TARANTE//A®

What's New in Secure Global Desktop Terminal Services Edition v4

Product Documentation
October 15, 2004

Contents

List of Figures

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.

1.1 *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 un-trusted 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 from 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.

1.2 *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 SGDEngine 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 ("Canaveral database') from the Console.
- The monitored status of the DMZ SPR is read from the TSE database ("Canaveral 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.

1.3 *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 Chapter 2, 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.

1.4 *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 (SGD-TSE) that consists of a SGD-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 SGD 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 SGD-TSE components when it has the DMZ Relay Server role installed on it.

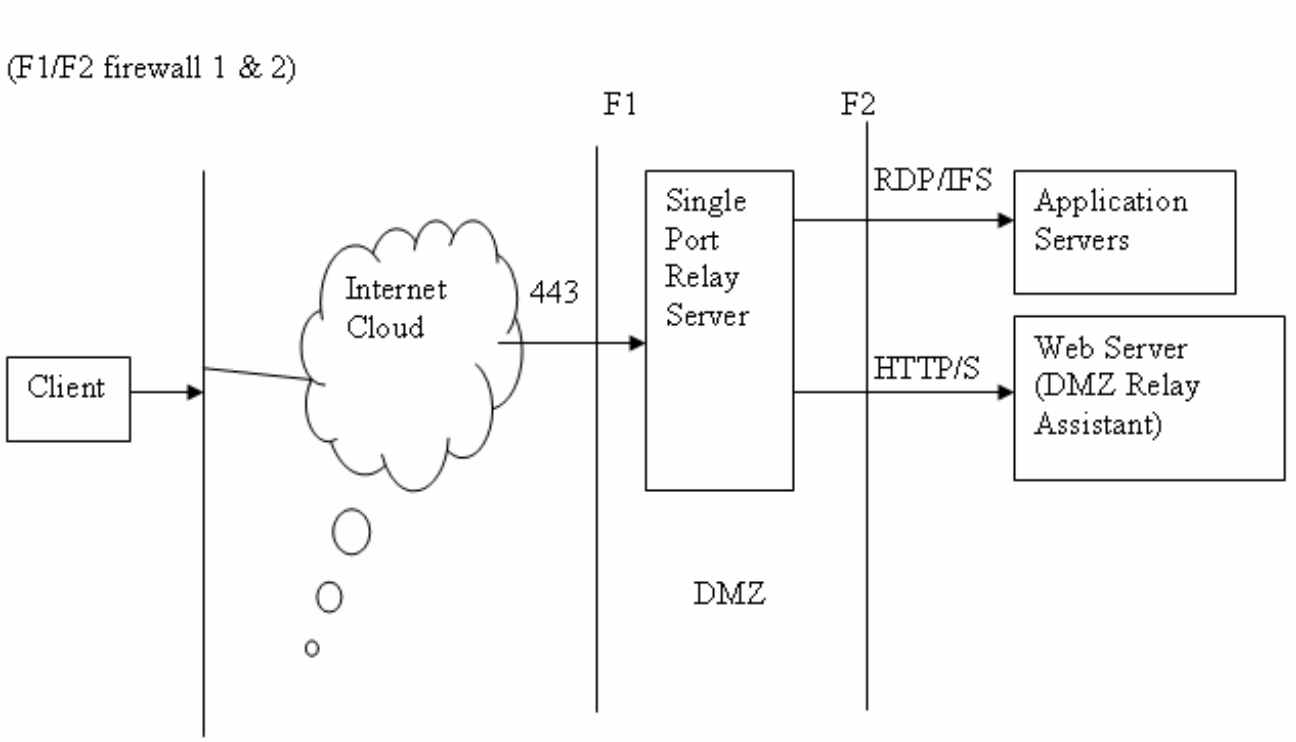


Figure 1: Single Port Relay Server in the DMZ

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 1 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.

