptom

N/A

Cause

N/A

Resolution

The Tarantella Client is about 5 MB.

Understanding why a user cannot log on to the Secure Global Desktop Launch Pad

Issue

A user who does not have administrative privileges goes to the Secure Global Desktop Launch Pad and downloads the Tarantella Client software; however, this user is unable to install the software on the Client.

Symptom

When attempting to download and install the Client from the Secure Global Desktop Applications Launch Pad, the process fails and the user receives a warning.

Cause

The user does not have the administrative privileges that are required to install the client.

Resolution

To install the Tarantella Client software, the user must have administrative privileges on the client computer. If you cannot grant administrative privileges to the user of the client computer, you have these options:

- You may logon to the client computer as an administrator and install the client
- You may push the Secure Global Desktop install to the client using a program such as the Windows 2000 IntelliMirror.

After you install the software on the Client computer, the user can log on to the client computer and perform all normal user operations using the Secure Global Desktop Launch Pad Web pages. For normal operations, a user does not need administrative privileges.

Corrupt installation detected error

Issue

User gets Install error 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 the user gets an Install error sometimes.

Cause

This may happen if the user tries to run the program from its current location.

Resolution

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

Client problems

Application Server's screen saver appears on the client computer

Issue

A screen saver appears on the client computer during an active session.

Symptom

The client computer that is both connected to an Application Server and has an active session running on it, displays a screen saver.

Cause

There is a screen saver set on the Application Server.

Resolution

Do not set a screen saver on any Application Server.

Client OS support

Issue

What client operating systems do you support?

Symptom

N/A

Cause

N/A

Resolution

Secure Global Desktop supports Microsoft Windows ® Terminal Services clients that run the following operating systems:

- Windows NT 4.0
- Windows 95
- Windows 98
- Windows Me
- Windows 2000 Professional
- Windows 2000 Server
- Windows XP
- Windows Server 2003

Secure Global Desktop supports Wyse Windows Based Terminals clients that run the following operating systems:

- Windows NT Embedded 4.0
- Windows CE 2.12
- Windows CE 4.x (CE .NET)

Application launch hangs at Connecting to Application Server message

Issue

Client cannot launch applications.

Symptom

When launching an application, the client hangs at the message box stating “Connecting to Application Server…”

Cause

Sometimes, the system directs an error message or information message to the desktop before an application launches. If the user is running Secure Global Desktop with seamless windows enabled for this application and an administrator has disabled the “Show Logon Dialog During

Seamless Windows Launch" option from the Management Console, the message will not be visible to the user and user's application appears to hang.

Resolution

To test if a user is experiencing the described behavior, disable seamless windows for the application in question, and ask the user to attempt the application launch again. If the application launches successfully without seamless windows enabled, do one of the following:

Re-enable the Show Logon Dialog During Seamless Windows Launch as one of the Launch Pad properties in the Management Console. Do so by clicking the **Manage>Connection Settings>Update Connection Options**. Scroll down Seamless Windows drop-down list box and select **Except During Logon** for the Seamless Windows option. This action will cause an error or message dialog box to be visible to the user before an application launch and the application can still run in seamless windows mode.

If a user still receives an error message before an application launch, have the user correct the error, and launch again.

Support for dial-up connections

Issue

Will an application launch if a user connects via a dial-up connection?

Symptom

N/A

Cause

N/A

Resolution

Yes, Secure Global Desktop does support dialup connections.

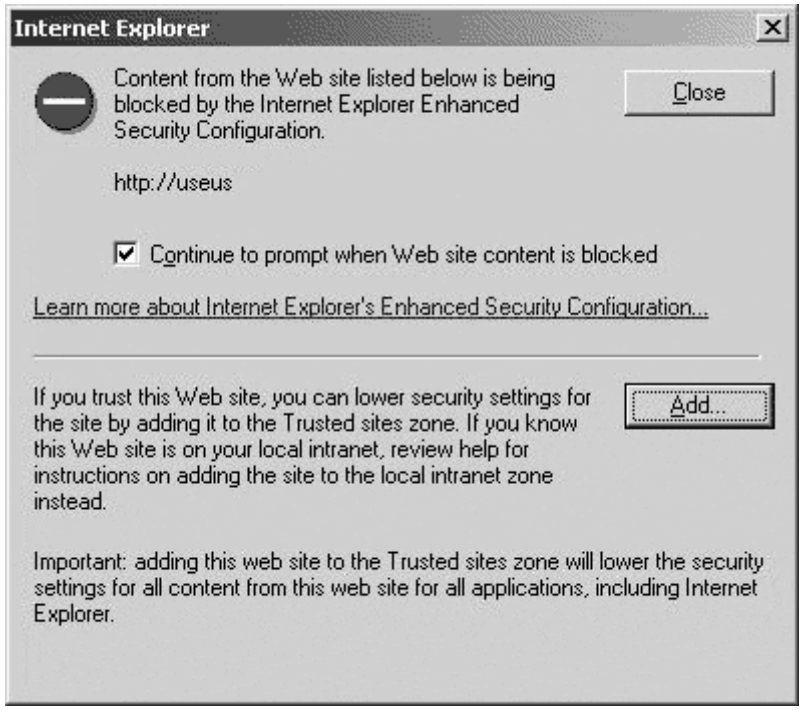
Launch Pad Favorites page is not displayed

Issue

Launch Pad Favorites page is not displayed after logon.

Symptom

Using Internet Explorer 6.0 on Windows 2003, when a user accesses the Launch Pad Web site, the following window appears.



The user clicks **Close** and is 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 the user accesses the Launch Pad Web site to add the site to the Trusted Sites list.

NOTE

This problem also occurs when a user launches a provisioned Internet Explorer application, on an Application Server with Internet Explorer Enhanced Security Configuration setting. You should then implement the resolution on the Application Servers.

Painting issue with Microsoft's Office Assistant

Issue

Microsoft's Office Assistant does not behave properly for an application launched through Secure Global Desktop when the Client is running in seamless windows mode.

Symptom

When using an application from Microsoft's Office suite, the Office Assistant may launch correctly; however, if you move the Office Assistant, the system will not repaint it.

Cause

We are aware that this is an issue and are currently working on a resolution.

Resolution

Please disable Microsoft's Office Assistant. You can do this by uninstalling the Office Assistant from the Application Servers.

Application launch fails with Server Not Available error

Issue

Users are not able to launch any applications through Secure Global Desktop.

Symptom

When attempting to launch applications through Secure Global Desktop, users receive the following error message: "No application servers are available to process this request".

Cause

The application delivery servers may not be talking to the Load Balancer or the load limits on your application servers may be hitting a threshold.

Resolution

1. Check the status of the Application Server.
2. Check to see if the Application Server is available by logging on to the Management Console.
3. Select **Monitor>Load Balancer**. Look for the Application Server in question. Does it exist? Are all of the values are set to zero? Did the Secure Global Desktop Services Monitor service stop or hang?
4. Restart the Secure Global Desktop Services Monitor service on the Application Server.
5. If the Monitor service does not restart, then reboot the computer.
6. Attempt to launch an application.
7. If the same error occurs, restart the Load Balancer and Load Balancer Assistant services, which are located on the Web Server, and attempt to launch an application once more. If you have installed the Load Balancer role on other computers, restart the aforementioned services on those computers as well.
8. Check the load limits for that server. By default, Secure Global Desktop enables load limits on the Secure Global Desktop system.

9. Check to see if the server is at its load limits. To do this, select **Monitor>Load Balancer**, and then select **Options>Load Balancer**. Note the values for the limits in both areas and compare the values. If the server is running at the available memory or CPU capacity threshold, applications will not launch until more resources become available. To affect a change immediately, you can disable or change the load limits. However, you may want to monitor this server intermittently to see that these changes have not adversely affected this server's ongoing performance.

Copy and paste large files or bitmaps

Issue

An application may fail if you copy and paste a large bitmap or a large file or bitmap to an application run by Secure Global Desktop.

Symptom

The application that receives the pasted data may fail.

Cause

This is an RDP issue.

Resolution

Check the Microsoft site to see if a patch is available.

Desktop Windows commands and seamless windows mode

Issue

Some Menu items, such as Minimize All / Tile, do not have any effect on sessions that are running under Secure Global Desktop Seamless Windows.

Symptom

If a user invokes the Taskbar's Context menu by performing a right click on the Windows shell's taskbar, then Windows generally launches the Windows arrangements menu, which shows the following types of item/actions: Cascade windows, Tile Windows Vertically, Tile Windows Horizontally, Minimize All windows, and Undo Tile.

However, the above Menu Item has no effect on a window that is created as a Seamless Secure Global Desktop session.

Cause

This is by design.

Resolution

N/A.

Removing user name and domain from Wyse terminals

Issue

User name and domain information appears on all terminals.

Symptom

When pushing a Wyse terminal configuration to multiple devices using Rapport, the user name and domain used to configure the master device is replicated to all the devices.

Cause

The Rapport software is configured to retrieve all the settings from the Wyse device. This provides the administrator with the utmost flexibility in what gets pushed down to the other devices. As pa art of this retrieval, the connection setting information is also pulled out. As a result, when an unedited configuration is pushed to other devices, the device inherits the settings of the master device.

Resolution

Remove the domain and user information from the file that gets pushed to the terminals. This is a one-time step that you have to follow for all connections before you push all the connection information to the terminals.

1. Retrieve the terminal configuration from the master Wyse terminal using Rapport.
2. Backup the file, settings.reg located in the GetCECFG folder.
3. Edit the settings.reg file.
4. Scroll down to the section beginning with HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBT\Clients\Registration\Canaveral\Connections.
5. In the parameters section, you will see tags called UserName= and DomainName=.
6. Edit these entries for all the connections. If you want to remove the user name just delete the username (until the ;). Repeat for the Domain. Alternatively, you can enter a different username/domain combination.
7. After you have completed this for all the connections, save the file to the SendCECFG folder on the Rapport server.
8. Push the setup file to the devices using Rapport.

Non-existent printer issue

Issue

Series of error messages.

Symptom

When an application is launched, a series of message boxes may be displayed on the Application Server before the application opens.

Cause

The client computer may have such printers installed that are not currently available or are non-existent.

Resolution

Delete the printers that do not exist and verify that all other printers are available.

Second application launch from CE device

Issue

Second application launch fails on CE device.

Symptom

An application launch from a CE client fails if there is already a Secure Global Desktop session launched through SPR.

Cause

This is due to the limited memory of CE devices.

Resolution

Launch Windows Desktop from the CE device as the first application and then launch other applications from the launched Windows Desktop session.

Configuration

Specifying a command parameter for an application

Issue

You need to specify an argument, or command parameter for the application.

Symptom

To launch successfully, an application requires a special launch command.

Cause

N/A

Resolution

Specify the argument in the Command Line Parameters section of the Launch Settings section for the application in question. To do this, select **Manage>Applications**, select the relevant application, click **Update**, enter the command string in the Command Line Parameters box, and click **Update**.

Disconnecting a user versus logging off a user

Issue

Is there a difference between disconnecting a user and logging off a user?

Symptom

Yes, there is a difference. From the Management Console you can enable a user to disconnect from a session and permit that user to reconnect to a previously disconnected session. Associated with this function is the ability for a Secure Global Desktop administrator to disconnect or log off users who use Windows Terminal Services. An administrator may want to terminate an inactive session for the following reason; when a user disconnects a session, that user may forget to reconnect or log off from the session. This persistent connection continues to use Secure Global Desktop resources; it uses one Secure Global Desktop and one WTS license.

Cause

Disconnecting a user keeps the application running on the server so that the user can re-connect to his or her previous session. If you log off the session, the application terminates on both the Client and the server, and the session releases any licenses that it held.

Resolution

To maximize the use of existing licenses, the Secure Global Desktop administrator may wish to prohibit users from disconnecting sessions. To do this, a Secure Global Desktop administrator should select **Options>User>Update Options**, and set the **Reconnect On Launch** property to **Never**, and clear the **Allow User To Change This Option** check box.

Configuring published addresses for use with private/public networks

Issue

The customer wishes to have client computers on both private and public networks use the same set of Secure Global Desktop Servers.

Symptom

Client computers are not able to connect to Secure Global Desktop when using a private or public IP address for the Published Address entry (for the Application Server in the Management Console).

Cause

This is consistent with how most network devices work when dealing with a network that is using Network Address Translation (NAT) devices (for example, Cisco Pix Firewalls).

Resolution

Configure the Published Address to use a DNS name instead of an IP address. To do this, perform the following:

1. Identify two DNS Servers that you want to use: one public DNS Server and one private DNS Server.
2. Identify the public IP addresses to use. This number depends on the number of Secure Global Desktop servers.
3. On any network device (for example, firewall), validate that the required inbound TCP ports are open for the public IP addresses identified.
4. Identify the DNS names for the public IP addresses that were identified in Step 2 (for example, canapp_server1.<company>.com).
5. On the public DNS server, create an “A” record for each DNS name and relate it the public IP address reserved for the Secure Global Desktop server. Repeat this process for any other servers.

6. On the private DNS Server, create a Primary DNS zone that relates to the public zone used in Step 4 (for example, <company>.com).
    - If you are using a Windows 2000 DNS Server, open the DNS MMC snap in.
    - For the Forward Lookup Zones, right click and select **New Zones**.
    - Check Standard Primary Zone and click **Next**.
    - Type in the zone name and click **Next**.
    - Click **Next** again, and then click **Finish**.
7. On the private DNS server create an “A” record for each DNS name and relate it the private IP address of the Secure Global Desktop Server.
    - Click on the New Zone that you created.
    - Right click and select **New Host**.
    - Enter in the name (e.g. canapp_server1) and the private IP address.
    - Create an “A” record for all the other Secure Global Desktop servers in the same manner.
    - Configure your Secure Global Desktop Server to use the Published Address by logging on to the Management Console to do the following:
        - Select **Manage>Servers**, select the server you wish to modify, and click **Update Server**.
        - In the **Published Address** field, enter the DNS name for this server (e.g. canapp_server1.<company>.com).
        - Click **Update**.
        - Repeat the process for any other servers.

Running Secure Global Desktop with an ISA server

Issue

When running Secure Global Desktop behind an ISA server, it appears that data move to the internal address only.

Symptom

A user cannot download the ActiveX Client and this prevents the user from logging onto the Launch Pad. In addition, if the user is able to log on, that user accesses a URL that uses the internal address.

Cause

You need to configure ISA and Secure Global Desktop to use the correct address.

Resolution

You need to configure the following:

1. You should use a Fully Qualified Domain Name (FQDN) as your published address for your server. Externally, this name resolves to your outside IP address, and internally, this name resolves to your inside IP address.
2. You need to configure your ISA server to “Send original host header instead of internal name.”

- Here are the steps to configure this. Please refer to the ISA documentation if you have any questions about setting this up.
- Open up the ISA console.
- Under publishing, create a new web publishing rule
- Under the Action tab, select **Send Original Host Header**.

3. You need to configure your ISA Server to have our required ports open, so you need to setup server publishing rules for the following ports 80, 4660, and 3389.

Cannot locate application executable when launching an application

Issue

The system cannot find the executable for the application the user is attempting to launch.

Symptom

When launching an application, the user receives the error statement “Cannot find the file ‘<path>\<application name>.exe’ (or one of its components). Make sure the path and filename are correct and that all required libraries are available.”

Cause

The application’s executable path is not correct for the server you have chosen.

Resolution

Modify the application path in the Management Console so that the application has the correct path. Make sure that the path specified corresponds to the server you have selected for this application. For example, if you have chosen `c:\temp\my.exe` as the application path and server1 as your server, then make sure that `c:\temp\my.exe` is physically located on server1.

Installing Secure Global Desktop on a domain controller

Issue

Domain controllers have different security settings.

Symptom

When installing all the roles on a Secure Global Desktop server, you can only run an application as a Domain Administrator.

Cause

Domain Controllers do not allow Log On Locally rights; you need to give users Log on Locally rights in order to use Terminal Services on a Domain Controller.

Resolution

To allow a user to log on locally to a domain controller:

1. Select **Start>Programs>Administrative Tools>Domain Controller Security Policy**.
2. Expand **Windows Settings>Local Policies**.
3. Click **User Rights Assignment**.

4. Give **Log on Locally** rights to the groups you want to have access.

To have this policy to take affect immediately:

You will need to type in the following command at a command prompt:

```
secedit /refreshpolicy machine_policy /enforce
```

After installing the Application Server role, the server “blue screens”

Issue

The Application Server reserves some default drives to use for client drive mapping.

Symptom

After installing of the Application Server Role, the server “blue screens”.

Cause

Secure Global Desktop Application Server Role, by default, reserves drives I through Q for use with client drive mapping. If your operating system is on those drives, then the server will “blue screen” when the Secure Global Desktop Monitor Service starts up.

Resolution

1. Boot into Safe Mode.
2. Change the Secure Global Desktop Services Monitor to start manually and then reboot.
3. Log on to the Management Console.
4. Select **Options>System>Update Options**.
5. Change the Secure Global Desktop Drive Sharing: **First Letter for Drive Map** and **Last Letter For Drive Map** to drives that your server is not already using, such as “Q” for the first letter and “W” for the last. This is assuming that you are not using these letters for your drives already. If you are using any of these drives, select a different, unused drive sequence.
6. Start the Secure Global Desktop Monitor Service.
7. If the system does not blue screen again, change your service to start up automatically.

