Sun Secure Global Desktop 4.4 Release Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 820-2548
October 2007, Revision 01

Submit comments about this document at: `http://docs.sun.com/app/docs/form/comments`

Please
Recycle

Adobe PostScript

Contents

Preface

The *Sun Secure Global Desktop 4.4 Release Notes* provide information about the system requirements and support, and the new features and changes, for this version of Sun Secure Global Desktop (SGD). This document is written for system administrators.

Using System Commands

This document might not contain information on basic UNIX® system commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to your system documentation for this information. This document does, however, contain information about specific SGD commands.

Shell Prompts

Shell	Prompt
C shell	*machine-name*%
C shell superuser	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use ls -a to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% **su** Password:
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. To delete a file, type **rm** *filename*.

* **The settings on your browser might differ from these settings.**

Related Documentation

The documents listed as online are available at

http://docs.sun.com/app/docs/coll/170612.

Application	Title	Part Number	Format	Location
Installation	*Sun Secure Global Desktop 4.4 Installation Guide*	820-2549	HTML PDF	Online Software CD and online
Administration	*Sun Secure Global Desktop 4.4 Administration Guide*	820-2550	HTML	Online
Reference	*Sun Secure Global Desktop 4.4 Reference Manual*	820-2551	HTML PDF	Online Online
User	*Sun Secure Global Desktop 4.4 User Guide*	820-2552	HTML	Online

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at http://docs.sun.com/app/docs/form/comments.

Please include document title and part number (*Sun Secure Global Desktop 4.4 Release Notes*, part number 820-2548) in the subject line of your email message.

CHAPTER 1

System Requirements and Support

This chapter contains the system requirements for installing and using SGD version 4.40.

Topics in this chapter include the following:

Hardware Requirements

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact an SGD sales office `(http://www.sun.com/secure/contact/)`.

The requirements for a server hosting SGD can be calculated based on the *total* of the following:

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD and runs applications

The following are the requirements for installing and running SGD:

- 256 megabytes of free disk space, plus another 300 megabytes at install time
- 256 megabytes of random-access memory (RAM)
- 1 gigahertz processor
- Network interface card (NIC)

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 20 megabytes for each user
- On SPARC® technology platforms (SPARC platforms), 15 megahertz for each user
- On x86 platforms, 20 megahertz for each user

Caution – The actual central processing unit (CPU) and memory requirements can vary significantly, depending on the applications used.

Operating System Requirements

The following table describes the supported installation platforms for SGD.

Operating System	Supported Versions
Solaris™ Operating System (Solaris OS) on SPARC platforms	8, 9, 10, 10 Trusted Extensions
Solaris OS on x86 platforms	10, 10 Trusted Extensions
Red Hat Enterprise Linux (Intel x86 32-bit)	4, 5
Fedora Linux (Intel x86 32-bit)	7
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

Localized Messages During Installation on Linux Platforms

When you install SGD on Linux platforms, localized messages in the supported languages can only be displayed if the `gettext` package is installed. If the `gettext` package is not installed, English is used during the installation.

Fedora 7

SGD fails to install if the `libXp.so.6` library is not available on the server. This library was deprecated in Fedora Core 3. However, the file is still available in the `libXp` package.

5250 and 3270 Applications

The `libXm.so.3` library is required to support 5250 and 3270 applications. This library is available in the OpenMotif 2.2 package.

SUSE Linux Enterprise Server 9 With Service Pack 2

SGD fails to install if the `libgdbm.so.2` library is not available on the server. SUSE Linux Enterprise Server 9 with Service Pack 2 contains version 3 of the library by default. Obtain and install version 2 of the library before installing SGD.

SUSE Linux Enterprise Server 10

SGD fails to install if the `libgdbm.so.2` and `libexpat.so.0` libraries are not available on the server. SUSE Linux Enterprise Server 10 contains version 3 and version 1 of these libraries by default. Obtain and install the required version of these libraries before installing SGD.