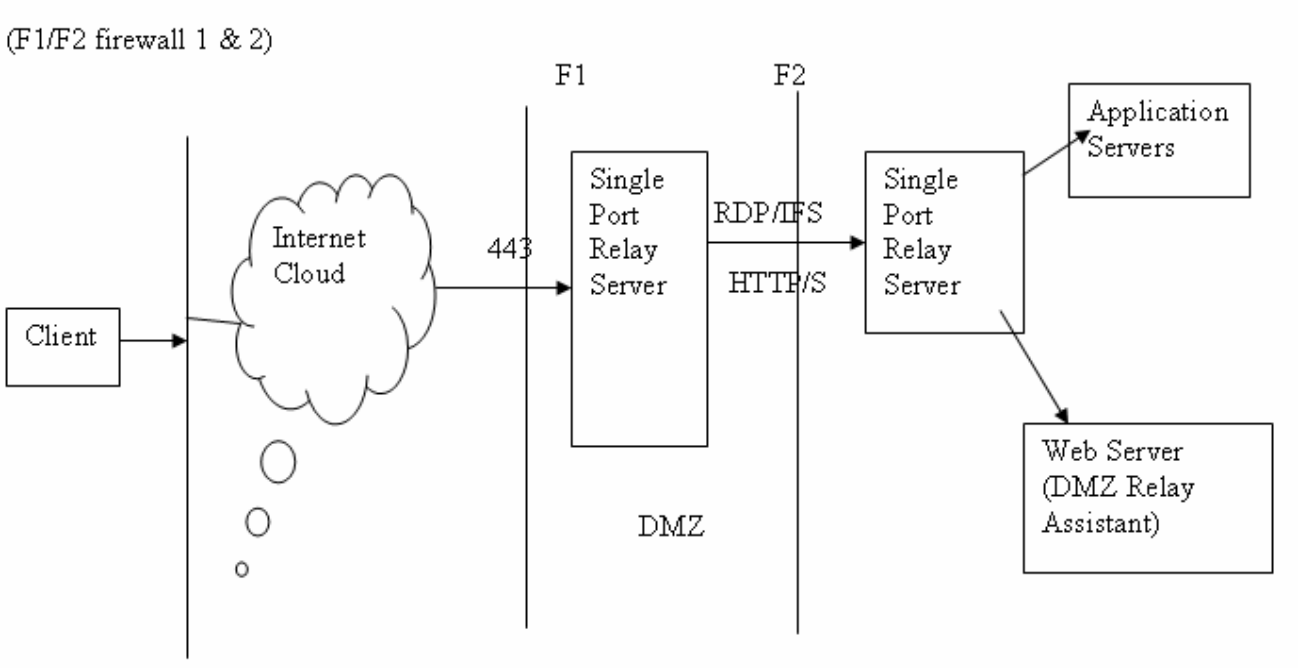


Figure 2: Cascaded SPR with Single Port Relay Server in the DMZ and in the Secure Network

1.5 *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 ('Canaveral') 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.

1.6 *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 SGD-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 Application 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).

1.7 *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 SGD-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, SGD-TSE routes the client connections to the Internal IP Address.

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 the DMZ SPR.

Disable Best Internal Address Discovery
By default, SGD-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 then clear this check box.

Internal Address to Use
Members (servers) of the SGD-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 configuration changes every 2 minutes, which means it takes at least 2 minutes or more for DMZ SPR configuration values 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 SGD-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.

1.8 *DMZ SPR Resource Kit*

To install the SGD-TSE Resource Kit on a DMZ SPR server in the DMZ, the administrator can 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.

2 Ticketing Authority

2.1 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 SGD-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.

2.2 What and How is the New Ticketing Authority Protecting Against?

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.

2.3 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 3):

- 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.