Time-outs when using the Management Console

Issue

In large domains, it can take a while to return all the information. The default settings of the Secure Global Desktop time-out variables are 90 seconds for ASP pages and 60 seconds for COM+ components.

Symptom

When using the Console, you get a time-out error.

Cause

When you have large domains, the administrator's request could time-out, as the default time-out for the ASP pages is 90 seconds and 60 seconds for the COM+ components.

Resolution

To resolve this, increase the time-outs for the ASP pages and COM+ components:

1. Select **Start>Settings>Control Panel>Administrative Tools>Internet Services Manager**.
2. Expand the Default Web Site, right-click on the Console entry and select **Properties**.
3. Click the **Directory** tab on the **Console Properties** window, and click **Configuration**.
4. Click the **Application Options** tab.
5. Increase the value of **ASP Script Timeout**, and click **OK**. Try **120** seconds, and if time-out behavior still occurs increase once again.

To increase the time-out for the COM+ components:

1. Select **Start>Settings>Control Panel>Administrative Tools>Component Services.**
2. Expand **Component Services>Computers>My Computer>COM+ Applications>Secure Global Desktop Management Engine>Components**.
3. Right click on **CuDataAccess.Modifier.1** and select **Properties**. Click the **Transactions** tab.
4. For the Transaction time-out, increase the time (to say, 120). Do this for each of the following and set each of the following to the same time value:
   - CuLogic.ApplicationManager.1
   - CuLogic.ConfigManager.1
   - CuLogic.DomainManager.1
   - CuLogic.LicPolicyManager.1
   - CuLogic.MaintenanceManager.1
   - CuLogic.OrgManager.1
   - CuLogic.ProdKeyMgr.1
   - CuLogic.ServerManager.1
   - CuLogic.UserManager.1

To manage more than 1000 users:

When you manage more than 1000 users in a domain, you may time-out for because the process exceeds the time-out limit or the query exceeds the page selection limit. When you must select more than 1000 users, consider selecting these users by proxy. To do this, select the groups to which these users belong and make the application assignments at the group level.

Cannot add groups from other domains

Issue

Secure Global Desktop exists in an NT 4.0 Master/Resource Domain configuration. However, the administrator is unable to add users and groups from the Master Domain into the Secure Global Desktop system.

Symptom

N/A

Cause

The reason that you cannot add users from the Master Domain is because the Secure Global Desktop Service account does not have rights to read objects from the Master Domain.

Resolution

To correct this problem, you have these options:

- You can establish a one-way trust
- You can establish a two-way trust
- You can deploy Secure Global Desktop so that the Secure Global Desktop Service account exists in the Master Domain.

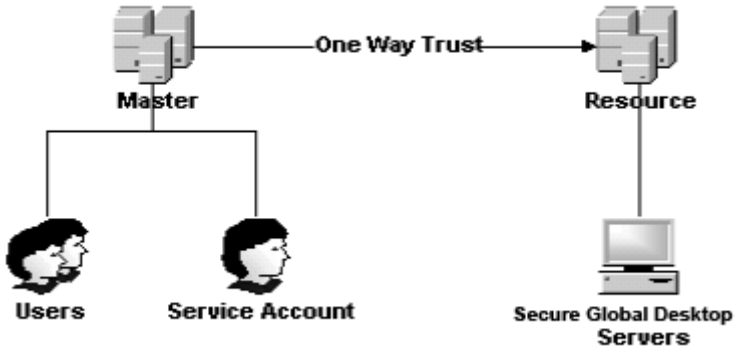


FIGURE 18. Establish a one-way trust

NOTE

The Secure Global Desktop Service account must have administrative rights on Secure Global Desktop servers in the Resource Domain, and users in the Master Domain must have logon rights on the Application Servers in the Resource Domain.

Changing the User Profiles storage location on an Application Server

Issue

The location for user profiles in Windows 2000 is, by default:

```
%SystemDrive%\Documents and Settings
```

Underneath this folder, each user will have a sub-folder that contains desktop items, Start Menu items, temp folders, etc. In some cases, in order to keep users from accessing the system drive, administrators may want to change the location for user profiles.

Symptom

N/A

Cause

N/A

Resolution

Two registry entries determine the path for the local Default User profile.

The following registry entry sets the name of the directory into which the system stores the Default User profile:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\ProfileList\DefaultUserProfile Reg_Sz Default value
="Default User"
```

The following registry entry sets the path in which the Default User folder is stored:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\ProfileList \ProfilesDirectory Reg_Sz Default value
="%SystemDrive%\Documents and Settings"
```

Configuring SSL for the Management Console and Launch Pad sites

Issue

Configuring the Management Console and Launch Pad sites for SSL.

Symptom

When viewing the Management Console or Launch Pad sites, the user will get the following error message.

“You're about to be redirected to a connection that is not secure."

Cause

This is normal behavior when an SSL Web site is about to redirect you to a non-https URL.

Resolution

You need to update the CanaveralDB to support SSL. You do this from the Management Console. In the Management Console, click **Options>Administrator** and select the **SSL Available** check box and click **Update**. Next, click **Options>User** and select the **SSL Available** check box and click **Update**.

Supporting multiple domains

Issue

The network in which you deploy Secure Global Desktop contains multiple domains. How can users access Secure Global Desktop if the Secure Global Desktop install was to another domain?

Symptom

The Management Console only displays users, groups, servers, or OUs from one domain, the domain used for the Secure Global Desktop install.

Cause

You need to add other domains to the Secure Global Desktop system.

Resolution

Verify or create a trust between the Secure Global Desktop domain and the new domain that you will add to the Secure Global Desktop system. This trust can be one way or two ways.

- If the domain exists in the same Active Directory Forest, the trust already exists as a transitive trust.
- You may need to change the lmhosts, WINS, or DNS entries to establish trusts properly across networks that consist of multiple subnets.

The COM+ user account that was set during the Secure Global Desktop installation must have Administrator rights within the domain.

Adding another domain into the Secure Global Desktop system:

1. Log on to the Management Console.
2. Click **Manage>Domains>Add Domain**.
3. In the **Domain Name** field, enter the domain NetBIOS name. Secure Global Desktop will add the Domain Type and Domain DNS, as appropriate.
4. Click **Next**, and then click **Add**.

You can now add Domain information (pertaining to objects such as groups and OUs) from the second Domain, and you can provision applications.

Diagnostics

Settings Test failure

Issue

Terminal Server selects the **Use connection settings from user settings** check box by default.

Symptom

You may receive the following error message:

Tarantella Client unable to test the settings correctly.

Cause

If you have cleared this check box, you may receive an error when you run a Settings Test from the Management Console (**Manage>Servers (select a server)>Diagnose Server>Settings Test**).

Resolution

1. Click **Start>Settings>Control Panel>Administrative Tools>Terminal Server Configuration>Connections**.
2. Right click **RDP-Tcp** and select **Properties** from the shortcut menu.
3. Click the **Client Settings** tab and then under the Connection area, select the **Use connection settings from user settings** check box.
4. Click **OK** to save your settings.

Disconnect

Reconnecting a session after a client loses its network connection

Issue

A client computer with Secure Global Desktop sessions running loses a network connection to the Application Server, and the user wishes to reconnect to the disconnected sessions.

Symptom

The sessions do not show up in the Disconnected Sessions list in the Launch Pad Connections page.

Cause

This problem can occur after an abnormal connection loss. For example, WTS may take some time to disconnect a session when the network cable is pulled. However, once the WTS server notifies Secure Global Desktop of the disconnected session, Secure Global Desktop will change the session status and reflect the new state to the user.

Resolution

It is not possible to change the current behavior. The user must wait a few minutes, and the user can reconnect to his or her previous session. Users can contact a Secure Global Desktop administrator, the administrator can watch for the session status change (**Monitor>Sessions** and see Session State), and then notify the user when the session state changes to disconnect.

Installation

Cannot upgrade Secure Global Desktop

Issue

A systems administrator cannot upgrade an existing Secure Global Desktop installation.

Symptom

When you are upgrading the Secure Global Desktop software, installation fails to run and aborts displaying the following message box.

Cause

The administrator has logged on to the server computer as a non-domain user.

Resolution

The user who is performing an upgrade must log on to the computer where Secure Global Desktop is installed as a domain user. Additionally, the user who is installing Secure Global Desktop, at minimum, must have administrative rights on the local computer.

“Join Team” installation fails

Issue

The Join Existing Team installation sequence fails.

Symptom

The Join Existing Team installation sequence displays “Logged in user is not part of the Secure Global Desktop Administrator group” error and fails.

Cause

This happens if the Secure Global Desktop Administrator Group name contains double byte characters.

Resolution

The administrator can add servers to the Secure Global Desktop team using the Console. It does not affect the Console functionality in any way.

Load balancing

Explaining load balancing

Issue

How does Load Balancing work?

Symptom

N/A

Cause

N/A

Resolution

We use the available CPU and memory in our load-balancing algorithm to determine the Server Rating. The better the Rating, the more likely it is that the particular server will receive the next application session. Rating=1 is the best rating.

You can view this rating by clicking **Monitor>Load Balancers** and viewing the **Server Rating** column.

If you would like to disable or change the default settings for the load-balancing scheme, click **Options>Load Balancer**. Select **Update Options** and change the number of Processor Available Cycles and/or one or more of the Memory values that Secure Global Desktop uses in its algorithm. Alternatively, you may wish not to use load limits, and you would do this from the same by clearing the relevant check boxes.

NOTE

Currently, load limits can be set system wide. They are not set on a per application server basis.

All application sessions are being sent to one server

Issue

Secure Global Desktop is sending all application sessions to the same server.

Symptom

N/A

Cause

The other servers may be offline or that server may have a higher server rating than the other servers.

Resolution

Look at the server rating. Click **Monitor>Load Balancer**. Look at the Online Status for the server, and if a server is offline, then look at the server and either restart the Secure Global Desktop Monitor Services service or reboot the computer.

If the rating is higher on the server that is receiving the application delivery requests, then this is the expected behavior.

Explaining load limits

Issue

How does an administrator use load limits?

Symptom

In the Management Console, if a Secure Global Desktop administrator clicks Options and then Load Balancer, entries exist for six types of load limits.

Cause

N/A

Resolution

If a systems administrator wants an Application Server to stop serving out applications when its available load hits some threshold, then the administrator can use this feature. Use these limits to ensure that no server becomes too busy to provide good service to the users.

Launching spawned applications

Issue

Applications can spawn other applications. Where do these new applications run?

Symptom

N/A

Cause

N/A

Resolution

The spawned applications run on the server where the original application runs.

Domain-specific issues

Add Active Directory domain running on Windows Server 2003 from a different forest fails

Issue

Unable to add trusted Active Directory domain running on Windows Server 2003 from 2K domain.

Symptom

Unable to add a trusted Active Directory domain running on Windows Server 2003 to a Secure Global Desktop team in an Active Directory domain when the two domains are in different forests.

Cause

Even when there is two-way trust between domains, an Active Directory domain running on Windows Server 2003 does not allow any information to be read by a computer that belongs to a domain in a different forest. This is the result of the default security settings on a Windows Server 2003 domain controller.

Resolution

If you want to use an Active Directory domain running on Windows Server 2003 in a Secure Global Desktop team, make sure that the computer where Secure Global Desktop Web Server role is installed is a part of the same domain, or is a part of one of the domains in the same Windows Server 2003 forest.

Ports

Changing the ports on which Secure Global Desktop runs

Issue

Systems administrators want to be able to specify which ports Secure Global Desktop runs on.

Symptom

N/A

Cause

N/A

Resolution

At this time, ports are not configurable.

Identifying ports that must be opened on the client side for Secure Global Desktop

Issue

Client computers are not able to connect to any Secure Global Desktop servers.

You must open specific ports on the client side for Secure Global Desktop.

Symptom

All connection attempts time out.

Cause

You need to open certain TCP ports to be outbound from the client to the server.

Resolution

Confirm that the following TCP ports are open in the expressed direction based on this chart.

TABLE 15. Table of client-side ports with destinations

Source	Destination	Port
Client	Secure Global Desktop Launch Pad Web Server	TCP 80 or TCP 443 (outbound)
Client	Secure Global Desktop Application Server	TCP 3389 (outbound)
Client	Secure Global Desktop Application Server (IFS)	TCP 4660 (outbound)

NOTE

The client makes all connection attempts.

When the Single Port Relay Server is deployed and configured to use SSL port 443, confirm that TCP port 443 (outbound) is open.

Configuring Secure Global Desktop for use with a firewall

Issue

Client computers are not able to connect to any Secure Global Desktop servers.

Symptom

All connection attempts time out.

Cause

You must open certain TCP ports for inbound connections to your Secure Global Desktop servers.

Resolution

Confirm that the following TCP ports are open in the expressed direction based on this chart. See "Table of client-side ports with destinations".

When the Single Port Relay Server is deployed and configured to use SSL port 443, confirm that TCP port 443 (outbound) is open.

Identify the ports that must be opened on the server side

Issue

Client computers are not able to connect to any Secure Global Desktop servers.

Symptom

All connection attempts time out.

Cause

Secure Global Desktop requires certain TCP ports to be open for inbound connections to your Secure Global Desktop servers.

Resolution

Confirm that the correct TCP ports are open in the expressed direction based on this chart.

TABLE 16. Table of server-side ports with destinations

Source	Destination	Port
Client	Secure Global Desktop Launch Pad Web Server	TCP 80 or TCP 443 (inbound)
Client	Secure Global Desktop Application Server	TCP 3389 (inbound)
Client	Secure Global Desktop Application Server (IFS)	TCP 4660 (inbound)

NOTE

The client makes all connection attempts.

Product keys

IFSPort.dll fails to register during the install

Issue

The IFSPort.dll fails to register during the install.

Symptom

You will see an entry in the System Event log:

The Print Spooler service terminated with the following error: The access code is invalid.

Event ID - 7023.

Cause

This may happen if you install corrupt print drivers. You can refer to MSDN articles Q243222 and Q257493. In some cases, this will happen if any antivirus software is running.

Resolution

There is not a proper fix for this problem, but there is a workaround. Ignore IFSPort.dll registration failure, and the installation will continue. After the install, you should do the following:

1. Stop all the Secure Global Desktop services.
2. Stop and start Print Spooler service.
3. Go to System32 folder and register IFSPort.dll using RegSvr32.exe.
4. Start all Secure Global Desktop services.

Finding your Product keys

Issue

How do I find my Product Key?

Symptom

N/A

Cause

N/A

Resolution

1. Log on to the Management Console.
2. Click **Home>Product Keys**.

3. You will see a list of product keys, and you can manage these product keys from this screen. You can also retrieve product key information by clicking **Home>About**. This lists the available product keys.

NOTE

In the event that you need the product key information and the browser interface is not available, you may extract this information from the SQL database.

---

4. Launch the SQL Enterprise Manager.
5. Expand the view for a list of Databases.
6. Expand the view for the CanaveralDb database.
7. Select **Tables**.
8. Right-click the table named **Product Keys**, select **Open Table>Return All Rows** from the shortcut menu.

Managing your Product Keys

Issue

How do I change or upgrade my Product Key?

Symptom

N/A

Cause

N/A

Resolution

1. Log on to the Management Console.
2. Click **Home>Product Keys**.
3. Here, you can select and delete existing product keys, or you can add upgrade product keys.

For more information on Product Keys, refer to Types of Product Keys.

Expiry dates and product keys

Issue

Home>Summary page displays warning about product key.

Symptom

Secure Global Desktop Administrators get a warning on the **Home>Summary** page “Product key will expire in NNN days. If the product key expires (30 days for evaluation key and 60 days for base key), then this message changes to “Product key expired”.

Cause

The base key has expired and the administrator has not activated the system using the Activation Key.

Resolution

Follow the steps in "Steps for activation" to activate the system.

Unable to add product key

Issue

Administrator is unable to add a new Product Key.

Symptom

When an Administrator tries to add a new product key (either base key, upgrade key or activation key) through the console, the following error is shown

“Please enter a valid key”

Cause

It might be due to one of the following reasons

- The administrator typed the key incorrectly. Keys are case-sensitive.
- Upgrade keys are tied to the base key and they cannot be used across systems.
- The key entered is not valid for this Secure Global Desktop installation. It was generated on some other installation of Secure Global Desktop.

Resolution

Check if you entered the key correctly.

You cannot use an activation key from some other installation of Secure Global Desktop. Upgrade keys are also tied to the base key in the system, if you try to use an upgrade key from some other system it will not work.

For more information on the keys in Secure Global Desktop system, refer to "Types of product keys"

Local file saving and printing

Enabling/Disabling local file saving and printing

Issue

How does a Secure Global Desktop administrator disable local file saving and printing?

Symptom

N/A

Cause

N/A

Resolution

Perform the following steps:

1. Log on to the Management Console.
2. Click **Manage>Connection Settings>Update Options**.
3. Set client drive sharing from the Client Drive Sharing list:

- To turn this feature on, select **Secure Global Desktop** for Windows 2000 and **Secure Global Desktop** or **Native** for Windows 2003.
- To turn this feature off, select **Off**.