Solaris 8, 9 and 10 OS

You must install at least the End User Solaris OS distribution to get the libraries required by SGD. If you do not, SGD does not install.

SGD fails to install if the `/usr/lib/libsendfile.so` library is not available on the server. This library might be included with the Core Solaris Libraries (`SUNWcsl`) package, or you might have to apply patch number 111297 to obtain it.

Solaris 8 OS `/dev/random` Pseudo Device

Users might not be able log in to SGD on Solaris 8 OS platforms if the server does not have the `/dev/random` pseudo device. You might have to install patch number 112438 to obtain this device.

Web Server Requirements

A web server is an essential part of a working SGD installation. When you install SGD, you install the SGD Web Server. The SGD Web Server is an Apache web server that is preconfigured for use with SGD. The SGD Web Server consists of the components listed in the following table.

Component	Version
`Apache HTTP Server`	1.3.36
`mod_ssl`	2.8.27
`OpenSSL`	0.9.8d
`mod_jk`	1.2.15
`Apache Jakarta Tomcat`	5.0.28
`Apache Axis`	1.2

You can use your own web server with SGD. How you do this is described in the *Sun Secure Global Desktop Software 4.4 Administration Guide*.

Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- SGD servers must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for an SGD server must always succeed.
- All client devices must use DNS.
- Client devices must be able to make Transmission Control Protocol/Internet Protocol (TCP/IP) connections to SGD on the following TCP ports:
  - **80** - For Hypertext Transfer Protocol (HTTP) connections between client devices and the SGD Web Server. The port number might vary depending on the port selected on installation.
  - **443** - For Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) connections between client devices and the SGD Web Server.
  - **3144** - For standard (unencrypted) connections between client devices and SGD.
  - **5307** - For secure connections between client devices and SGD. Secure connections use Secure Sockets Layer (SSL).

Note – The initial connection between a client device and SGD is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open for connections to SGD. You can configure SGD to always use secure connections.

- To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine the TCP ports that must be open, for example:
  - **22** - For X and character applications using Secure Shell (SSH)
  - **23** - For Windows, X and character applications using Telnet
  - **3389** - For Windows applications using Windows Terminal Services
  - **6010 and above** - For X applications

The *Sun Secure Global Desktop Software 4.4 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls.

Client Requirements

To use the webtop at `http://`*server.example.com*`/sgd`, where *server.example.com* is the name of an SGD server, you need the SGD Client and a supported web browser.

The SGD Client can operate in two modes:

- **Webtop mode**. The SGD Client uses a special web page, called a webtop, to display the controls for SGD. This is the default mode.
- **Integrated mode**. The SGD Client displays the controls for SGD in the desktop Start or Launch menu. Depending on other configuration factors, a web browser might only be needed for initial authentication, and for determining proxy server settings.

The following table lists the supported client platforms, the supported web browsers, and the supported desktop menu systems when the SGD Client is operating in Integrated mode.

Supported Client Platform	Supported Web Browsers	Integrated Mode Support
Microsoft Windows Vista	Internet Explorer 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Microsoft Windows XP Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Microsoft Windows 2000 Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Solaris 8+ OS on SPARC platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Sun Java Desktop System Launch Menu
Solaris 10 OS Trusted Extensions on SPARC platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Not supported
Solaris 10 OS on x86 platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Sun Java Desktop System Launch Menu
Mac OS X 10.4+	Safari 2.0+ Mozilla Firefox 2.0+	Not supported
Fedora Linux 7 (Intel x86 32-bit)	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu

Supported Client Platform	Supported Web Browsers	Integrated Mode Support
Red Hat Desktop version 4	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu
SUSE Linux Enterprise Desktop 10	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu
Ubuntu 7.04	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome Start Menu

Beta versions or preview releases of web browsers are not supported.

Web browsers must have the JavaScript™ programming language enabled.

To support the following functionality, web browsers must have Java technology enabled:

- Downloading and installing the SGD Client automatically
- Determining proxy server settings from the user's default web browser.