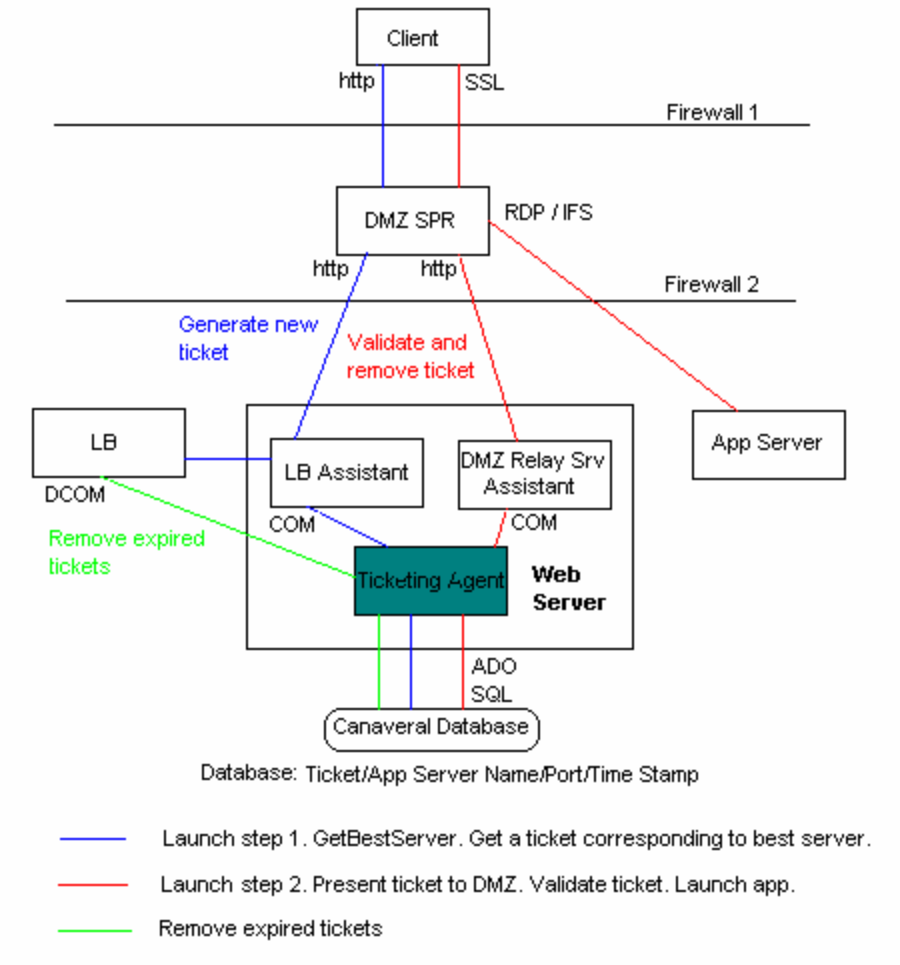


Figure 3: Ticketing Authority

3 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.

3.1 *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 Restriction
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 Restrictions	Low Restrictions	Medium Restrictions	Highest Restrictions
Disable Windows Explorer's default context menu.	False	True	True	True
Disable registry editing tools.	False	True	True	True
Disable the 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

Lockdown Policy Setting	No Restrictions	Low Restrictions	Medium Restrictions	Highest Restrictions
Remove Search menu from Start Menu.	False	False	True	True
Disable context menu for taskbar.	False	False	Yes	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 from 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 the Tools menu.	False	False	False	True
Prohibit user from changing My Documents path.	False	False	False	True
Remove common program groups from Start Menu.	False	False	False	True
Remove Documents menu from Start Menu.	False	False	False	True
Remove user's folders from the 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 SGD-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 message explaining 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.

NOTE: 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 right-clicks 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 Management snap-in to view and change drive characteristics. Also, see the Prevent access to drives from My Computer setting. **NOTE:** 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 users from using programs to access local and network drives. And it does not prevent them from using the Disk Management snap-in to view and change drive characteristics. Also, see the Hide these specified drives in My Computer setting.

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 the Open 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 to 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. **TIP:** 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 setting. Also, see the Do not keep history of recently opened documents and Clear 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 Start menu, click the Advanced tab, and then, under Start menu items, click the Favourites menu. If you are using the classic Start menu, click Display Favourites under Advanced Start menu options. **NOTE**: The items that appear in the Favourites menu when you install Windows are preconfigured by the system to appeal to most users. However, users can add and remove items from this menu, and system administrators can create a customized Favourites menu for a user group. **NOTE:** 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.

4 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 which 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 SGD-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 SGD-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.