4. Set client printer sharing from the Client Printer Sharing list:
   - To turn this feature on, select **Secure Global Desktop** or **Native** for Windows 2000 and Windows 2003.
   - To turn this feature off, select **off**.
5. To permit Secure Global Desktop to manage the devices to your benefit when you select Secure Global Desktop as the printer sharing option, select **If Vendor Driver Not Available** from the Unidriver list.

Using local file saving

Issue

How does local file saving work?

Symptom

N/A

Cause

N/A

Resolution

Secure Global Desktop implements an SMB server (Microsoft's Server Message Block protocol) on the client. This server allows access to client-side drives from Secure Global Desktop applications. Every application server reserves a set of drives (configurable within the Management Console), for mapping client-side drives.

Within a Secure Global Desktop application, whenever a file open or save operation is attempted the client-side drives would be visible as

- C on Client (I:)
- D on Client (J:)
- E on Client (K:)
- and so on.

A user cannot save to a local drive

Issue

Why am I unable to save to my local drive?

Symptom

N/A

Cause

Client drive mapping is disabled in the Management Console; the required port, if operating through a firewall, is not open for outbound traffic; or you need to restart the Tarantella Connection Manager.

Resolution

This is what you will see if local file saving is working:

- The Local drive C is seen as C: on client (H:)
- The Local drive D is seen as D: on client (I:)
- And so on …

Log on to the Management Console, and click **Manage>Connection Settings>Update Settings** and verify that Secure Global Desktop Drive Sharing is enabled. If it is not enabled, enable it and click **Update**. Exit from any launched applications, re-launch an application, and attempt to save a file again.

If operating through a firewall, you must open port 4660 for traffic outbound from the client side (and thus, inbound traffic on the server side).

To restart the Tarantella Connection Manager, exit from any launched applications, right-click the Tarantella Connection Manager icon in the system tray, and select **Exit**. Re-launch an application and attempt to save a file.

Printer Drivers

Adding new driver files to existing directories

Issue

New driver files added to existing driver directories are not recognized.

Symptom

A printer that uses a new printer driver whose files are newly added uses the Secure Global Desktop Unidriver instead of the added printer driver.

Cause

The Secure Global Desktop system checks for new printer driver files when the Secure Global Desktop Monitor service starts, and after that, only if the additional driver path is changed.

Resolution

After adding the printer driver files, specify the path of its subdirectory in the **Additional Driver Path** field of the **Manage>Servers>Add Roles** page.

Seamless windows

Changing the client screen resolution

Issue

It is inadvisable to change a client's screen resolution while a Secure Global Desktop session is running in seamless mode.

Symptom

You may see unpredictable behavior.

Cause

This is a known limitation that Secure Global Desktop inherits from the Microsoft Terminal Services Advanced Client ActiveX Control.

Resolution

Users can proceed in this sequence: terminate a session, change the screen resolution for the client from the Management Console, and then launch a new Secure Global Desktop session.

Server problems

Terminal Server license error

Issue

Terminal Server licensing error.

Symptom

When a user logs on and launches an application, Terminal Server Licensing error is displayed. Further, the event log has an entry for terminal service error.

Cause

When Windows OS is installed it gets 90-120 days grace period to install Terminal License Server. Till then it keeps issuing temporary licenses. Once the grace period is over it stops issuing new licenses. Hence the client cannot launch applications.

Resolution

If the licensing grace period is over, install the Terminal Server Licensing service on your Domain Controller:

1. Select **Start>Settings>Control Panel>Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select **Terminal Licensing Service**, click **Next** and follow the steps.
4. Activate the License Server.

The icon for the application is incorrect

Issue

The icon displayed for an application is not the correct one.

Symptom

The icon displayed for an application is not the correct one.

Cause

When creating the application, the Management Console could not access the Application Server. This may happen if the Application Server is down when you added an application or if you have not yet specified an application server for that application. Additionally, you may have failed to select an .exe or you may have selected an incorrect .exe, which would cause an incorrect icon to display.

Resolution

This is as designed.

To add the application icon after you create the application, perform the following steps:

1. Check that the application has at least one application server assigned to it.
2. Click on the **Manage>Applications**.
3. Select an application and click **Update Application**.
4. Select an updated Application Path.
5. Click **Update**.

The new icon will now be associated with the application.

Primary Database Server is down

Issue

The administrator cannot make any updates to the system.

Symptom

The **Home>Summary** page displays an issue that the Primary Database Server is down. The Console displays an error if the administrator tries to update the system.

Cause

The Primary Database Server fails or is offline.

Resolution

The administrator should open the **Monitor>Database Connections** page. This page shows the database connection status for all the Database Servers. The administrator can now take a decision whether to promote the Backup Database Server, or to take down the Primary for maintenance and bring it up again.

Add server fails

Issue

The Add Server operation fails.

Symptom

The Add Server function of **Manage>Servers>Add Server** fails with an error:

Remote Install Failed.

Cause

This could be because the administrator account supplied to the Console Add Server sequence has never logged into the remote server and the MSI service requires that the profile for the account running the .msi exist on the server. Thus, the operation fails as no account profile exists on the remote server for the Administrator account that is operating on the Management Console.

Resolution

Go to the remote server, log on, log off, and then attempt the Add Server operation again.

Server shutdown

Issue

If you shut down the computer that runs any Secure Global Desktop server, the server might still appear with an Online status in the Management Console.

Symptom

While shutting down computer the Secure Global Desktop Server may be unable to update its offline status in the Secure Global Desktop database, so the server status may show as Online for zero to four minutes. At that point, Secure Global Desktop will detect that the server is offline.

Cause

When Secure Global Desktop shuts down and attempts to update the Secure Global Desktop database with the server's new offline status, this attempt may fail.

The system does not consider dependencies when it shuts down a server, so the services that Secure Global Desktop requires to send the database update (RPCSS and Workstation) are frequently unavailable. Those services may already be shutdown.

Resolution

If you need to shut down a server it is recommended that the server be explicitly disabled using the Update Server Status link in the (**Manage>Server, select server>Change Status>Disable**).

Installs on remote servers fail

Issue

Add Server, Add Role, and Upgrade Server operations fail on remote servers.

Symptom

- The Add Server function of **Manage>Servers>Add Server** fails with an error:

  Remote Install Failed
- The Add Role function of **Manage>Servers>Add Role** fails. The Manage>Servers page displays the status of the role as The administrator can look at the Secure Global Desktop log file on the server on which the role was being installed to debug.

Cause

The Depot may be secured with SSL.

Resolution

On the Web Server, allow plain HTTP access to the Depot folder, even if other folders are marked as HTTPS. Try the operation again.

NOTE

To verify that the Depot is accessible using the Web browser (IE), type in `http:/<web server name>/Depot/SGD-TSE-Roles.msi` *in the browser, and see if the* **File Download** *dialog opens for SGD-TSE-Roles.msi.*

Diagnose Server error

Issue

Diagnose Server displays misleading error.

Symptom

Clicking **Diagnose Server** on the **Manage>Servers** page displays an error message "Secure Global Desktop is unable to remote control user sessions."

Cause

This happens when you diagnose a server on which you have configured the Windows Terminal Services for remote control without user's permission.

Resolution

Confirm the cause and ignore the error. For more information, refer to "Notifying end users of session shadowing bids".

Incorrect Application Server Status

Issue

Tarantella Connection Manager displays incorrect status for an Application Server.

Symptom

The **Monitor>Load Balancer** page of the Management Console consistently displays the running status of one of the Application Servers as **FALSE**. The Secure Global Desktop Monitor service is running on the Application Server and restarting the service or the Application Server does not display the correct status.

Cause

This is a Windows WMI utility related issue.

Resolution

Run wmiadap.exe with the /f option to create the required WMI classes.

"Object Expected" Error

Issue

Console displays "Object expected" error.

Symptom

The administrator is able to log on to the Console and access the respective overview pages by clicking a tab, but when the administrator clicks a link on any of the Console pages, the Console displays Server Problem page with "Object expected" error.

Cause

This happens when the status of the AspAllowSessionState flag is set to False, possibly by the IIS Lockdown tool.

Resolution

Do the following:

1. Run the following command from the command prompt.

```
cscript c:\inetpub\adminscripts\adsutil.vbs SET W3SVC/1/
AspAllowSessionState TRUE
```

2. Select **Start>Programs>Administrative Tools>Internet Services Manager**.
3. Right-click your computer name and select **Restart IIS** from the shortcut menu.

Server roles

Problems adding the Application Server role

Issue

I receive an error when I try to push or add the Application Server role to my server.

Symptom

The error is as follows:

Sorry, an error occurred while trying to update the Secure Global Desktop installation on this server.

Install not possible, please check that the server can handle this role.

Cause

Windows Terminal Server is in the wrong mode, it must be in Application Server mode.

Resolution

To check the Terminal Server Mode of your server, do the following:

1. Select **Start>Programs>Settings>Control Panel>Administrative Tools** and select **Terminal Services Configuration**.
2. Select **Server Settings** from the left pane, and then in the right pane, look at the Terminal server mode.
3. The attribute for the Terminal server mode should say Application Server. If the attribute for the Terminal server mode says Remote Administration, then use **Add/Remove Programs>Add/Remove Windows Components** to change the server mode.

Secure Global Desktop Server roles

Issue

What is a server role?

Symptom

N/A

Cause

N/A

Resolution

With almost any software solution, there are proprietary components that are necessary to achieve functionality. The Secure Global Desktop server roles are components or services necessary for Secure Global Desktop to function. When you are managing your servers from the Management

Console, you can view or update the active server roles for each server. A list of the various server roles follows:

- Web Server
- Load Balancer Server
- Application Server
- Relay Server

For more information on these roles, see Ticketing Authority.

Shadowing

A single session can only be shadowed once

Issue

Can multiple administrators shadow one session simultaneously?

Symptom

N/A

Cause

N/A

Resolution

No, a session can be shadowed only once at any given time.

Shadowing privileges and permissions

Issue

Do you need to be a Secure Global Desktop Administrator to shadow a session?

Symptom

N/A

Cause

N/A

Resolution

Yes, you must be a Secure Global Desktop Administrator to shadow a session. Peer shadowing is forthcoming in a future release.

Notifying end users of session shadowing bids

Issue

Can a session be shadowed without the end user knowing?

Symptom

N/A

Cause

N/A

Resolution

Yes, using a specific Windows Terminal Server feature in conjunction with Secure Global Desktop, you can do this.

No, using Secure Global Desktop alone, you cannot do this. When an administrator attempts to shadow a session, the user receives a prompt to approve the request, which will successfully establish the shadow session.

If you would like to shadow a session without a prompt appearing to the client, you must follow this procedure.

1. Select **Start>Programs>Administrative Tools>Terminal Services Configuration**.
2. Select **Connections**, and then select **RDP-TCP**.
3. Click the **Remote Control** tab, clear the setting for **Use Remote Control With The Following Settings**, and verify that the **Require User's Permission** check box is cleared.

NOTE

If you click **Diagnose Server** *on the* **Manage>Servers** *page after selecting a server on which you have configured the Windows Terminal Server feature as above, you get an error message "Secure Global Desktop is unable to remote control user sessions."*

Using a WTS Client for shadowing

Issue

Why would the WTS Client download when I am simply shadowing a session?

Symptom

When a Secure Global Desktop Administrator tries to shadow an active session, you may see the Client installation start.

Cause

N/A

Resolution

This is as designed.

When a Secure Global Desktop Administrator attempts to shadow an active session, he or she is actually launching a WTS session. Therefore, that administrator needs a Client.

Shortcuts

Explaining the timing of shortcut creation

Issue

When does Secure Global Desktop create the shortcuts?

Symptom

N/A

Cause

N/A

Resolution

The administrator may enable or disable shortcut creation.

To enable or disable shortcut creation:

1. Log on to the Management Console.
2. Click **Options>User**.
3. Under the **Features** area, select a shortcut option for the **Shortcuts** drop-down list.
4. The shortcut parameters operate this way.
   - If the administrator selects **None**, the user will see no shortcuts.
   - If the administrator selects **All**, the user receives shortcuts for all applications and these shortcuts appear on the user's desktop under the Windows Start menu.
   - If the administrator selects **User's Choice**, a user can customize his own or her own interface. The user can decide which applications will have shortcuts and where those shortcuts will appear.

After a user logs on to a site and after the Client install, a user can log on to the Launch Pad and manage the shortcuts from the **Options** page. If the user deletes the shortcuts using the Tarantella Connection Manager, then the shortcuts will return when the user does one of the following: logs on to the Client system, exits from and returns to the Launch Pad, or initiates a Refresh from the Connection Manager.

If a user logs on to a client computer as a different user, then Secure Global Desktop will prompt the user for a username, password, and domain name to access the application.

The user must enter the login information of the person who owns these application shortcuts or the shortcuts will not work.

File associations

File associations do not work as expected

Issue

User reports an issue related to file associations.

Symptom

The user is not able to open a document with file association.

Cause

Adding or removing a server after the administrator has added an application affects file associations. Besides, after the Administrator has provisioned an application, the file associations on the Application Server may change.

Resolution

Update the file associations for the application from the **Manage>Application>Update File Associations** page. This will once again look at all the servers and get the intersection of applications.

IFS error

Issue

File associations are not working even though the user has enabled them.

Symptom

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

FIGURE 19. Secure Global Desktop IFS disabled error

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

In order to achieve this, the administrator should assign the application the Connection Settings with the Client Drive Sharing set as Secure Global Desktop. For more information on Connection Settings, refer to "Connection settings".

Launch 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.

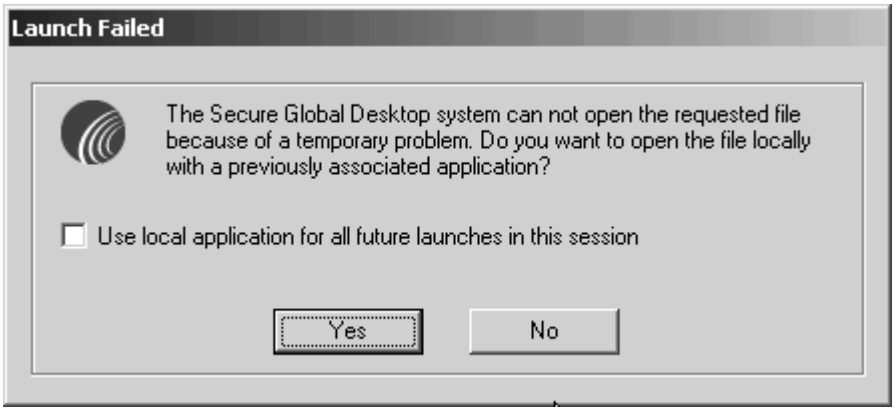


FIGURE 20. Launch Failed error

Cause

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

Resolution

The user can choose to open the file with another application on the Server, or open a local application for the current session. The user can also choose to use the local application for all future launches in the current session.

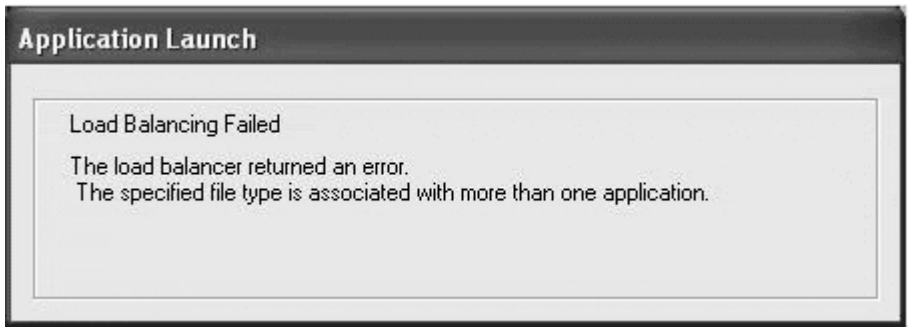
Load Balancing Failed error

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 provisioned an application with a file association. Then the administrator may have associated another application with the same file extension on the Application Server, and then provisioned this second application with the same file association as the first one.

As an example, consider the case when the administrator provisions Notepad with .txt file association. Then, the administrator associates WordPad on the Application Server with .txt by

modifying the registry. Subsequently, after the Secure Global Desktop Engine restarts due to reboot or any other reason, the administrator provisions WordPad with .txt file association.

Resolution

Update file associations from the **Manage>Applications>Update File Associations** page of the Console, for the application that was originally provisioned with the file association that was changed in the registry; in our example, update file associations for Notepad to remove the association of .txt file extension.

Correct icons not displayed

Issue

The client computer does not display correct icons according to file associations for the files.

The client computer does not display correct icons for the files after removing file association for documents for an application.

Symptom

The user reports that the correct icons as per file associations are not displayed for the documents after enabling file association for documents for an application or the original icons are not displayed after removing file associations.

Cause

This is standard Windows behavior after changing icons.

Resolution

On the client computer, do the following:

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.

SQL Server

SQL server connection problem after an upgrade

Issue

You have recently upgraded you Secure Global Desktop software and now Secure Global Desktop is unable to communicate with the SQL server.

Symptom

Problems exist with the communication between the SQL server and Secure Global Desktop.

Cause

The connection string for the SQL server was input to the Secure Global Desktop install/upgrade program in the wrong format.