If Java technology is not available, the SGD Client can be downloaded and installed manually.

The following are the supported plug-ins for Java technology:

- Sun Java Plug-in tool version 1.6.0
- Sun Java Plug-in tool version 1.5.0

Note – Sun Java Plug-in tool version 1.6.0 is the *only* supported plug-in for Microsoft Windows Vista platforms.

When users start more than one user session using the same client device and web browser, the user sessions join rather than the new session ending the existing session. For user sessions to join in this way, the web browser must be configured to allow permanent cookies. If permanent cookies are not allowed, user sessions always end and this might cause application windows to disappear.

For best results, client devices must be configured for at least 256 colors.

Serial port mapping is only supported on UNIX, Linux, and Microsoft Windows platforms.

SGD Enhancement Module Requirements

The SGD Enhancement Module is a software component that can be installed on an application server to provide the following additional functionality to SGD:

- Advanced load balancing
- Client drive mapping (CDM)
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

The following are the supported installation platforms for the SGD Enhancement Module:

Operating System	Supported Versions
Microsoft Windows	Windows Server 2003 Windows 2000 Server Microsoft Windows XP Professional* Microsoft Windows Vista Ultimate* Microsoft Windows Vista Business*
Solaris OS on SPARC platforms	8, 9, 10, 10 Trusted Extensions†
Solaris OS on x86 platforms	10, 10 Trusted Extensions†
Red Hat Enterprise Linux (Intel x86 32-bit)	4, 5
Fedora Linux (Intel x86 32-bit)	7
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

* On Microsoft Windows XP Professional and Microsoft Windows Vista platforms, only CDM is supported. Seamless windows and advanced load balancing are not supported. Only full Windows desktop sessions are supported, not applications.

† On Solaris 10 OS Trusted Extensions platforms, audio and CDM are not supported.

Application servers that are not supported platforms for the SGD Enhancement Module can be used with SGD to access a supported application type using any of the supported protocols.

Supported Application Types

You can use SGD to access the following types of applications:

- Microsoft Windows
- Character applications running on Solaris OS, Linux, HP-UX and AIX
- X applications running on Solaris OS, Linux, HP-UX and AIX
- IBM mainframe and AS/400
- Web applications (using HTML and Java technology)

Supported Protocols

SGD supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) version 5.2
- X11
- HTTP
- HTTPS
- SSH version 2 or later
- Citrix Independent Computing Architecture (ICA)
- Telnet VT, American National Standards Institute (ANSI)
- TN3270E
- TN5250

Security Support

SGD supports secure connections from clients using the following protocols:

- SSL version 3.0
- Transport Layer Security (TLS) version 1.0

The following encryption cipher suites are supported:

- `RSA_WITH_AES_256_CBC_SHA`
- `RSA_WITH_AES_128_CBC_SHA`

- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_DES_CBC_SHA

SGD supports Base 64-encoded PEM-format X.509 certificates that are signed with any of the following Certificate Authority (CA) certificates (root certificates):

- Baltimore CyberTrust Code Signing Root
- Baltimore CyberTrust Root
- Entrust.net CA
- Entrust.net Client CA 1
- Entrust.net Client CA 2
- Entrust.net Server CA 1
- Entrust.net Server CA 2
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2
- Equifax Secure Global eBusiness CA
- GeoTrust Global CA
- The Go Daddy Group, Inc. Class 2 CA
- GTE CyberTrust Root
- GTE CyberTrust Global Root
- GTE CyberTrust Root 5
- Starfield Technologies, Inc. Class 2 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium CA
- Thawte Server CA
- http://www.valicert.com
- VeriSign Class 1 Public Primary CA - G1
- VeriSign Class 1 Public Primary CA - G2
- VeriSign Class 1 Public Primary CA - G3
- VeriSign Class 2 Public Primary CA - G1
- VeriSign Class 2 Public Primary CA - G2
- VeriSign Class 2 Public Primary CA - G3

- VeriSign Class 3 Public Primary CA - G1
- VeriSign Class 3 Public Primary CA - G2
- VeriSign Class 3 Public Primary CA - G3
- VeriSign Class 4 Public Primary CA - G2
- VeriSign Class 4 Public Primary CA - G3
- VeriSign/RSA Secure Server

Additional certificate types can be supported by installing the CA's certificate (the root certificate) for that CA.