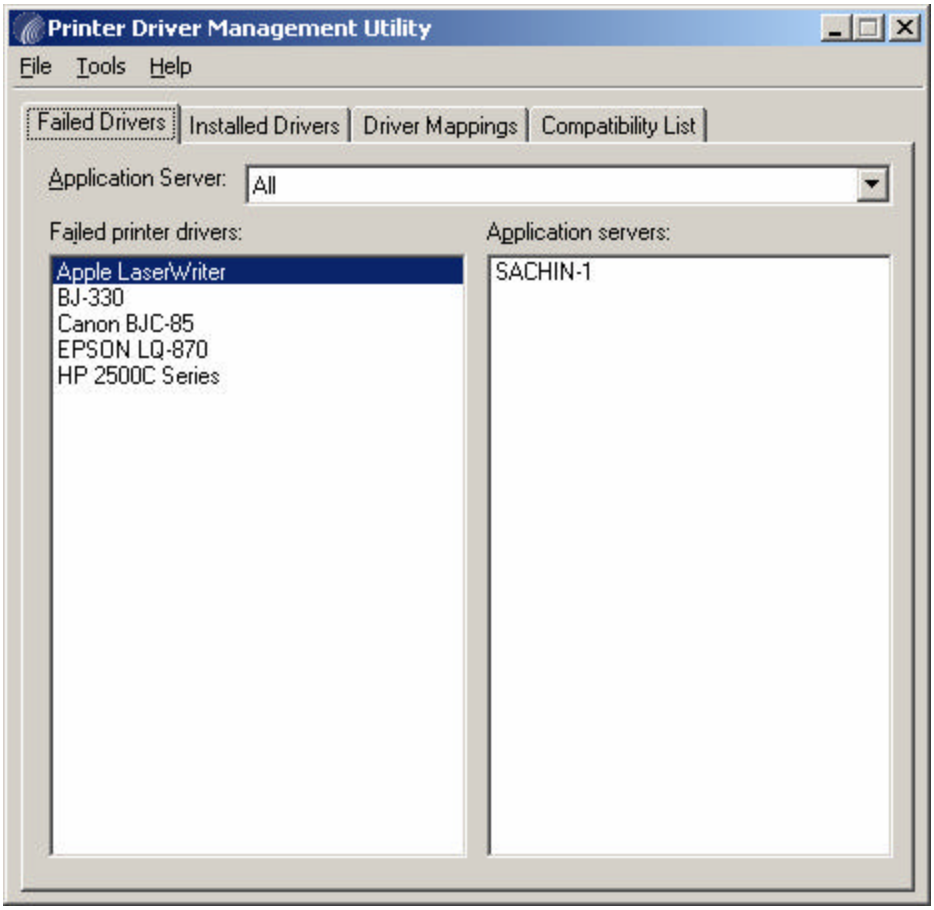
4.1 *User Interface*

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

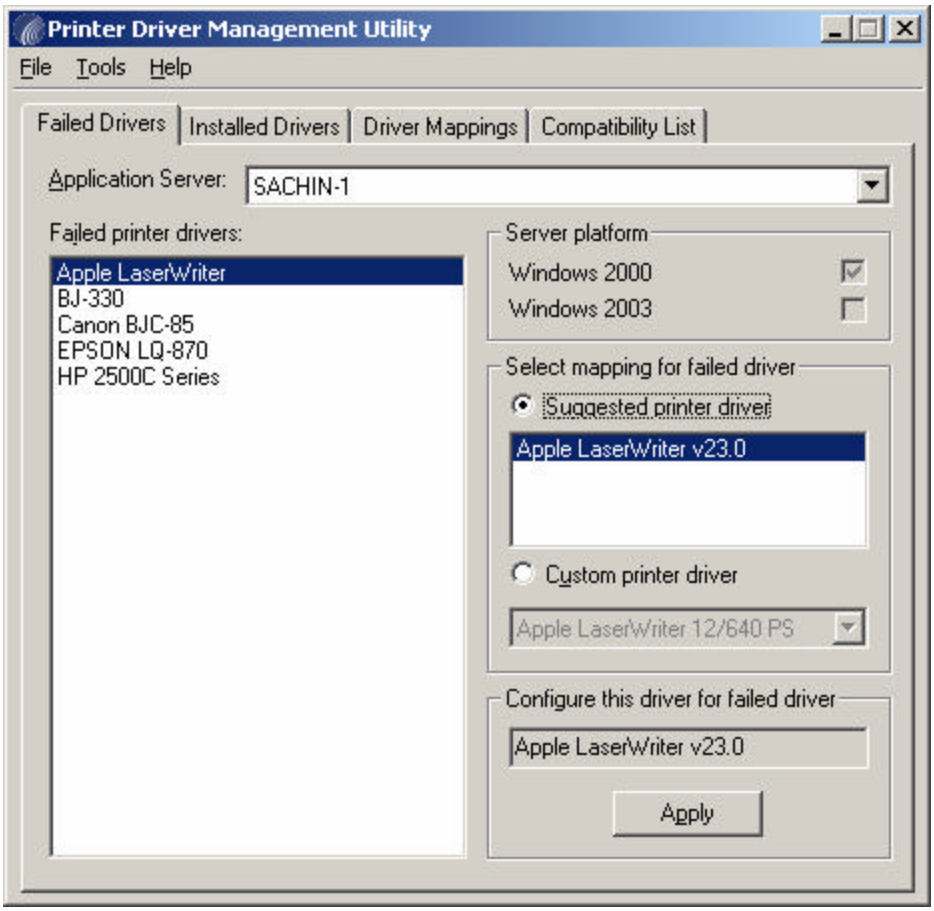
This tab shows a list of failed drivers for the SGD-TSE team and allows a user to map an alternate driver for the failed one.