Resolution

Reinstall or re-upgrade Secure Global Desktop and do *not* use the DNS name in the SQL connection string. Use the computer name alone in the connection setting. Do *not* use a string that shows both the computer name and domain information. For example, do *not* use a string in this format:

```
machine-name.dept.server.company.com
```

Do use a string that shows only the computer name. For example, use a string in this format:

```
Machine-name
```

To find the correct name of the server that runs the SQL server, click My Computer, click the **Network Identification** tab, click **Properties**, and copy the value that appears in the **Computer Name** box.

Windows Terminal Services settings and seamless windows

A WTS session cannot launch application in an NT 4 environment

Issue

User(s) cannot successfully launch an application in an NT 4 environment and the effort shows the server's desktop.

Symptom

The user will notice the logon to the WTS server and may notice the logon script completing in a window that shows the desktop. The application launch window will continue showing only the server's desktop.

Cause

The WTS settings associated with the user account is preventing a successful launch of the application.

Resolution

On the Windows 2000 computer that is the Application Server, click **Start>Run**. Type `usrmgr.exe` and click **OK**. View the User Account properties for the username in question. Click **TS Config>Initial Program** and select the **Inherit Client Settings** option.

Windows Terminal Services session with seamless windows

Issue

How do I enable/disable the WTS session window?

Symptom

When I launch an application, my application runs within a window.

Cause

You may need to enable Seamless Mode.

Resolution

When adding or updating an application, Seamless Windows is an option that appears in the in the Management Console under **Options>Connections Settings**. If the option for Seamless Windows is enabled, then the application will appear and operate as if it were running locally on the client computer. If Seamless Windows is disabled, the application will run within a WTS shell.

Launch Pad

Netscape error

Issue

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

Symptom

The following error is displayed forcing the user to click **Reload**.

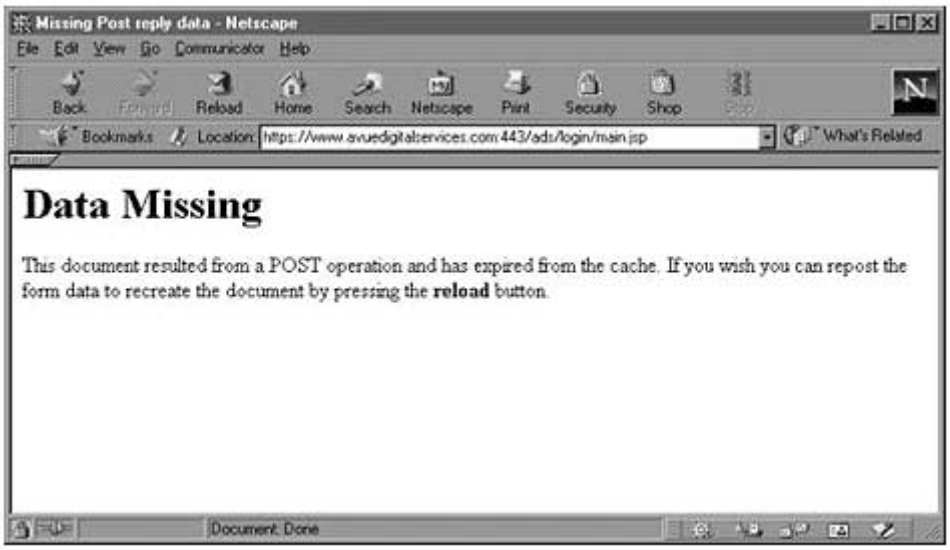


FIGURE 21. Netscape “Data Missing” error

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.

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

Slow logon

Issue

Slow logon to Console and Launch Pad.

Symptom

Logon to the Console and Launch Pad takes more than a minute.

Cause

The logon to Console and Launch Pad uses the domain NetBIOS name to communicate with the domain. Using the NetBIOS name to attempt to resolve an AD domain can take some time.

Resolution

Check for wrong DNS suffix entries in TCP/IP network properties on the Web Servers.

To check the DNS entries:

1. Right click **My Network Places** on the desktop and select **Properties** from the shortcut menu.
2. Right click the local area connection and select **Properties**.
3. Select the **Internet Protocol (TCP/IP)** check box and click **Properties**.
4. Click **Advanced**, click the **DNS** tab, and verify the DNS entries on the **Advanced TCP/IP Settings** window.
5. Click **OK**.

IE setting for SharePoint server

Issue

Client computers cannot login to Launch Pad Web part in SharePoint Portal Server.

Symptom

Even after entering correct credentials on the Login page, a user is not able to login to Launch Pad Web part in SharePoint Portal Server and is returned to the Login page.

Cause

Internet Explorer settings do not allow third party cookies.

Resolution

On the client computers, 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.
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.

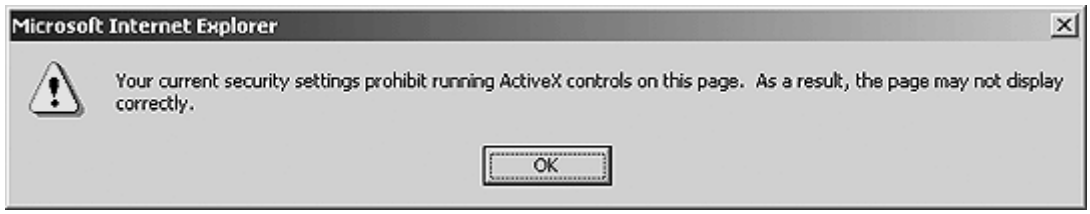
Security settings error

Issue

Insufficient rights, security settings of browser.

Symptom

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



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**.

Event Log

This section lists some event log messages and the sections of this guide that can provide you more information on the message.

TABLE 17. Event log messages

Message	Reference
Error: CuLogic - Secure Global Desktop Identity account cannot retrieve user group membership information from domain <domain name>. Possible causes include the identity account not having sufficient permissions to access information in Directory. To correct this problem, refer to section 'Concepts - Active Directory Synchronization - Prerequisites' in the Secure Global Desktop Administrator Guide.	"Prerequisites"
Error: HRESULT. Incremental data synchronization from Primary Database to Backup Database has failed. Please synchronize Backup database through Management Console.	"Synchronization of the Backup Database Server"

Secure Global Desktop TSE Installing WBT Add-on for Windows CE 2.12-based Wyse Terminals

What's in this chapter?

This chapter contains all of the information you need to have to install the Secure Global Desktop TSE WBT add-on and manage a Windows CE 2.12-based Wyse terminal.

This chapter assumes you are familiar with the following:

- Basic Web Server administrative functions
- FTP server operations
- Wyse terminal

Getting Started

This section lists the minimum requirements and step-by-step procedures for installing the Secure Global Desktop TSE WBT add-on for Wyse/WinCE 2.12 terminal.

Installing Secure Global Desktop TSE WBT add-on for Wyse/WinCE 2.12

This section lists the activities you must complete before you install the add-on image or before you upgrade. Follow this procedure if you are working with a Wyse terminal and your Wyse terminal does not come packaged with the Secure Global Desktop TSE add-on.

Copy the Secure Global Desktop TSE Files

Place the files on the FTP server

Perform the activities in this section before you install the add-on.

From the FTP server, perform the following:

1. Check the Tarantella Web site for the latest version of the client software.
2. Ensure that there is no beta version of the Secure Global Desktop TSE software installed on the client devices. If there is a version, you will need to reflash the device with a new Wyse image before proceeding.
3. Place the two files, `SGD-TSEaddon.bin` and `params.ini`, on an FTP server.

Manage the Secure Global Desktop TSE files from the Client

From the client, perform the following:

1. Press the `F2` function key on the client to enter the **Terminal Properties**.

2. Click the **Upgrade** tab.

To install the Secure Global Desktop TSE add-on:

1. Select the **Use Local FTP Information** option.

2. In the **Server Name** field, enter the FTP server's IP address.
3. In the **Server Directory** field, enter the proper directory path. This is the path to the ftproot, the path with the root folder.
4. Enter a user ID and password.

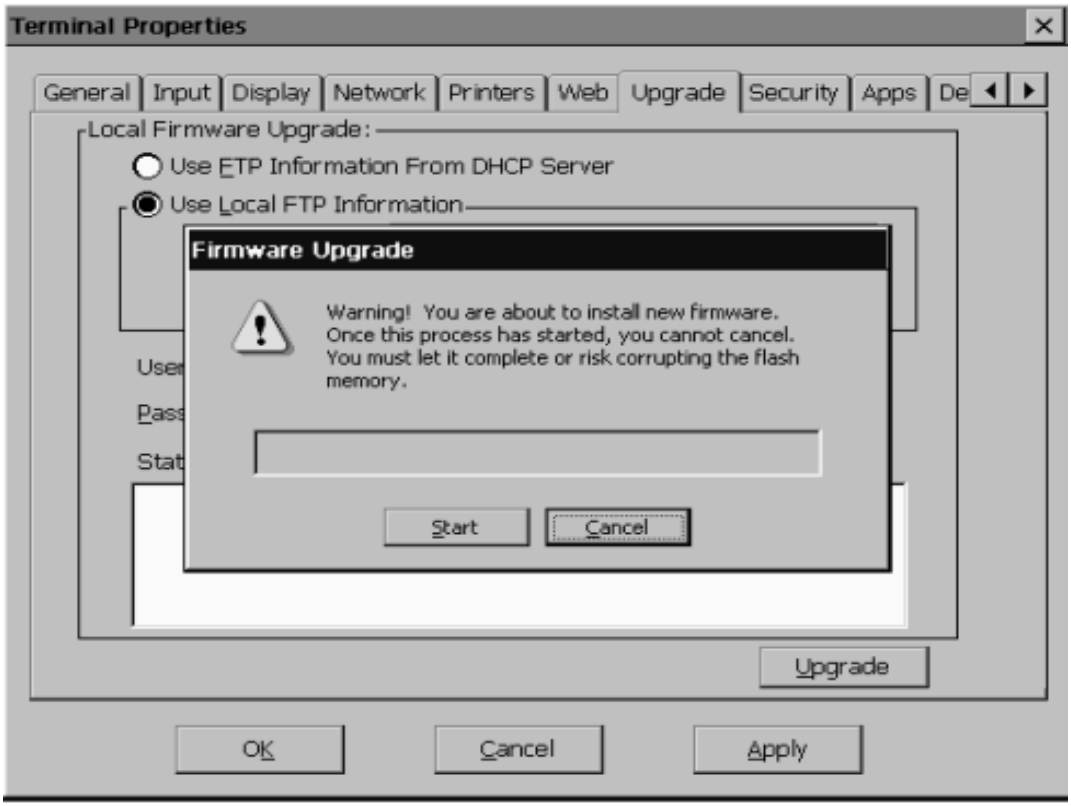
NOTE

The default User ID is Anonymous, and the password is any five characters.You can use the default user ID and password when the FTP server permits anonymous connections.

---

5. Select the **Save Password** check box to save the password.

6. When you are ready to proceed, click **Upgrade**.



7. On the **Firmware Upgrade** dialog box, click **Start**.
8. When this process completes, the machine re-starts.

NOTE

The Secure Global Desktop TSE CE add-on uses the RDP client, and the add-on will not work without it. So remember, do not remove the RDP client.

Configure the connection

To configure a Secure Global Desktop TSE connection on the Client machine:

1. Click the **Configure** tab on the **Winterm Connection Manager**.
2. Click **Add.**

3. In the **New Connection** dialog box, select **Tarantella Connection Manager** from the drop-down list and click **OK**. The **Secure Global Desktop TSE Connection** dialog box appears.

To establish the connection:

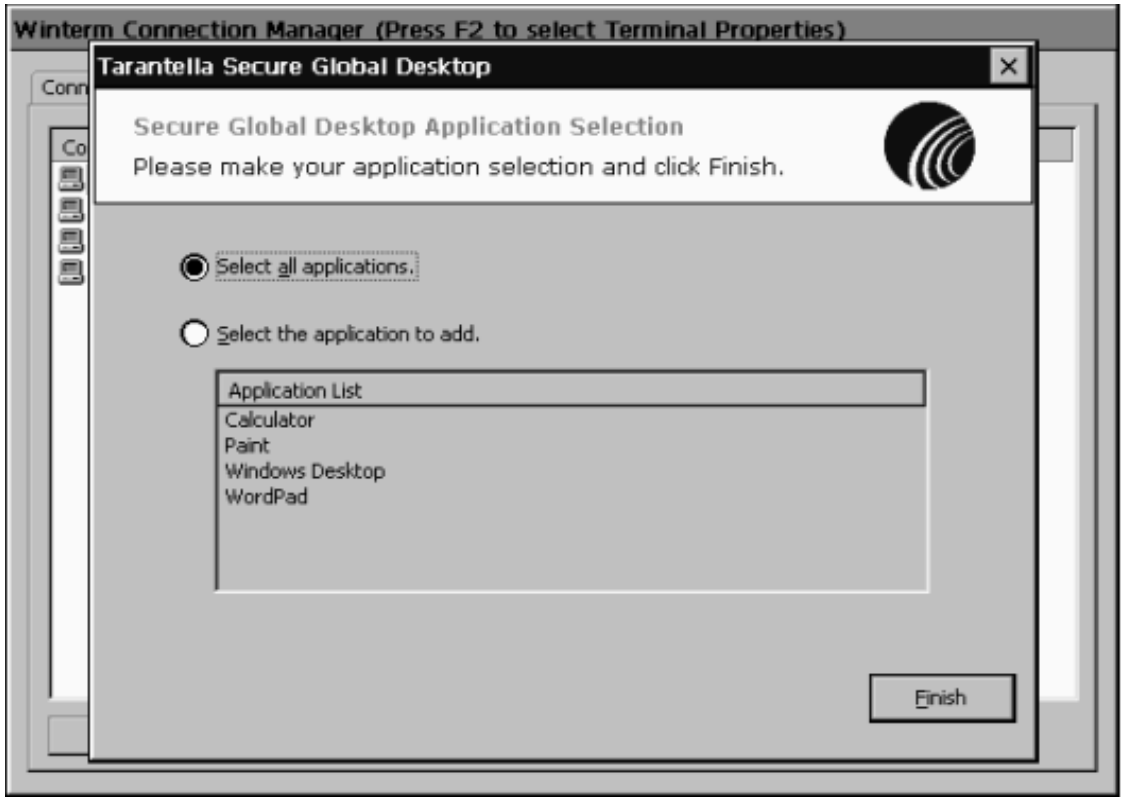
4. In the **Secure Global Desktop TSE Connection** dialog box, type the URL of the Secure Global Desktop TSE Launch Pad that you intend to use in the **Launch Pad Address** field.

   For example:

   `http://<servername>/launchpad`

5. In the **User Name** field, enter the user name.

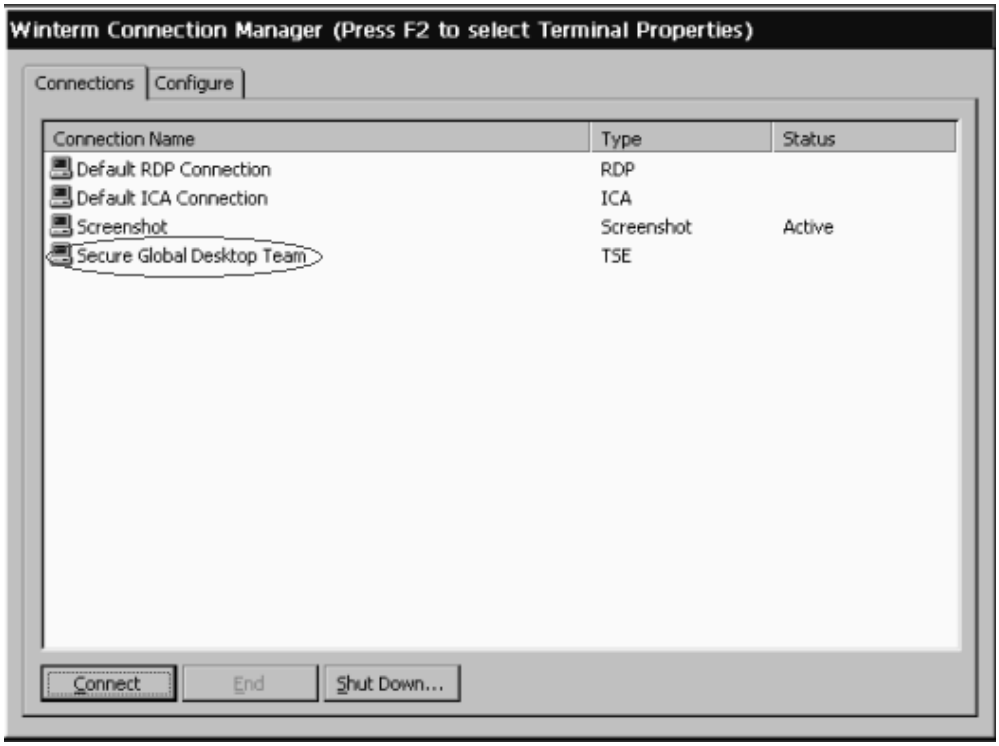
6. In the **Domain field**, enter the domain that you will use. This domain should exist in Secure Global Desktop TSE; it should have been provisioned by the Secure Global Desktop TSE Administrator.
7. Click **Next.**
8. Choose the way you will select applications:
   - **Select All Applications** to select all the displayed applications. Go to Step 9.
   - **Select An Application** to select one application at a time. Go to Step 10.