Proxy Server Support

To use SGD with a proxy server, the proxy server must support tunneling.

For the webtop, you can use HTTP, Secure (SSL) or SOCKS v5 proxy servers.

For SOCKS v5 proxy servers, SGD supports the Basic and No Authentication Required authentication methods.

Supported Authentication Methods

The following are the supported mechanisms for authenticating users to SGD:

- Lightweight Directory Access Protocol (LDAP) version 3
- Microsoft Active Directory
- Network Information Service (NIS)
- Microsoft Windows Domains
- RSA SecurID
- Web server authentication (HTTP/HTTPS Basic Authentication), including Public Key Infrastructure (PKI) client certificates

SecurID Authentication

SGD works with versions 4, 5, and 6 of the RSA Authentication Manager (formerly known as RSA ACE/Server).

Supported LDAP Directory Servers

SGD supports version 3 of the standard LDAP protocol. You can use LDAP authentication and the LDAP search methods for third-party authentication with any LDAP version 3-compliant directory server. SGD supports this functionality on the following directory servers:

- Sun Java System Directory Server version 4.1+ (formerly known as Sun ONE, Netscape™ software, or iPlanet Directory Server)
- Microsoft Active Directory

Other directory servers might work, but are not supported.

Active Directory authentication is only supported on Microsoft Active Directory servers.

The Directory Services Integration (sometimes known as webtop generation) functionality is supported on the following directory servers:

- Sun Java System Directory Server version 4.1+ (formerly known as Sun ONE, Netscape software, or iPlanet Directory Server)
- Microsoft Active Directory

Other directory servers might work, but are not supported.

Printing Support

SGD supports printing to PostScript, Printer Command Language (PCL), and text-only printers attached to the user's client device.

The SGD `tta_print_converter` script performs any conversion needed to format print jobs correctly for the client printer. To convert from Postscript to PCL, Ghostscript must be installed on the SGD server.

To support SGD Portable Document Format (PDF) printing, Ghostscript version 6.52 or later must installed on the SGD server. The Ghostscript distribution must include the `ps2pdf` program. Microsoft Windows clients devices must have Adobe Reader version 4.0 or later.

SGD supports printing with the Common Unix Printing System (CUPS). CUPS version 1.1.19 or later must be installed on the SGD server. Additional configuration is required.

When printing from a Windows application that uses the Microsoft RDP protocol, SGD supports the printers supported by the Microsoft Windows application server.

Smart Card Support

SGD enables users to access a smart card reader attached to their client device from applications running on a Windows Server 2003 application server. Users can do the following:

- Log on to a Windows Server 2003 server using a smart card.
- Access the data on a smart card while using an application running on a Windows 2003 Server, for example, to use a certificate for signing or encrypting an email.

SGD works with any Personal Computer Smart Card (PCSC)-compliant smart card and reader.

Logging on to a Windows Server 2003 application server using a smart card has been tested successfully with smart cards listed in the following table.

Client Operating System and Libraries	Smart Card
Microsoft Windows XP Vista	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows XP Professional	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows 2000 Professional	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Solaris OS with Sun Ray™ thin client PCSC Bypass package (`SUNWsrcbp`)	ActivCard 64K CryptoFlex 32K
Fedora Linux with `pcsc-lite 1.2.0`	ActivCard 64K CryptoFlex 32K GemPlus GPK16000

CHAPTER 2

New Features and Changes

This chapter describes the new features and changes in versions 4.40, 4.31 and 4.30 of SGD.

Topics in this chapter include the following:

New Features in Version 4.40

This section describes the features that are new in the Sun Secure Global Desktop Software 4.40 release.