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 application 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 SGD-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.

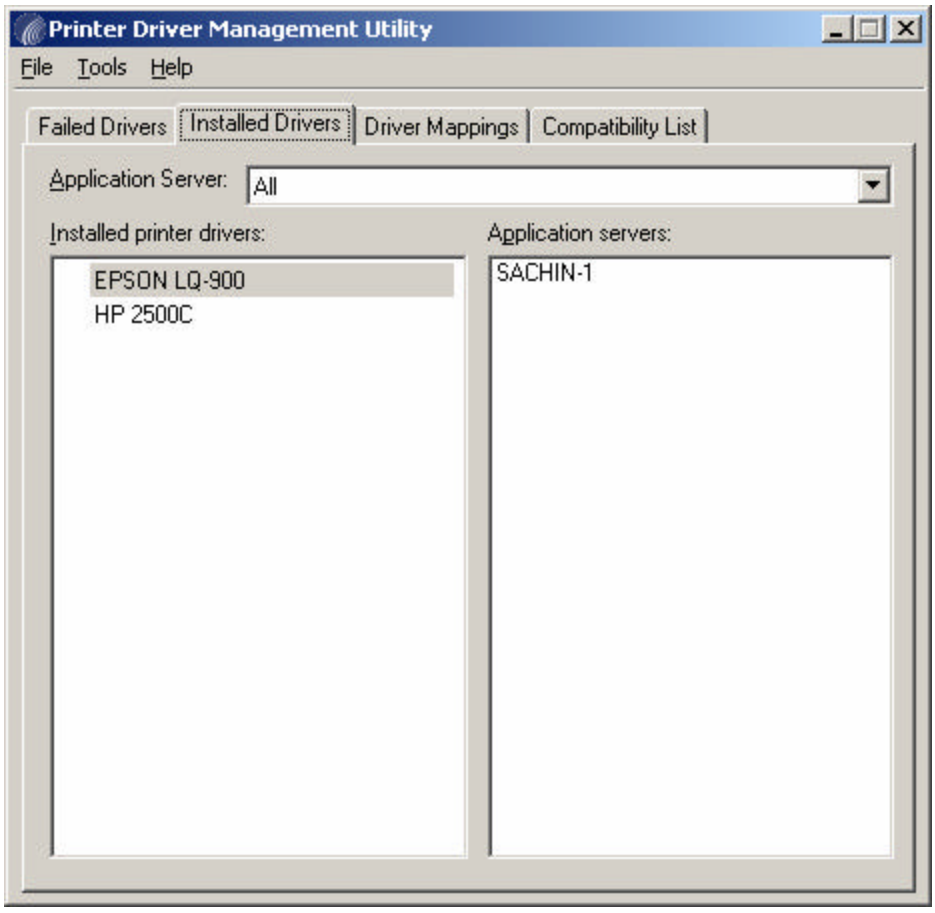
When the user hits the **Apply** button the mapping is done and added to the SGD-TSE database. The new setting is displayed in the **Driver Mappings** tab.

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 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 application 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.