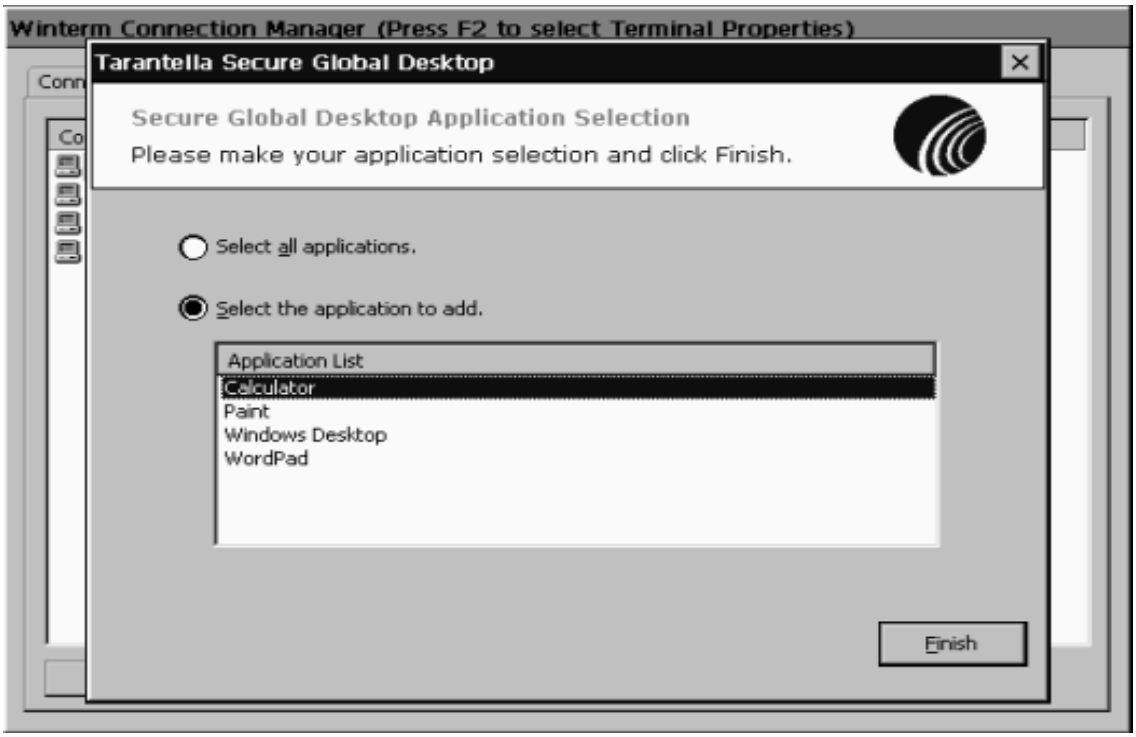
9. If you choose **Select All Applications**, click **Finish**.

   A single Secure Global Desktop TSE connection called **Secure Global Desktop Team** appears on the **Winterm Connection Manager** dialog box. You will use the **Secure**

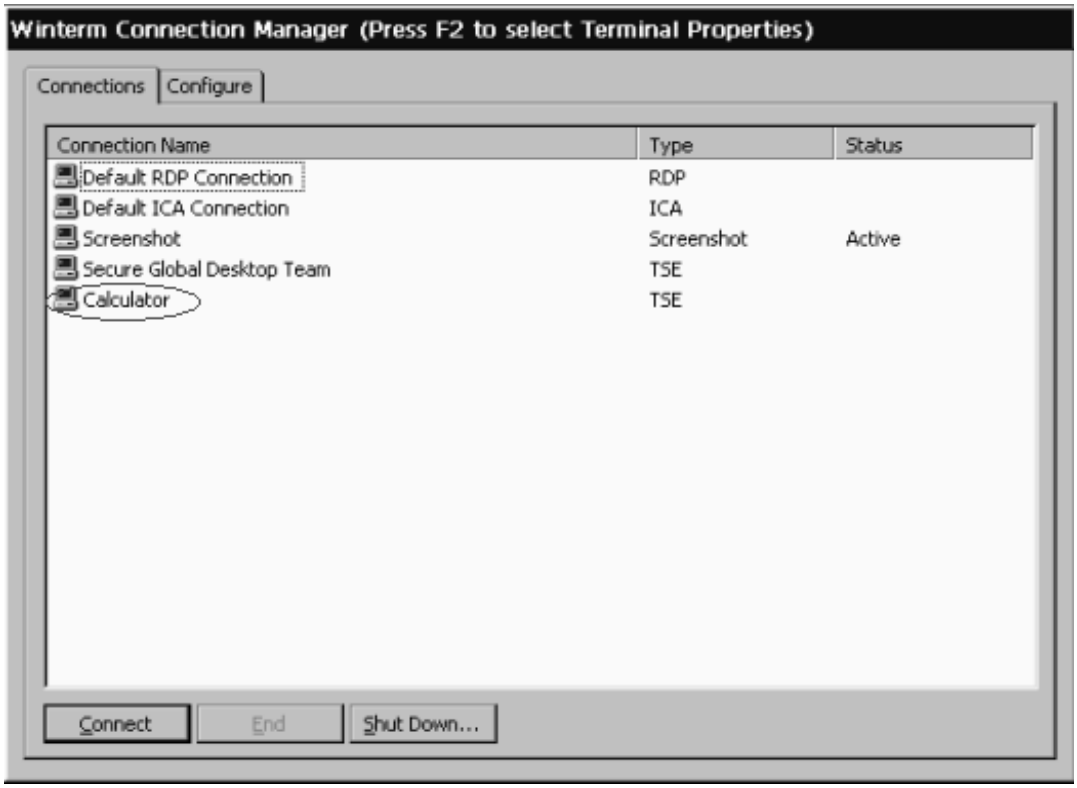
Global Desktop Team connection to access the list all of the applications that are available to you from the Secure Global Desktop TSE server.



10. If you choose **Select An Application**, you must select the application you want to use, and then click **Finish**.



11. A single Secure Global Desktop TSE application connection appears in the **Winterm Connection Manager** for the selected Secure Global Desktop TSE application.



NOTE

Repeat this procedure to add connections to other individual applications.

Launching an application

To launch an application:

1. Click the **Connections** tab on the **Winterm Connection Manager**.
2. Double click a Secure Global Desktop TSE connection icon. If you have not saved your password, the **Secure Global Desktop TSE Connection** (authentication) dialog box appears.

3. In the **Secure Global Desktop TSE Connection** dialog box, enter your credentials and click **OK**.

4. If you double clicked a specific application connection icon in Step 2, the application is launched. If you clicked the **Secure Global Desktop Team** Connection icon, the list of applications is retrieved. Select an application and click **Launch** to launch the application.

Installing WBT Add-on for Wyse CE 2.12 or Wyse CE .NET with Rapport

What's in this chapter?

This chapter addresses an administrator's interactions with the Wyse Rapport software, and it explains how administrators use this software to push the Secure Global Desktop TSE WBT add-on for Wyse/WinCE 2.12 or Wyse CE .NET to many user terminals concurrently.

Getting Started

This section tells you how to obtain files and how to push them through Rapport to the Wyse CE 2.12 or Wyse CE .NET terminals. In terms of Wyse Rapport tasks, these instructions are only skeletal, so you may need to obtain your Rapport software documentation to see step-by-step procedural instructions.

Requirements

You will need three sets of files.

First, for Rapport, you will need the following files, which you can download from Wyse Technology Inc., www.wyse.com:

- Wyse Rapport 3.02 (the Service Pack, SP 1 is optional)
- Wsnmp.tpl, version 33 or greater

Second, for the Wyse terminal image, you will need to obtain an image file from Wyse. Obtain the image that is appropriate for your Wyse terminal model.

Files for different Wyse model numbers will have different names too; however, for all models you will need files with the following extensions and a params.ini file, which you can download from Wyse, www.wyse.com:

- <file name for your CE or CE .NET model>.rsp
- <file name for your CE or CE .NET model>.wye
- params.ini

Third, for the Secure Global Desktop TSE add-on, you will need to download the appropriate files from the download page, http://www.tarantella.com/products.

For Wyse CE 2.12, click **Download** from the *Secure Global Desktop TSE WBT add-on for Windows CE 2.12-based Wyse terminals* section of the **Download** page to receive these files:

- SGD-TSE.rsp
- SGD-TSE\SGD-TSEaddon.bin
- \SGD-TSE\Params.ini

For Wyse CE .NET, click **Download** from the *WBT Add-on for Windows CE .NET-based Wyse Terminals Download* section of the **Download** page to receive these files:

- SGD-TSE.rsp
- SGD-TSE\SGD-TSEaddon400.bin
- SGD-TSE\Params.ini

Using Rapport to push the Secure Global Desktop TSE add-on

The following procedures explain how to push the Secure Global Desktop TSE add-on to Wyse CE or Wyse CE .NET terminals using the Wyse Rapport software.

As you proceed to register and distribute the software, remember, if you are distributing software packages to Write filter enabled clients, you must disable the Write filter prior to sending updates. This is necessary to ensure that you save the updates to the client's physical Flash memory.

You must re-enable the Write filter after you finish placing the new software on the devices.

NOTE

You should perform this procedure on a test device before you implement this procedure in the production environment.

Enabling Rapport for Secure Global Desktop TSE

1. Obtain the download from the Tarantella Web site.
2. Ignore the documentation that downloads with the Secure Global Desktop TSE files and continue to use this Rapport document.
3. Extract the downloaded files.
4. On the Rapport server, replace the wsnmp.tpl file with the .tpl file that comes with the download.
5. Start Rapport.

Pushing the WYSE factory image to the terminals

This is an optional step.

1. Obtain the required files for the terminals from the Wyse Web site.
   - <file name for your CE or CE .NET model>.rsp
   - params.ini
   - <file name for your CE or CE .NET model>.wye

   See the Wyse documentation for instructions on registering software packages.
2. From the Rapport console, drill down in the directory tree to the following path:

   ```
   Rapport\rapport\software manager\CE images
   ```
3. From the CE image, create a new software package, to re-image the client's flash memory.
4. Drag and drop the software package onto the Client Manager to send the image to the devices.

Pushing the Tarantella Secure Global Desktop TSE from Tarantella add-on to the terminals

1. Obtain the required files from the directory that received the download from the Tarantella web site. For more information, see "Enabling Rapport for Secure Global Desktop TSE".

   For Wyse CE 2.12:

   - \SGD-TSE.rsp
   - \SGD-TSE\SGD-TSEaddon.bin
   - \SGD-TSE\Params.ini

   For Wyse CE .NET:

   - \SGD-TSE.rsp
   - \SGD-TSE\SGD-TSEaddon400.bin
   - \SGD-TSE\Params.ini

   See the Wyse documentation for instructions for registering software packages.

2. From the CE add-on, create a new software package using the \SGD-TSE.rsp file.
3. From the Rapport console, drill down in the directory tree to the following path:

   Rapport\rapport\software manager\CE addon

4. Drag and drop the software package onto the Client Manager to send the add-on to the devices.

Creating a master template terminal

An administrator must create a master CE or CE .NET device that will establish the required Secure Global Desktop TSE connections and will provide an administrator with data to send to multiple CE or CE .NETdevices.

1. Install the Wyse image. This first step is optional. For more information, see "Pushing the WYSE factory image to the terminals".
2. Install the add-on. For more information, see "Pushing the Tarantella Secure Global Desktop TSE from Tarantella add-on to the terminals".
3. Configure your device to meet your requirements.

Obtaining the configurations from the master template terminal

The administrators must obtain the connection configuration from the master template before they send it to other terminals.

1. From the Rapport Console, drill through the Software Manager to the Client Configuration, and select the GetCEcfg folder, which resides in:

   Rapport\rapport\software manager\Client Configuration

2. Drag and drop the GetCEcfg onto the Client Manager.
3. At the prompt, select the terminal that will act as the master terminal. You will pull the configuration from this terminal.
4. Follow the instructions in the Wyse dialog boxes to complete this task.

NOTE

For additional information, see the Rapport documentation provided by Wyse Technology Inc.

Sending configurations to all of the terminals

To create all of the terminals, you must do the following:

- Send an image file
- Send a Secure Global Desktop TSE client
- Send the CEcfg

An administrator must send the connection configuration to all other terminals.

1. In the getCEcfg folder, locate the settings.reg file.
2. Drag the settings.reg file from the getCEcfg folder to the sendCEcfg folder.

NOTE

A common start location is C:\Inetpub\ftproot\Rapport\GetCEcfg.
A common destination location is C:\Inetpub\ftproot\Rapport\SendCEcfg.

3. Click on the sendCEcfg folder, which resides in:

   `Rapport\rapport\software manager\Client Configuration`

4. Drag and drop sendCEcfg onto the Client Manager.
5. At the prompt, select the terminals that are to receive the configuration.
6. Follow the instructions in the Wyse dialog boxes to send the configuration to these terminals.

Re-enabling the Write filters

An administrator must re-enable the Write filters after distributing software packages to the clients. If the administrator leaves the Write filter disabled, the clients no longer have protection and may be susceptible to flash memory corruption.

Considerations

When you use Wyse Rapport to distribute the Secure Global Desktop TSE clients to many clients from the server, this procedure is all you need. You not need use the procedures that appear in either "Secure Global Desktop TSE Installing WBT Add-on for Windows CE 2.12-based Wyse Terminals" or "Installing WBT Add-on for Windows CE .NET-based Wyse Terminals", those procedures are just for loading a Secure Global Desktop TSE client onto a single client from that client.

Installing Secure Global Desktop TSE Client on Embedded terminals

What's in this chapter?

This chapter explains the minimum requirements for Wyse Windows NT Embedded 4.0 and Wyse Windows XP Embedded terminals to operate as clients for Secure Global Desktop TSE . It also explains how to install the Secure Global Desktop TSE software.

Getting Started

Requirements

The minimum requirements for flash and RAM for the Wyse Windows NT Embedded 4.0 terminal are 96-MB flash and 96-MB RAM. As of the product release date, you can have any of the following terminals configured to meet this requirement: Winterm 8235LE, 8360SE, 8440XL, and 8630LE. In the future, look for other Wyse NT Embedded 4.0 terminals that meet the minimum requirements for flash and RAM.

The minimum requirements for flash and RAM for the Wyse Windows XP Embedded terminal are 192-MB flash and 256-MB RAM. As of the product release date, you can have any of the following terminals configured to meet this requirement: Winterm 9440XL or 4235LE and also model number WT9235LE with WYSE XP Embedded v2002. We have also tested In the future, look for other Wyse XP Embedded terminals that meet the minimum requirements for flash and RAM.

In case of Wyse Windows XP Embedded terminals, the free RAM size should be at least 8MB. If you do not have that much space, you may do one or more of the following:

1. Remove unwanted software.
2. Delete the temporary Internet files.
3. Select **Control Panel>Ramdisk** and on the **Ramdisk Configuration** dialog box reduce the current Ramdisk size.

Installation

The installation of the Secure Global Desktop TSE client is slightly different for a Windows XP Embedded terminal from that for a Windows NT Embedded 4.0. However, for either platform, you should first disable the Write filter.

Disable the write filter

Disable the write filter for the duration of the installation and then enable it again, disable it as follows:

1. Log on to the Wyse terminal as an administrator.

2. Select **Start>Settings>Control Panel>Administrative Tools** and double-click **Write Filter**. You may also select **Start>Programs>Write Filter**.
3. Click **Flush Cache** and wait while the cache is flushed.
4. Select the **Disable Write Protect** check box when it is enabled after the cache is flushed.
5. Click **Exit**.
6. Restart the terminal.

Install Secure Global Desktop TSE on Windows Embedded Terminal

If you are working with a Windows embedded terminal, follow this procedure.

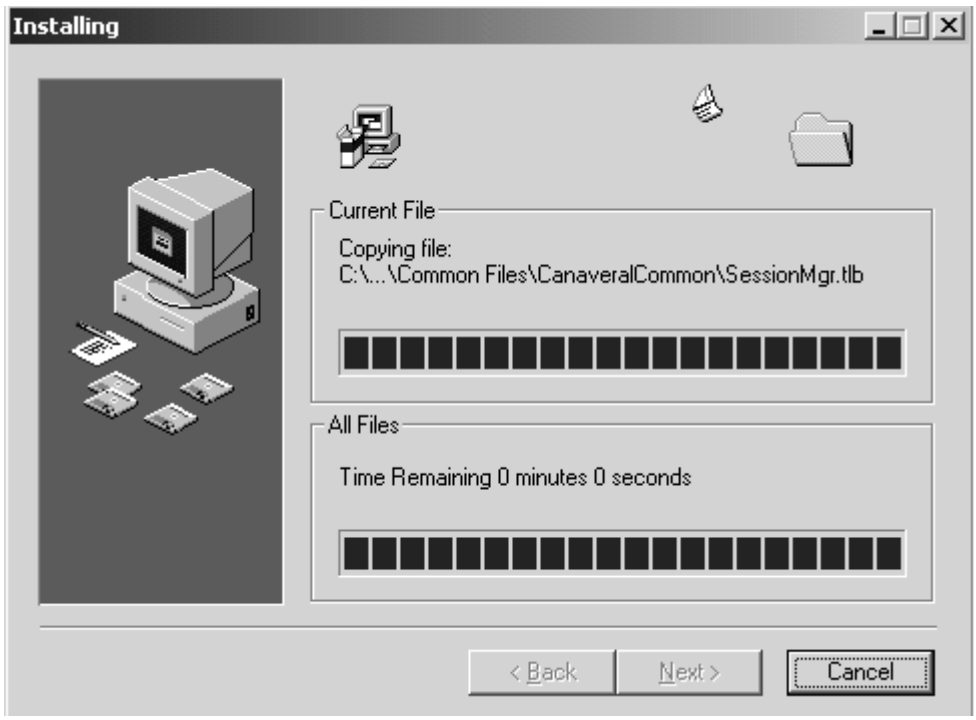
1. Log on to the terminal as an administrator.
2. You will need administrator privileges for the installation, but you can use normal user-level privileges for general operations.
3. Locate a copy of the iQclntmgrNT.exe.