SGD Administration Console

The SGD administration tools, Object Manager, Array Manager, Configuration Wizard, and Session Manager have been replaced by the SGD Administration Console. The SGD Administration Console is a web application. The Administration Console can be used by SGD Administrators to configure SGD.

The Administration Console is localized into the languages supported by SGD: English, French, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

To use the Administration Console, your browser must have JavaScript enabled.

Wherever possible, run the Administration Console on the primary server in the SGD array. Some operations, for example, creating new objects or editing object attributes, are best done on the primary server. If you perform these operations on a secondary server and the primary server is not running, your changes are not implemented.

Note – The SGD distribution includes a web archive (WAR) file for the Administration Console, `sgdadmin.war`. Using this file to deploy the Administration Console on another web application server is not supported.

You can start the Administration Console in one of the following ways:

- Click the Administration Console link on the webtop of an SGD Administrator.
- Click the Launch the Sun Secure Global Desktop Administration Console link on the SGD Web Server Welcome Page at `http://`*server.example.com*, where *server.example.com* is the name of an SGD server.
- Go to `http://`*server.example.com*`/sgdadmin`, where *server.example.com* is the name of an SGD server.

See the *Sun Secure Global Desktop 4.4 Administration Guide* and the *Sun Secure Global Desktop 4.4 Reference Manual* for more details about the Administration Console.

Terminology Changes

The Administration Console uses different terminology compared to previous SGD releases.

The following table lists some common terms used in version 4.31 and the corresponding term used in the Administration Console.

SGD Version 4.31	Administration Console
array member	SGD server
browser-based webtop	webtop
emulator session	application session
Enterprise Naming Scheme (ENS)	local repository
ENS equivalent name	user profile
Fully Qualified Name	user identity
host	application server
intelligent array routing	load balancing group
login authority	system authentication

SGD Version 4.31	Administration Console
login profile	user profile
person object	user profile object
Tarantella Federated Naming (TFN)	*Not used*
webtop session	user session

Attribute Name Changes

Some attributes have been renamed for the Administration Console. The *Sun Secure Global Desktop 4.4 Reference Manual* includes the attribute names used in the Administration Console, along with the previous attribute name used in Object Manager and Array Manager.

The Desktop Direct URL

The Desktop Direct Uniform Resource Locator (URL) enables users to log in and display a full-screen desktop without displaying a webtop.

To be able to use the Desktop Direct URL, the user must be assigned an application object called My Desktop (`cn=My Desktop`). This object is created automatically when SGD is installed. By default, the object is configured to run the default desktop application available on the SGD server, for example, the Sun Java Desktop System. You can reconfigure this object to run any application you want, but it works best with full-screen desktop applications. If users require different desktop applications, you can create additional My Desktop objects as required. However, users must be assigned only one My Desktop application.

Note – Users can be assigned any number of applications, but the Desktop Direct URL only gives users access to the My Desktop application.

The Desktop Direct URL is `http://`*`server.example.com`*`/sgd/mydesktop`, where *server.example.com* is the name of an SGD server. This URL displays the SGD Login page. Once the user has logged in, the desktop session displays and the web browser can be closed.

Note – There are no controls for suspending or resuming the desktop application. Users must log out of the desktop application as normal.

Support for Roaming Profiles

Users with Microsoft Windows client devices can have roaming user profiles. Roaming user profiles provide the user with the same working environment, no matter which Microsoft Windows computer they use. If Microsoft Windows users have roaming user profiles, the SGD client profile is automatically adjusted to allow for this, as follows:

- Settings specific to the user's client device, for example the proxy server configuration, are stored on the client device.

  By default, this is *homedrive*`\Documents and Settings\`*username*`\Local Settings\Application Data\Sun\SSGD\profile.xml`

  Settings specific to the user, for example the preferred language, are stored in the location of the roaming user profile.

- Usually, this is *homedrive*`\Documents and Settings\`*username*`\Application Data\Sun\SSGD\profile.xml`

Note – This location also contains the user's `hostsvisited` and `certstore.pem` files.