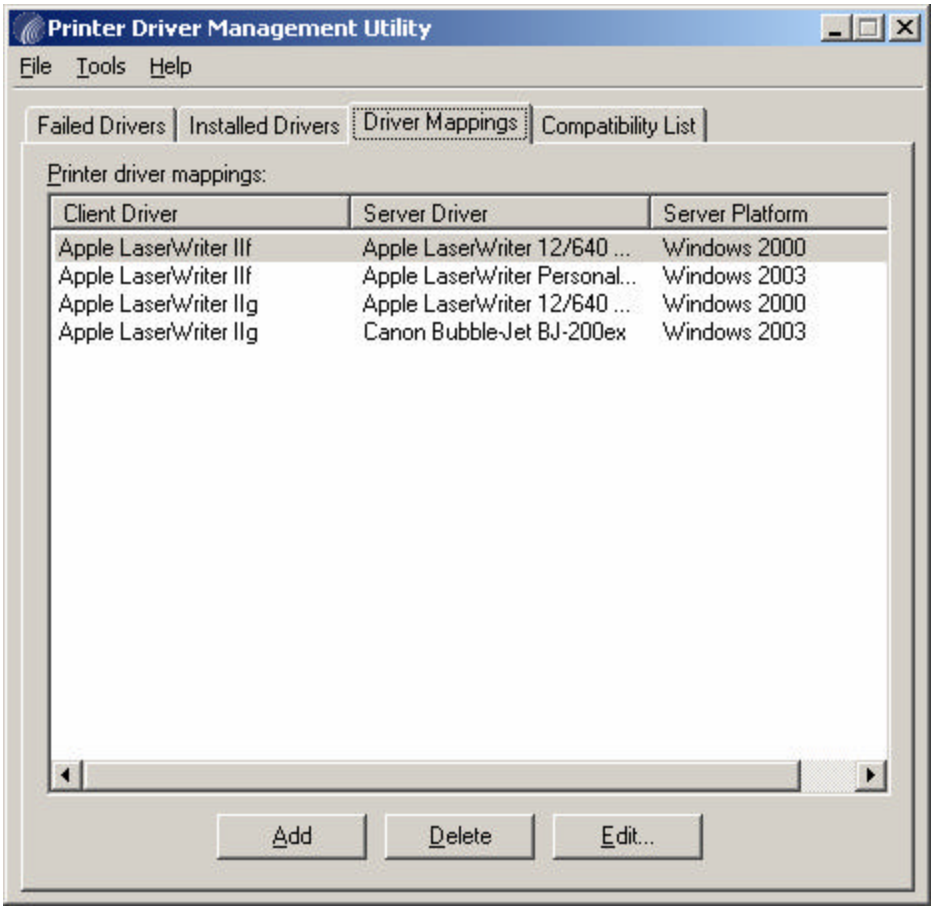
Replicate installed driver
Select a server from the **Application Servers** combo box. To replicate a driver on all remaining application servers in the team that have the same operating system installed as that of the selected server, right click the driver and select **Replicate** menu item. The utility 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: The driver installation will fail if the driver is in use, i.e. 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 SGD-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.

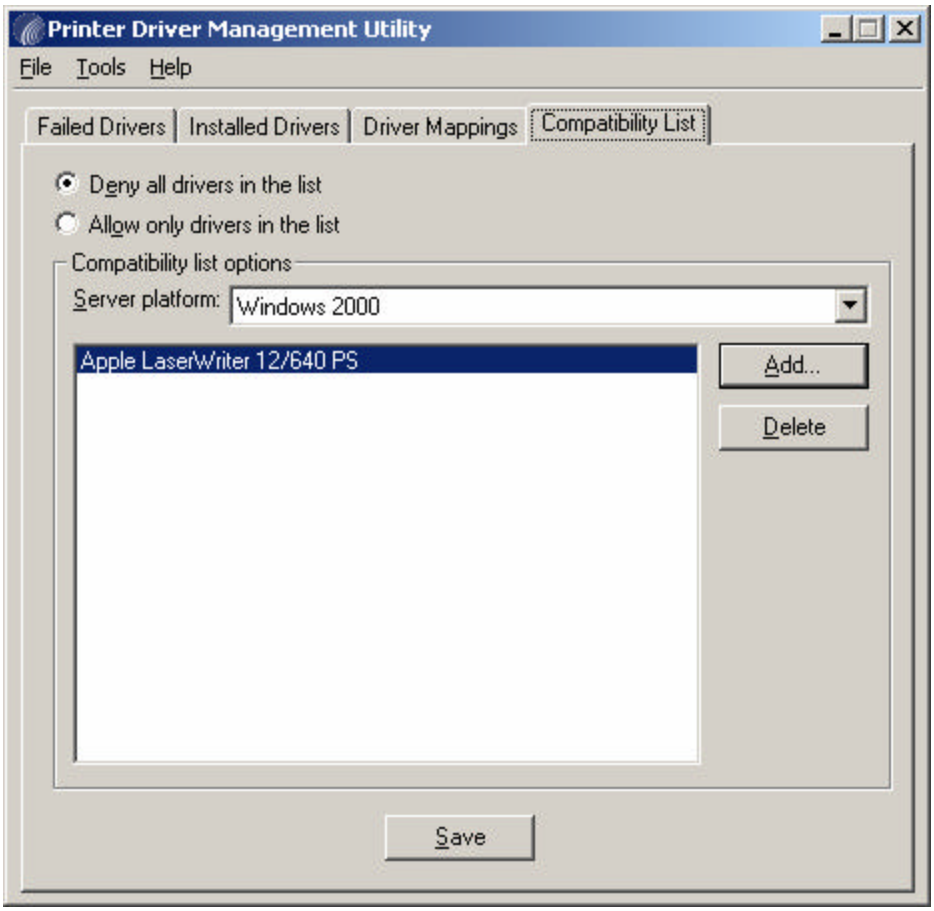
Edit custom mapping

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.