   This is a separate installation program for the NT-embedded terminals. You may find this program on the Secure Global Desktop TSE Web server at this path:

   `\\<Web Servername>\C$\inetpubs\wwwroot\depot\iQclntmgrNT.exe`
4. When you locate the `iQclntmgrNT.exe` file, copy it to a folder on a different server, and share the folder.
5. Run `iQclntmgrNT.exe` from a shared folder.
6. Read the **Welcome** dialog and click **Next**.

7. Select the installation destination folder or accept the default destination folder and click **Next**.

8. Wait for the installation to complete.



9. Verify that the installation completes successfully. After a successful completion, you will see a Secure Global Desktop TSE icon in your system tray (in the lower right-hand area of your desktop).
10. Log off the terminal now as you no longer require administrator privileges.

11. Log on to the terminal using the User account.
12. Access the Secure Global Desktop TSE Launch Pad. The address will reflect your web server's name followed by the literal launchpad.

    For example, `http://<web_machine_name>/launchpad`
13. When you see the **Log On** page, log on.
14. Launch an application.

Known problems

This section looks at troubleshooting topics.

Write Filter Cache

Issue

Write filter cache on the Wyse terminal fills.

Symptom

The count for the number of blocks used increases with time.

Cause

Write filter cache on Wyse terminal fills up during use.

Resolution

Reboot the terminal once every day or two, or shut down the terminal before you leave at the end of each workday.

Problems loading the Secure Global Desktop TSE Client software

Issue

You may have to disable the terminal's Write filter for the duration of the Secure Global Desktop TSE client install.

Symptom

The installation fails.

Cause

You may have failed to disable the Write filter before installing Secure Global Desktop TSE.

Resolution

Disable the Write filter for the duration of the installation and then enable it again after the installation. So before the installation, you set the wfilter startup parameter to **Disabled** and after the installation, you reset the wfilter startup parameter to **Boot**.

Shortcuts not created

Issue

Desktop shortcuts are not created automatically.

Symptom

After restarting the terminal, the shortcuts are not created automatically on the desktop. The Secure Global Desktop TSE Client does not appear automatically in the system tray of the Wyse Windows XP Embedded terminal.

Cause

This is because the Secure Global Desktop TSE Connection Manager shortcut is not created in the **Programs>Startup** folder.

Resolution

Manually launch Secure Global Desktop TSE Connection Manager from **Start>Programs>Secure Global Desktop TSE Connection Manager** to create the shortcuts. For the next startup, create Secure Global Desktop TSE Connection Manager shortcut in the **Programs>Startup** folder so that Secure Global Desktop TSE Client launches when the device starts up and shortcuts are created automatically.

Installing WBT Add-on for Windows CE .NET-based Wyse Terminals

What's in this chapter?

This chapter contains all of the information you need to have to install the Secure Global Desktop TSE WBT add-on and manage a Windows CE .NET-based Wyse terminal.

This chapter assumes you are familiar with the following:

- Basic Web Server administrative functions
- FTP server operations
- Wyse terminal

Getting Started

This section lists the minimum requirements and step-by-step procedures for installing the Secure Global Desktop TSE WBT add-on for Wyse/WinCE .NET terminal.

Minimum Requirements

The following table presents the minimum requirements for flash and RAM by model for the Wyse Winterm devices.

TABLE 18. Minimum Requirements

Device	Flash	RAM
Model 3320	24 Megabytes	32 Megabytes
Model 3530	16 Megabytes	32 Megabytes
Model 3235	16 Megabytes	32 Megabytes
Model 3360	16 Megabytes	32 Megabytes

Installing Secure Global Desktop TSE WBT add-on for Wyse/WinCE .NET

This section lists the activities you must complete before you install the add-on image or before you upgrade. Follow this procedure if you are working with a Wyse terminal and your Wyse terminal does not come packaged with the Secure Global Desktop TSE add-on.

Copy theSecure Global Desktop TSE Files

Place the files on the FTP server

Perform the activities in this section before you install the add-on.

From the FTP server, perform the following:

1. Check the Tarantella Web site for the latest version of the client software.
2. Ensure that there is no beta version of the Secure Global Desktop TSE software installed on the client devices. If there is a version, you will need to reflash the device with a new Wyse image before proceeding.
3. Place the two files, `SGD-TSEaddon400.bin` and `params.ini`, on an FTP server.

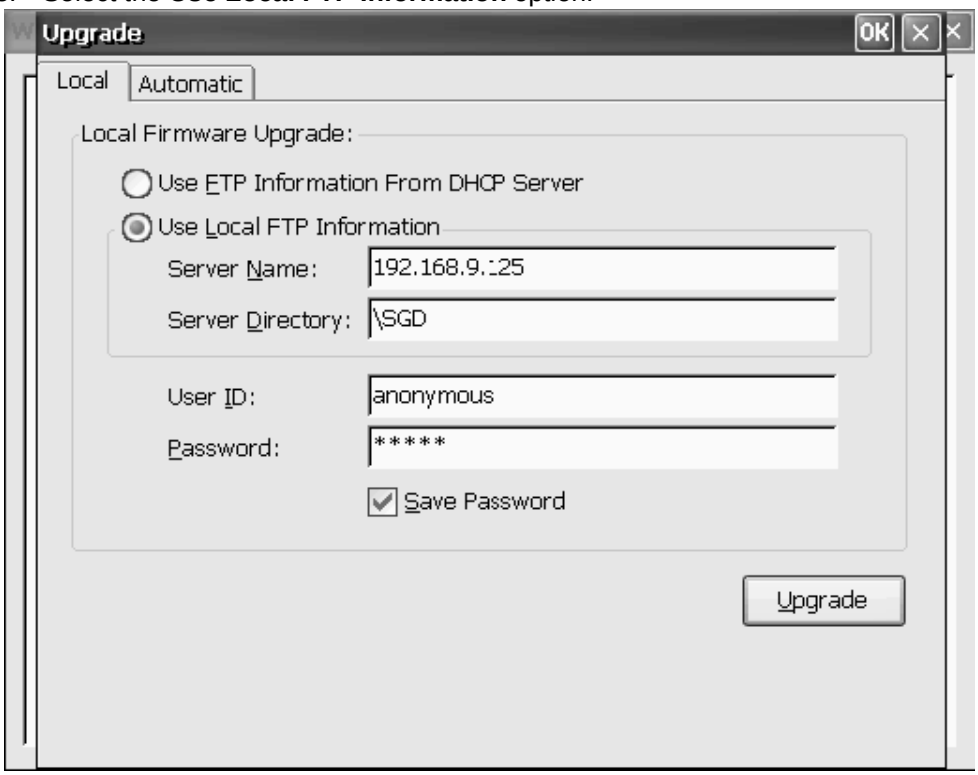
Manage the Secure Global Desktop TSE files from the Client

From the client, perform the following:

1. Press the **Control Panel** button on the client to enter the **Terminal Properties**.
2. Click the **Upgrade** tab.

To install the Secure Global Desktop TSE add-on:

3. Select the **Use Local FTP Information** option.

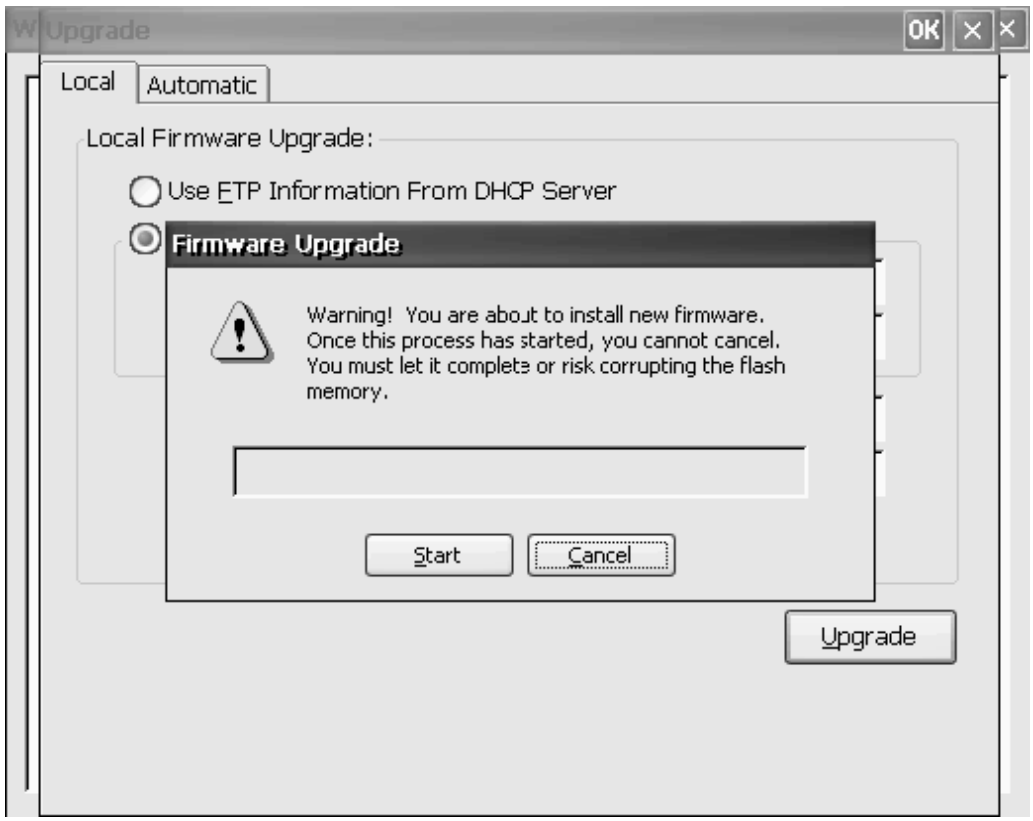


4. In the **Server Name** field, enter the FTP server's IP address.
5. In the **Server Directory** field, enter the proper directory path. This is the path to the ftproot, the path with the root folder.
6. Enter a user ID and password.

> **NOTE**
>
> *The default User ID is Anonymous, and the password is any five characters.You can use the default user ID and password when the FTP server permits anonymous connections.*

7. Select the **Save Password** check box to save the password.

8. When you are ready to proceed, click **Upgrade**.



9. On the **Firmware Upgrade** window, click **Start**.
10. When this process completes, the machine re-starts.

NOTE

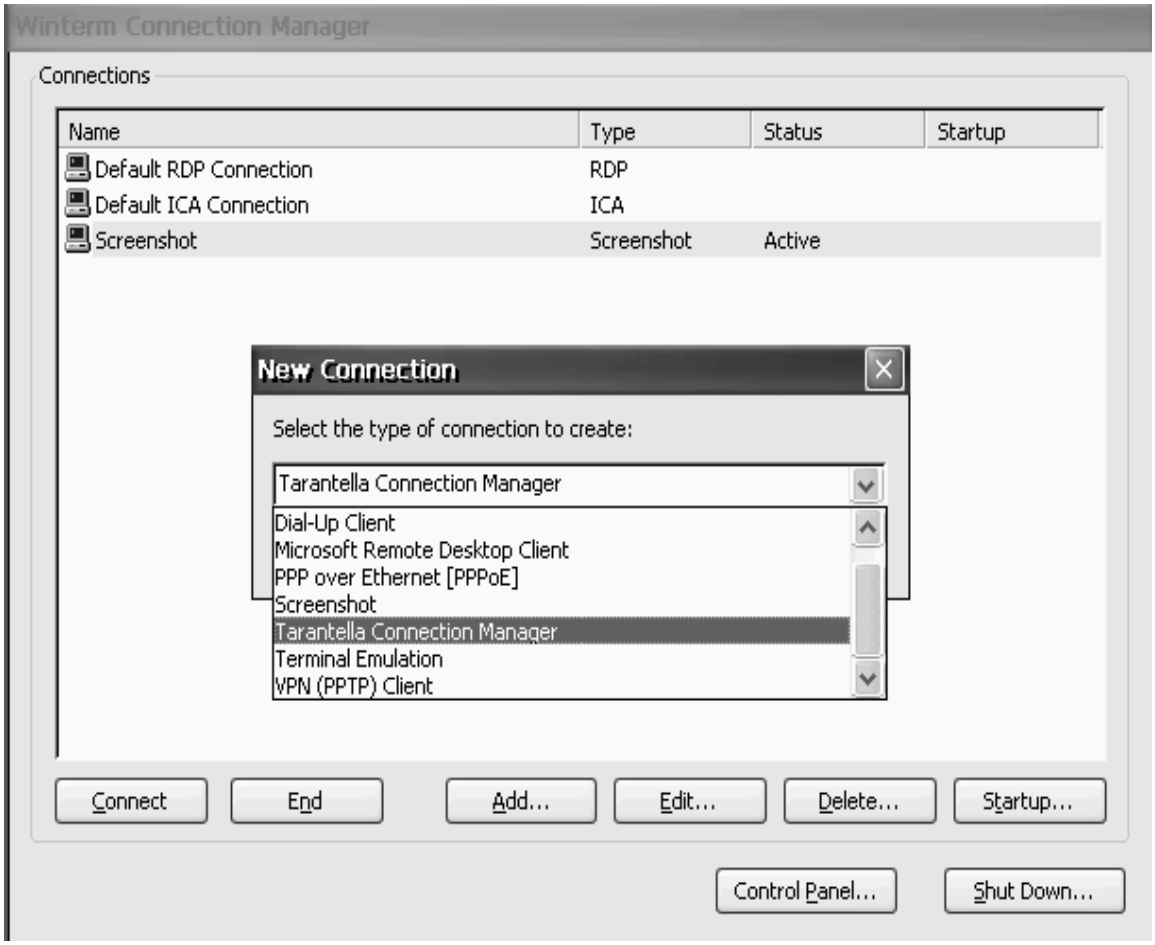
The Secure Global Desktop TSE CE add-on uses the RDP client, and the add-on will not work without it. So remember, do not remove the RDP client.

Configure the connection

To configure a Secure Global Desktop TSE connection on the Client machine:

1. Click **Add** on the **Winterm Connection Manager**.

2. In the **New Connection** dialog box, select **Tarantella Connection Manager** from the drop-down list and click **OK**.