The following settings from the SGD client profile are stored in the location of the user's roaming profile:

Client Profile Setting	Roaming Profile Entry
Login URL	`<url>`
Add Applications to Start Menu	`<mode>`
Automatic Client Login	`<autologin>` `<AT>`
Connect on System Login	`<autostart>`

Connection Failure	`<reconnect mode>`
	`<reconnect_attempts>`
	`<reconnect_interval>`

Automatic Timeout of Idle User Sessions

SGD Administrators can now configure an automatic timeout for idle user sessions.

The timeout enables user sessions to be suspended if there has been no application session or webtop activity for a specified time period. The timeout applies to all SGD servers in the array.

This timeout is only configurable from the command line. You cannot edit the timeout value using the Administration Console.

You configure the timeout with the following command:

```
$ tarantella config edit \
--tarantella-config-array-webtopsessionidletimeout secs
```

Replace *secs* with the timeout value, measured in seconds.

A setting of 0 turns off the user session idle timeout feature. This is the default setting.

In the following example, user sessions are suspended after 1800 seconds (30 minutes) of inactivity.

```
$ tarantella config edit \
--tarantella-config-array-webtopsessionidletimeout 1800
```

Netmask Filters for Specifying Network Addresses

You can now specify a netmask filter when setting the following attributes:

- External DNS names (`--server-dns-external`)
- Array routes (`--tarantella-config-array-netservice-proxy-routes`)

The netmask filter takes the format `v.w.x.y/z`. The previous "wildcard" type filters are still supported.

The following example uses a netmask filter to specify external DNS names.

```
$ tarantella config edit --server-dns-external \
  "192.168.55.0/24:boston.indigo-insurance.com"
```

Window Management Keys

A new Window Management Keys (`--remotewindowkeys`) attribute is available for the following object types:

- Windows application
- X application

Using this attribute, keyboard shortcuts that deal with window management can either be sent to the remote session or acted on locally. This setting is only effective for applications having a Window Type setting of Kiosk mode.

To exit kiosk mode when this attribute is enabled, use the key sequence Alt+Ctrl+Shift+Space. This minimizes the kiosk session on the local desktop.

Support for Solaris 10 OS Trusted Extensions

SGD runs on Solaris 10 OS Trusted Extensions with the following known limitations:

- SGD must be installed to a labelled zone. See the *Sun Secure Global Desktop 4.4 Installation Guide* for more information about installing SGD on Solaris 10 OS Trusted Extensions.
- Client drive mapping is not supported for UNIX platform client devices [6610354].
- Audio is not supported for UNIX platform applications [6610352].
- Integrated mode is not supported for Solaris 10 OS Trusted Extensions client platforms [6610371].
- Kiosk mode display for applications does not provide the best user experience for Solaris 10 OS Trusted Extensions client platforms [6594795].

Global Management of Passwords and Tokens

The Administration Console can be used to globally manage passwords and tokens for all users of SGD.

You can now manage passwords and tokens by user identity or by user profile. Previously, the Object Manager administration tool only supported management of passwords and tokens by user profile.

Subject Alternative Names for Server Certificates

If an SGD server has multiple DNS names, for example, it is known by different names inside and outside a firewall, you can specify the additional DNS names as *subject alternative names* when generating a Certificate Signing Request (CSR). This enables you to associate more than one DNS name with a server certificate.

The `tarantella security certrequest` command now prompts you to enter subject alternative names when generating a CSR.

The subject alternative names for a certificate can be displayed using the `tarantella security certinfo` command.

Time Zone Map File Attribute

A new Time Zone Map File attribute (`--xpe-tzmapfile`) is available.

The attribute enables you to specify a file that contains mappings between UNIX client device and Windows application server time zone names. The attribute applies to all SGD servers in the array.

New Features in Version 4.31

This section describes the features that are new in the Sun Secure Global Desktop Software 4.31 release.

Audio Support in X Applications

SGD Administrators can now enable sound in X applications accessed using SGD.