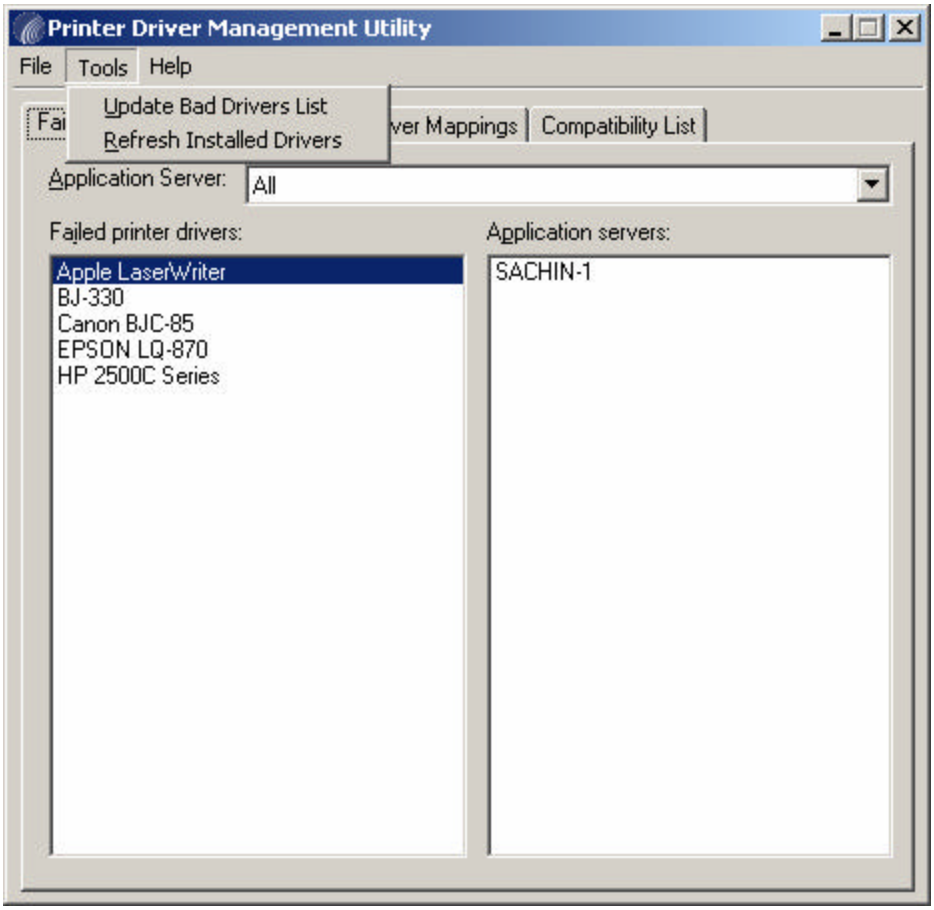
To save the list into the database click the **Save** button. A message box pops up asking for confirmation. Click **OK** to save the list.

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.

5 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.

6 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".

7 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 SGD-TSE team. These tasks can be scheduled to run at a specified time and on the specified server(s).

SGD-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 SGD-TSE database with actual domain objects. This will run daily at 3 AM.

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

7.1 *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 SGD-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.

7.2 Remove Task

The **Remove Task** action allows you to remove an existing Task from the SGD-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.

7.3 *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".

7.4 *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".

7.5 *Add Servers*

You can add servers from the SGD-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: You can add multiple tasks to multiple servers at one time by selecting multiple tasks to add and selecting multiple servers to receive.