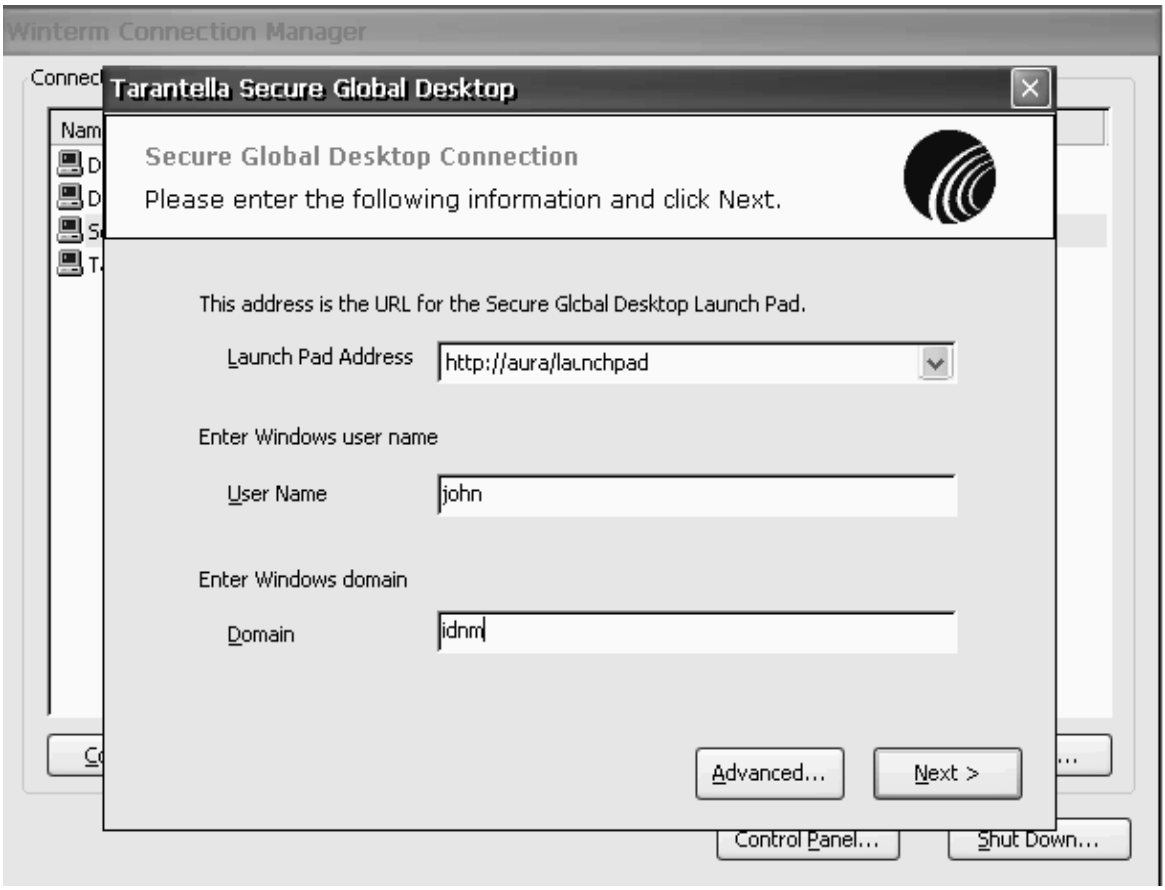


To establish the connection:

3. Type the URL of the Secure Global Desktop TSE Launch Pad that you intend to use in the **Launch Pad Address** field.

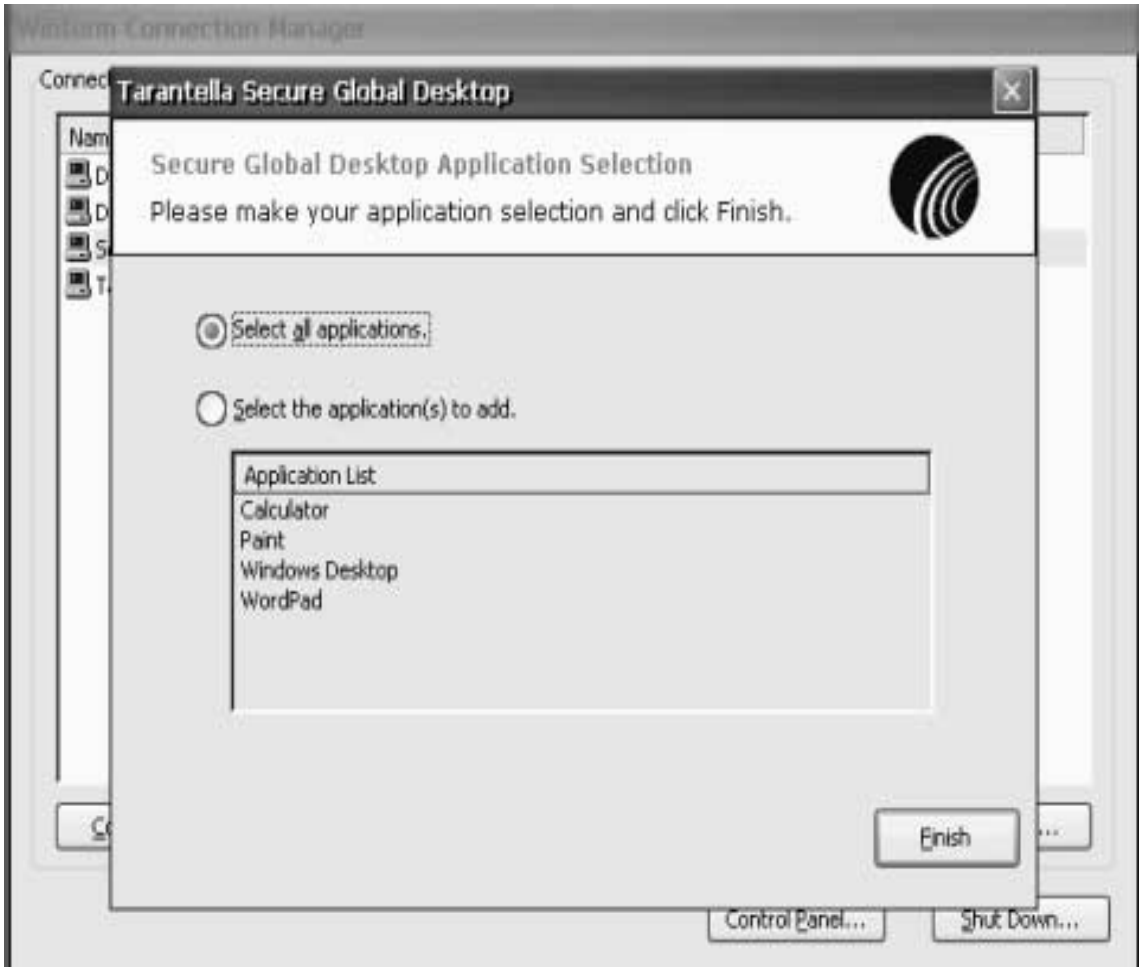
   For example:

`http://<servername>/launchpad`



4. In the **User Name** field, enter the user name.
5. In the **Domain field**, enter the domain that you will use. This domain should exist in Secure Global Desktop TSE; it should have been provisioned by the Secure Global Desktop TSE Administrator.
6. Click **Next**.
7. Choose the way you will select applications:
   - **Select All Applications** to select all the displayed applications. Go to Step 8.

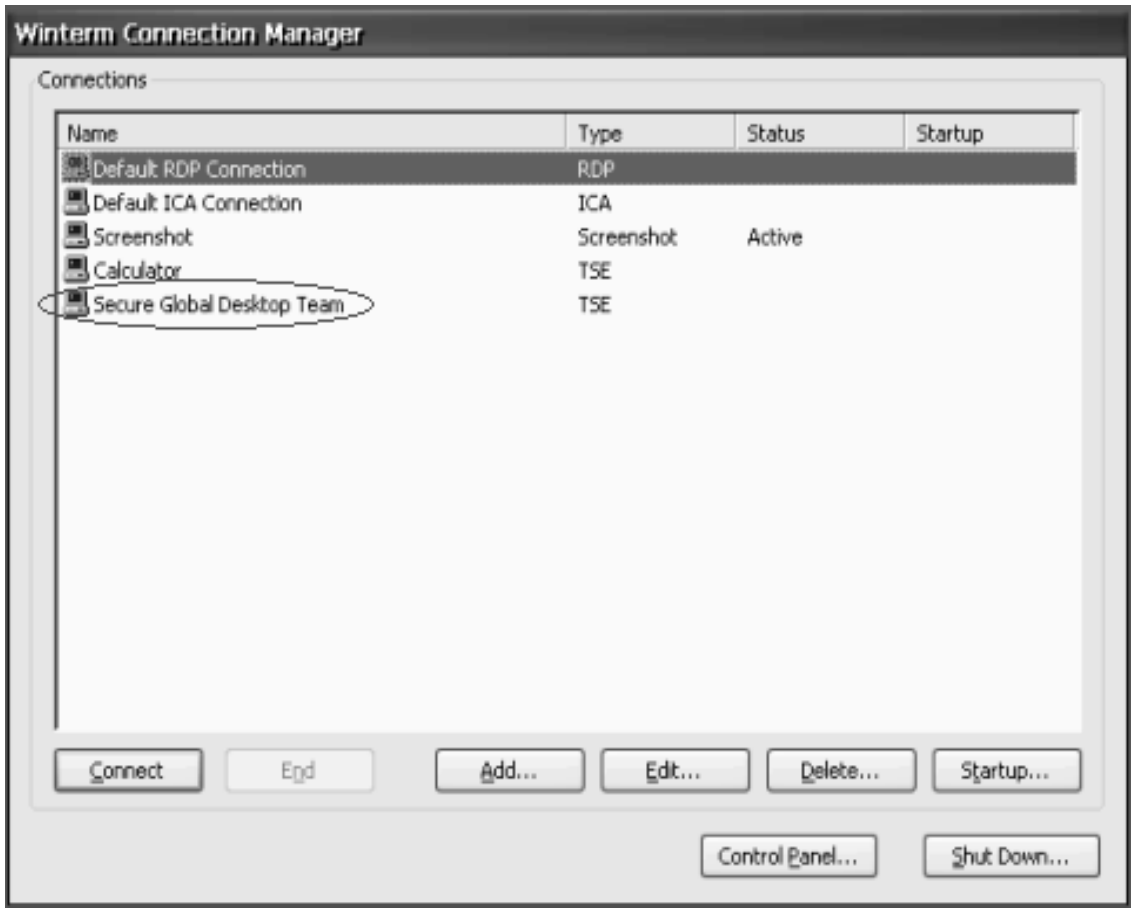
- **Select An Application** to select one application at a time. Go to Step 9.



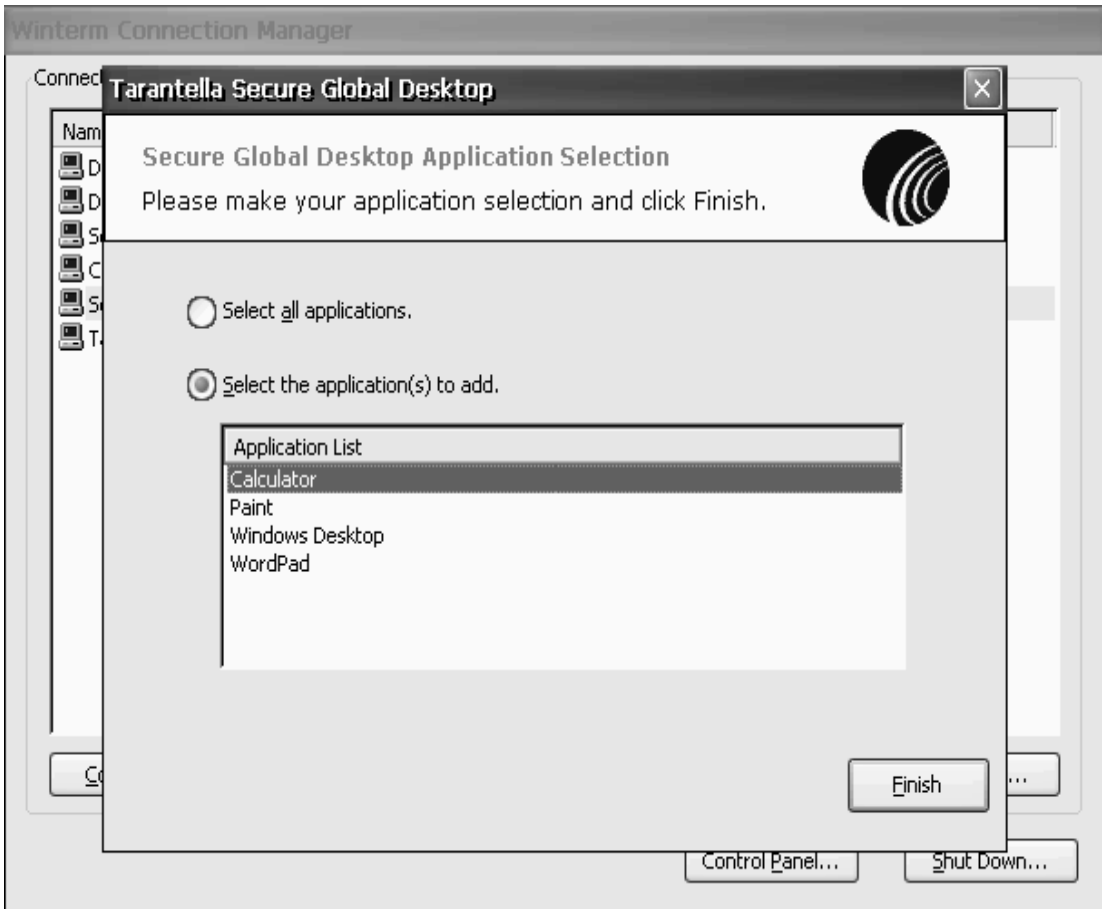
8. If you choose **Select All Applications**, click **Finish**.

   A single Secure Global Desktop TSE connection called **Secure Global Desktop TSE Team** appears on the **Winterm Connection Manager** dialog box. You will use the **Secure**

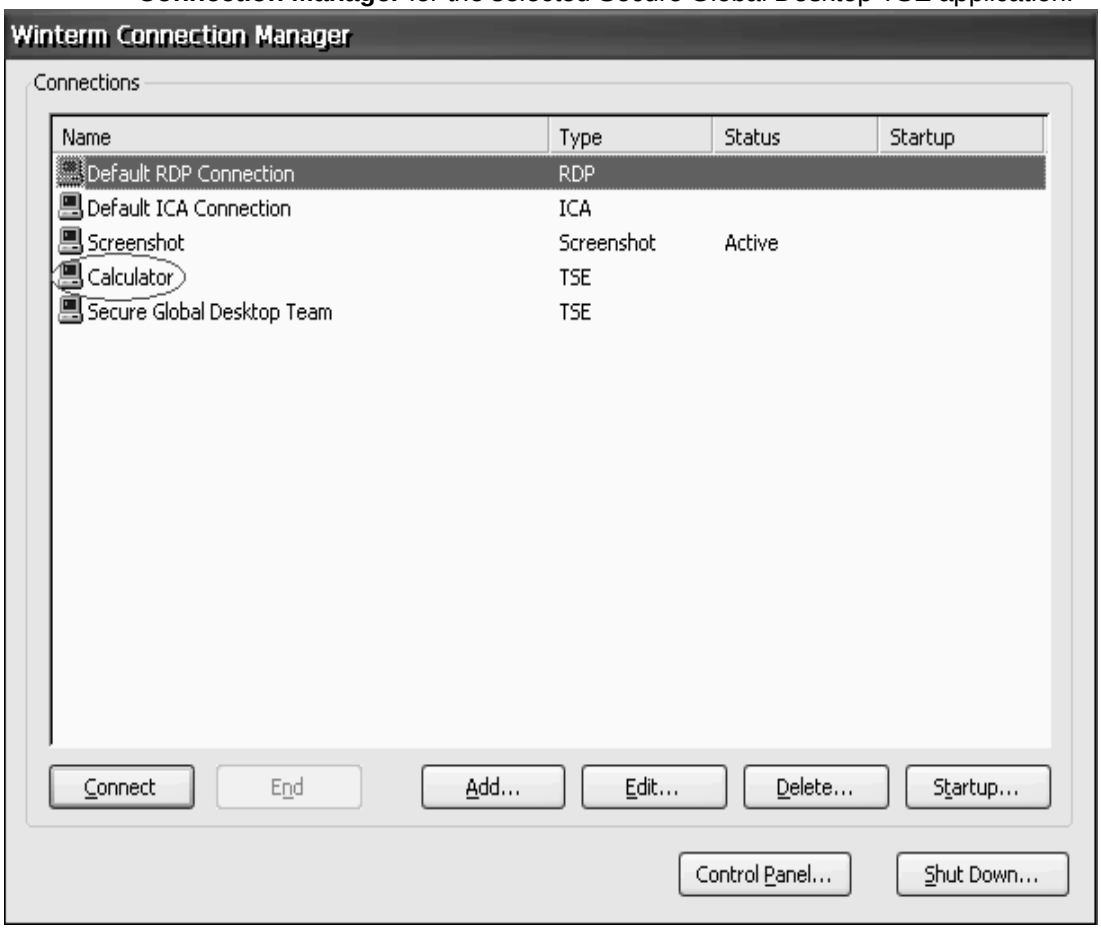
Global Desktop TSE Team connection to access the list all of the applications that are available to you from the Secure Global Desktop TSE server.



9. If you choose **Select An Application**, you must select the application you want to use, and then click **Finish.**



A single Secure Global Desktop TSE application connection appears in the **Winterm Connection Manager** for the selected Secure Global Desktop TSE application.



NOTE

Repeat this procedure to add connections to other individual applications.

Launching an application

1. To launch an application, double click a Secure Global Desktop TSE connection icon on the **Winterm Connection Manager**. The **Secure Global Desktop TSE Connection** (authentication) dialog box appears if you have not saved your password.

2. In the **Secure Global Desktop TSE Connection** (authentication) dialog box, enter your credentials and click **OK**.

3. If you double clicked a specific application connection icon in Step 1, the application is launched. If you clicked the **Secure Global Desktop TSE Team** Connection icon, the list of application is retrieved. Select an application and click **Launch** to launch the application.

Secure Global Desktop Resource Kit

What's in this chapter?

This chapter provides information about the Secure Global Desktop Resource Kit (SGDRK) and using the SGDRK commands.

Secure Global Desktop Resource Kit

This section addresses the Secure Global Desktop Resource Kit.

The CRK is a suite of command line tools that Secure Global Desktop administrators can use to deploy their Secure Global Desktop system or to maintain it. With the kit, the administrators can do the following:

- Update the Secure Global Desktop system identity
- Update the Secure Global Desktop database connection settings
- Make a transform file to instruct the MSI installer to push the Tarantella Client to client computers
- Refresh application shortcut icons
- Capture incident data for technical support

This kit provides features that supplement the features found in the Management Console. The kit provides some features that the Console cannot perform.

The CRK works with other command line tools such as the WTS tools and the Windows Task Scheduler. Administrators can construct batch files and scripts that use the CRK to help them maintain their server-based computing data centers.