7.6 *Remove Servers*

To stop Tasks from running on servers:

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

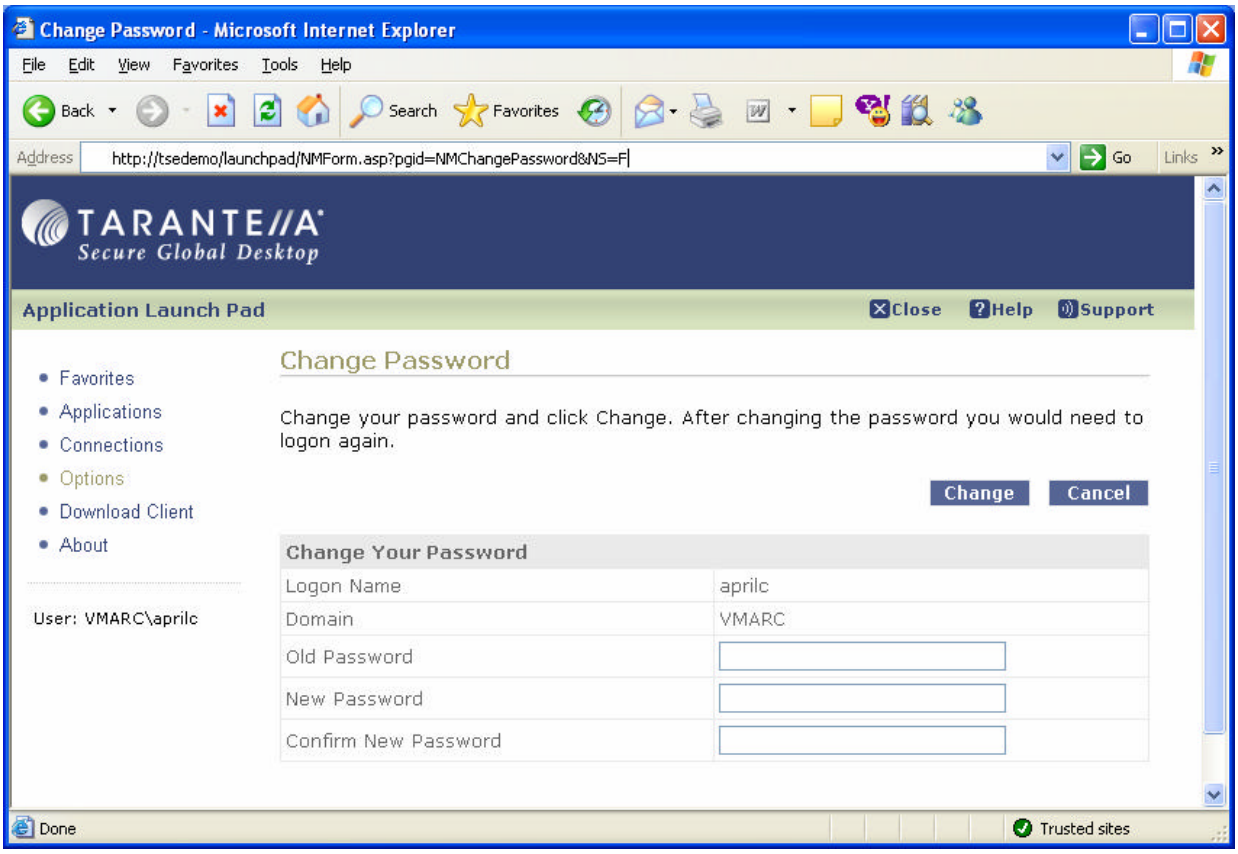
Select the servers and click **Remove**.

8 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. SGD-TSE Console administrators can disable this feature from **Console -> Options -> User** page.

When a user logs into the SGD-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.



9 Connection Setting Monitoring

9.1 *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.

10 Native Windows Client Connections

10.1 *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 SGD-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 SGD-TSE Printing support

10.2 *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 & 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.company.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 desktop 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 SGD, 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 SGD-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 SGD-TSE client software is installed or not on the machine that you use to reconnect to the application.

11 Native Macintosh Client Connections

11.1 *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 SGD-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 SGD-TSE Printing support

11.2 *Native Client on Apple Macintosh*

Launching SGD-TSE applications from a Macintosh client machine requires the Microsoft Remote Desktop Connection Client for Mac to be installed on the machine. More information can be obtained at this Microsoft Websites Mac section: http://www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient.

In addition to this client, a SGD-TSE plug-in from Tarantella has to be downloaded and installed in order to use Macintosh machines. This plug-in is currently only tested on Safari 1.1 (v100) and higher browser running on OS X version 10.3.

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 SGD-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 SGD-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.