This chapter deals with the following:

"Installing the CRK"

"Understanding the CRK"

"Using the CRK"

"Writing advance command lines"

Installing the CRK

The CRK has the same software and hardware requirements as Secure Global Desktop itself. Specifically, the software requirements for the CRK are:

- Secure Global Desktop 4.0
- Windows 2000 Server or Advanced Server with Service Pack 3, or Windows Server 2003

A Windows Installer file, CRK.MSI, packages the Secure Global Desktop Resource Kit. To install the kit, run the CRK install program and follow the instructions that appear during the install process.

Since some CRK commands work on individual servers rather than the team as a whole, we recommend that you install the CRK on all servers in your Secure Global Desktop team.

Understanding the CRK

This section discusses the major concepts that you will need to understand and use the CRK.

Exploring the CRK

As you read this section, you may want to follow along from the CRK. You can access this from the Windows Start menu; select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**. The shortcut opens a command prompt window. From the command prompt, type SGD-RK help to a get list of commands that CRK contains.

```
c:\program files\SGDRK>sgd-rk help
Secure Global Desktop Resource Kit (version 4.0). Try:
    SGD-RK command [args...]
where the following are commands:
   applications      List all the applications in the system
   client-transform  Generate a Tarantella Client transform
   connections        List all the connections monitored by the system
   count             Count the rows of output from another
   domains           List all the domains in the system
   for               Loop on the values of another command
   groups            List all the groups in the system
   help              Print a help message
   identity           Print or set the identity account for the system
   if                Test an environment variable's value
   os-info           Print operating system information
   ous               List all the organization-units in the system
   print             Print arguments to the output file
   refresh-icons     Refresh an application's icon
   registry          List Secure Global Desktop registry values
   servers           List all the servers in the system
   sql               Print or set the SQL connection string
   support-info      Report information for a support incident
   sync-database     Synchronize to domain information
   team              Print information about the server's team
```

```
   test              Test the exit-code of another command
   tracing           Print and set the development tracing level
   users             List all the users in the system
   web-port          Print or set the ports for the Secure Global Desktop
Web sites
```

To view detailed information about a particular command, type **SGD-RK help <command>**. To view detailed information about all of the commands type **SGD-RK help /a**.

For example,

```
c:\program files\SGDRK>SGD-RK help web-port

WEB-PORT -- Print or set the ports for the Secure Global Desktop web
sites

Syntax

  SGD-RKSGD-RK web-port [/h] [/q] [/action:set] [/http:Value] [/
https:Value]

Arguments

  /h            Suppress the header of the information table

  /q            Quiet mode

  /action:set   Set the ports

  /http         The port number for HTTP communication

  /https        The port number for HTTPS communication

Remarks

This command prints or sets the ports that Secure Global Desktop
components and clients use to communicate to the Secure Global Desktop
web sites. This command   only affects the port settings for Secure
Global Desktop. Use the Internet Services Manager to change the IIS
settings.

Examples

    SGD-RK web-port

    SGD-RK web-port /action:set /http:80 /http:443

Requirements

    Secure Global Desktop web server
```

Specifying options

Most commands have options that alter their behavior. Like many command line tools, CRK options begin with a slash character. There are two types of options:

- Flags
- Named values

Flags are single letters that turn on a particular command mode. If a flag is present, then the command uses the flag's associated mode. Administrators can combine flags together, so specifying **/fh** has the same effect as specifying **/f /h**.

Common flags are:

TABLE 19. Flag Options in CRK

Option	Usage
/h	Suppress headers in tables
/q	Quiet mode, answer yes to all prompts
/f	Answer yes to all prompts

Named value options follow the form `/<name>:<value>`, where a colon separates the name of the option and value of the option. For example, many commands use the `/action:set` option to indicate the set value of the action option. If a value has spaces in it, use quotes to surround the whole option. The option `/description:Secure Global Desktop Team on Server` has a value of *Secure Global Desktop Team on Server.*

Printing information

The CRK prints information in a tab-delimited table format. The tab-delimited format is easy to read as well as to import into spreadsheets and databases. The first row of the table contains the column names for the table, while the following rows contain the values of the table. If a /h flag is specified, the header row is omitted.

The CRK tries to format tables so that columns align correctly. It assumes that tabs are set every eight characters, which is true for the command prompt. To make columns line up, the CRK may insert multiple tab characters between values. So, when importing a CRK table into a Microsoft Excel spreadsheet, use the treat successive delimiters as one option. For blank values, the CRK will place a space character.

If a row exceeds the width of the command prompt window, the command prompt will wrap the row's information to the next line. When this happens, it is easier to read the information if the information is first saved to a file and then viewed using another program such as Windows Notepad. To do this, use the command redirection feature of the Windows command prompt. For example, type SGD-RK users > users.txt to save the list of users in a file named users.txt.

Checking administrator rights

For any command that accesses or modifies the Secure Global Desktop system settings, the CRK will check to see that the user who invokes the command, the logged on user, is a member of the Secure Global Desktop Administrators group. This check prevents unauthorized users from using the CRK to alter your Secure Global Desktop system.

Stopping a command

It is possible to abort and stop a command as it executes. Like many command line tools, the CRK stops when you press the Ctrl key and C key in combination.

Using the CRK

This section provides examples on how to use the CRK.

Generating a transformed client

The administrator can use the Secure Global Desktop Resource Kit to generate a Tarantella Client transform, which can be pushed to client computers through GPO. The client-transform command

creates a Windows Installer transformed file that can help install the Tarantella Client software without requiring the user to browse a Launch Pad web site. The source for the transform is the SGD-TSE-Client400.msi file which is found in Secure Global Desktop's depot folder by default. The transformed file can be used in an Active Directory group policy object (GPO) or directly from command line.

The command takes the following parameters:

- url: URL for the launch pad web site

You can also specify the following optional parameters:

- mst: Output .mst filename, default used if omitted
- msi: Source .msi file, default used if omitted
- /q option runs the command in silent mode
- domain: Domain to use for the launch pad web site

To transform a client

1. Select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**.
2. Type

   ```
   SGD-RK client-transform /url:http://<webserver name>/launchpad /
   domain:TestDomain /mst:SGD-TSE-Client400.mst /msi:SGD-TSE-
   Client400.msi
   ```

3. To install the resultant mst file on client computer, type

   ```
   msiexec /i SGD-TSE-Client400.msi TRANSFORMS="SGD-TSE-Client400.mst"
   ```

NOTE

To push the msi through GPO or other methods, please refer to the corresponding GPO or other relevant documentation.

Synchronizing domain information with Task Scheduler

The CRK contains a command to synchronize the Secure Global Desktop provisioning information with recent changes made to the network domains. To automate this operation, administrators can schedule this operation as a daily task on a Secure Global Desktop server using the Windows Task Scheduler.

1. Select **Start>Settings>Control Panel>Scheduled Tasks**.
2. Launch the **Add Scheduled Task** wizard. Click **Next**.
3. Click **Browse** and select the SGD-RK.exe program. Click **Next**.
4. Specify the frequency and start time. Click **Next.**
5. Specify a Secure Global Desktop administrator’s account for the task’s user account and click **Next**.
6. Select **Open advance properties for this task when I click Finish** and click **Finish**.
7. On the **Task** property tab, in the **Run** field, add `sync-database /q`. If SGD-RK.exe is installed on the C drive, the field should read

   ```
   “C:\Program Files\SGDRK\SGD-RK.exe" sync-database /q
   ```

8. Click **OK**.

Administrators can see the results from the last time the task scheduler ran a task in the Last Results property of the task. Like other command line tools, SGD-RK.exe will exit with a zero status after a successful run.

Altering the Secure Global Desktop Identity account

The Secure Global Desktop identity account is the security context that the Secure Global Desktop components use. CRK contains an identity command that changes the identity account or updates the account's password.

1. Select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**.
2. Type

```
SGD-RK identity /action:set /user:<account> /domain:<domain> /
password:<account_password>
```

The command will respond by prompting for confirmation that you want to proceed. If you provide confirmation, then the command will take a few minutes to complete.

Adjusting the ports used by the Secure Global Desktop web sites

By default, Windows Internet Information Services (IIS) uses port 80 for HTTP traffic and port 443 for HTTPS traffic. Administrators may alter the ports used by IIS in the Internet Services Manager. However, if they change the ports, they need to notify Secure Global Desktop of this port change using a CRK command.

The CRK contains the following command to alter the web ports that are used by Tarantella Clients and components to talk to the Secure Global Desktop web sites.

1. Select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**.
2. Type

```
SGD-RK web-port /action:set /http:<port> /https:<port>
```

Migrating to a new Secure Global Desktop Database server

Occasionally, it may be necessary to move the Secure Global Desktop database, CanaveralDB, from one server to another. The CRK contains a command to alter the connection string that a Secure Global Desktop components uses to connect to its SQL database.

The first step when migrating a Secure Global Desktop database is to back up the database on the current SQL Server and to restore it on the new database server. See the SQL Server documentation for details on performing this operation.

NOTE

The database you will be using as the new database should not already be in use in the Secure Global Desktop team as a backup database.

Next, configure the servers on the team to use the new database. On each server in the Secure Global Desktop team:

1. Select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**.
2. Type

   ```
   SGD-RK sql /action:set /server:<server_name> /database:<db_name>
   ```

Reporting a support incident

When reporting a problem to Tarantella support, it is important to provide as much information about the Secure Global Desktop configuration as possible. The CRK contains a command to print information that is important to technical support. Save the support information to a file and email the file to support at support@tarantella.com.

1. Select **Start>Programs>Secure Global Desktop Resource Kit>Secure Global Desktop Resource Kit Command Prompt**.
2. Type

   ```
   SGD-RK support-info > support.txt
   ```

NOTE

You should disable all virus checking software when running the command. The CRK support-info tool may take a few moments to complete.

Writing advance command lines

We designed the CRK not only to provide useful commands, but also to allow each command to work with other commands and with other command line tools. This section discusses advance usage of the CRK.

Specifying multiple commands

A single invocation of the SGD-RK tool can invoke multiple commands. When specifying multiple commands on a single command line, each command should begin with a double slash, so the SGD-RK tool can distinguish it from command options.

The SGD-RK tool will execute the commands in left to right order. To refresh-icons and then sync the database to the domain, type `SGD-RK //refresh-icons //sync-database`. Reversing the command order would reverse the order in which these commands execute.

Looping

The **for** command is a special command that uses another command. The **for** command reads the tab-delimited table that one command produces and invokes the remaining commands in the command line one time for each row of the output table.

Any command that produces a tab-delimited table may be used with the **for** command. For example, the **applications** command can be used alone to list all the applications in the Secure Global Desktop system or it can be used with the **for** command to invoke the remaining command, from the command line, once for each application in the Secure Global Desktop system.

Like the **for** command, the **count** command loops on the output of another command. Instead of invoking the remaining commands on the command line, the **count** command counts the rows in the output table and prints the count.

```
c:\program files\sgdrk>SGD-RK applications
ApplicationName ApplicationPath
Pinball         C:\Program Files\Windows NT\Pinball\PINBALL.EXE
Solitaire       C:\WINNT\system32\sol.exe
c:\program files\SGDRK>SGD-RK //for applications //print Ha
Ha
Ha
```

```
c:\program files\sgdrk>SGD-RK //count applications
Count
2
```

Passing information between commands

The **SGD-RK** tool will substitute options delimited by # characters with values stored in environment variables. For example, the `SGD-RK print #computername#` command will print the current value of the computer name environment variable. To view all the current environment variables, type **set** at the Windows command prompt.

Before invoking the other commands on the command line, the **for** command will add environment variables for each column in the output table. As the **for** command loops on each row of the output table, it will update these environment variables with the values from the current row. This feature enables the administrator to use the output of one command as the input to another command.

```
 c:\program files\sgdrk>SGD-RK applications
ApplicationName ApplicationPath
Pinball         C:\Program Files\Windows NT\Pinball\PINBALL.EXE
Solitaire       C:\WINNT\system32\sol.exe
c:\program files\sgdrk>SGD-RK //for applications //print
#ApplicationName#
Pinball
Solitaire
```

Branching

The **if** command will compare values of strings and numbers. If the comparison evaluates positively, then command processing continues. If the comparison evaluates negatively, the command processing stops and the SGD-RK tool exits.

The following table displays the comparison operators supported by the **if** command:

TABLE 20. Comparison Operators supported by the IF command

Operator	Usage
eq	Test for equality. Treat values as integers.
ne	Test for non-equality. Treat values as integers.
gt	Test for greater than. Treat values as integers.
lt	Test for less than. Treat values as integers.
ge	Test for greater than or equal to. Treat values as integers.
le	Test for less than or equal to. Treat values as integers.
Is	Test for equality. Treat values as strings.
isnot	Test for non-equality. Treat values as strings.
like	Test the first string to find lines that contains the second string.

```
C:\Program Files\SGDRK>SGD-RK connections
Status  ServerName      SessionId       Age
```

```
2       RHAWES-PAQ      1               5466
2       RHAWES-PAQ      4               46
C:\Program Files\SGDRK>SGD-RK //for connections //if #Age# gt 500 //
print Session #SessionID# is older than 500 minutes
Session 1 is older than 500 minutes
C:\Program Files\SGDRK>SGD-RK //for connections //if #Age# gt 50000 //
print Session #SessionID# is older than 50000 minutes
```

Like the if command, the **test** command will continue or terminate command processing depending on the outcome of the test it performs. Unlike the if command, which tests values, the test command tests the exit code of another command, a command that it invoked. If the exit code is zero, command processing continues. If the exit code is not zero, command processing terminates.

Working with other tools

The SGD-RK tool of the CRK can also invoke other command line tools. When it processes a command name, the SGD-RK tool first looks in its catalog of built-in commands for the command. If it does not find the command in its catalog, then it searches the path environment variable for an external tool that has the command, and then the SGD-RK tool invokes it. For example, the SGD-RK tool can invoke the terminal services command line tools such as the msg tool, which sends a message to a user of terminal services.

```
C:\Program Files\SGDRK>SGD-RK msg MIKES meet at 1PM today
```

Putting it all together

Taken together, these advanced features allow administrators to build powerful command lines that use the built-in commands of CRK in combination with other tools. The example below uses the CRK to disconnect all Secure Global Desktop connections that are older than 500 minutes. It uses the internal connections command and the external tsdiscon tool. It demonstrates the looping and parameter passing features of the for command. It shows how the if command can qualify the execution of other commands.

```
C:\Program Files\SGDRK>SGD-RK connections
Status  ServerName      SessionId       Age
2       RHAWES-PAQ      1               5466
2       RHAWES-PAQ      4               46
C:\Program Files\SGDRK>SGD-RK //for connections //if #Age# gt 500 //
tsdiscon #SessionID# /SERVER:#ServerName#
```

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, California.

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 21. 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

Secure Global Desktop Clients

What's in this appendix?

This appendix provides information on Secure Global Desktop Clients. It tabulates the Secure Global Desktop features along with their availability for various client operating systems.

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 22. Secure Global Desktop Clients and Features

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

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

TABLE 23. Connection Settings support on different Operating Systems

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	Yes	Yes	No	No	Yes	Yes	Yes	No	No
CE 4.x	No	Yes	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.

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 24. Abbreviations

Abbreviation	Meaning
ADSI	Active Directory Service Interfaces
API	Application Programming Interface
ASP	Active Server Pages
COM	Component Object Model
DCOM	Distributed COM
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTML	Hypertext Markup Language
IFS	Internet File Sharing
IIS	Internet Information Services
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
SGD	Secure Global Desktop
SMB	Server Message Block
SPR	Single Port Relay

TABLE 24. Abbreviations

Abbreviation	Meaning
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UI	User Interface
UPN	User Principal Name
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

COM+ Components and Secure Global Desktop Services

What's in this appendix?

This appendix lists the Secure Global Desktop Services and the COM+ Components.

COM+ Components

The COM+ table lists system-level applications that are available on-demand.

TABLE 25. COM+ components in Secure Global Desktop

COM+ Component	Description
Secure Global Desktop Database Access Engine	Links to the Secure Global Desktop database
Secure Global Desktop Domain Engine	Gets information from the domains
Secure Global Desktop License Engine	Enforces product key and third-party licenses
Secure Global Desktop Management Engine	Regulates the Console operations
Secure Global Desktop Application Engine	Application provisioning and launch information
Secure Global Desktop Jobs Framework Engine	Executes submitted jobs

Secure Global Desktop Services

The Secure Global Desktop Services table highlights continuously available background processes.

TABLE 26. Secure Global Desktop Services

Services	Description
Secure Global Desktop Engine Service	Resides on all servers in the Secure Global Desktop team. This service provides the ability to manage all the servers in the team.
Secure Global Desktop Load Balancer Service	Resides on all the Load Balancer Servers in the Secure Global Desktop team. This service provides application load balancing to the clients requesting an application in the Secure Global Desktop team.

TABLE 26. Secure Global Desktop Services

Services	Description
Secure Global Desktop Monitor	Resides on all Application Servers in the Secure Global Desktop team. This service provides application management, control, performance, and monitoring on the Application Servers, and communication with the Load Balancer.
Secure Global Desktop Single Port Relay	Resides on all the Relay Servers in the Secure Global Desktop team. This service manages the Secure Global Desktop relay server operations, thereby allowing single port traversal.