To hear sound in X applications, the following conditions must be met:

- The client device must be capable of playing sound.
- The SGD Client must be used to connect to SGD.
- The UNIX audio module of the SGD Enhancement Module must be installed and running on the application server.
- The X application must output sound using the Open Sound System (OSS). If your system uses the Advanced Linux Sound Architecture (ALSA), you might have to enable the ALSA OSS emulation modules in the kernel.
- The SGD UNIX audio service must be enabled in the Administration Console. The service is disabled by default.

The UNIX audio module contains an OSS audio driver emulator. The audio driver emulator is installed in the kernel when you install the UNIX audio module of the SGD Enhancement Module.

Note – As the UNIX audio module includes an audio driver emulator, the application server itself does not actually need to have a sound card.

Some X applications are hard-coded to use the `/dev/audio` or `/dev/dsp` devices for audio output. A new attribute for X application objects, Audio Redirection Library (`--unixaudiopreload`), enables an SGD audio redirection library to force the X application to use the SGD audio device.

Support for the Remote Desktop on Microsoft Windows Vista

Microsoft Windows Vista includes the Remote Desktop feature that enables you to access a computer using the Remote Desktop Protocol. You can now use SGD and Remote Desktop, for example, to give users to access their office PC when they are out of the office. Only full Windows desktop sessions are supported.

You can also install the SGD Enhancement Module on Microsoft Windows Vista client devices to provide support for client drive mapping. Advanced load balancing and seamless windows are not supported.

SSH Client Settings

A new SSH Arguments (`--ssharguments`) attribute is available for the following object types:

- X application
- Character application
- 3270 application
- 5250 application

With this attribute, you can specify the command-line arguments for the SSH client when the connection method for an application is SSH.

New Features in Version 4.30

This section describes the features that are new in the Sun Secure Global Desktop Software 4.30 release.

Integration with the Desktop Start or Launch menu

The SGD Client can now operate in either of the following modes:

- **Webtop mode** - Uses a web browser to display the webtop in the same way as previous releases. This is the default mode.
- **Integrated mode** - The webtop content (the links for starting applications) displays in the desktop Start or Launch menu so that users can run remote applications in the same way as local applications. Depending on how you configure Start or Launch menu integration, you might not need to use a web browser.

Note – Use Integrated mode if your organization prefers not to use Java technology on the client device.

To use Integrated mode, you must log in to SGD using the Login link on the desktop Start or Launch menu. Integrated mode is not available if you start a web browser and log in.

Working in Integrated mode simplifies session management. Unlike the webtop, it has no controls for suspending and resuming applications. Instead, when you log out, the Client automatically suspends or ends all running application sessions. When you log in again, the Client automatically resumes all suspended sessions.

Printing is also simplified. Printing is always “on” and print jobs go straight to the selected printer. Unlike the webtop, print jobs cannot be managed individually.

If you need to display a webtop, for example to resume a suspended application or manage printing, you click the Webtop link on the Start or Launch menu. The webtop displays in your default web browser.

If you configure the webtop content to display in groups, those groups are also used in the Start or Launch menu. If the group is configured to hide webtop content, the content does not display in the Start or Launch menu.

To log out of SGD, you click the Logout link on the Start or Launch menu.

For details of the desktop systems that can be used with Integrated mode, see “Client Requirements” on page 6.

Single Sign-On

You can now configure the SGD Client to start automatically when a user logs in to their client device. The SGD Client can also cache an authentication token that enables a user to start a user session automatically without having to log in manually. When the SGD Client is configured in this way, users experience the benefits of a single sign-on.

Automatic login is achieved using authentication token authentication. If the SGD Client presents a valid authentication token, the user is authenticated automatically to SGD. To obtain an authentication token, users must perform an initial log in using a web browser and then manually generate the authentication token by editing their client profile. A separate token is needed for each SGD server the user connects to.

Managing Client Configuration With Profiles

The desktop Start or Launch menu and single sign-on features mean that the SGD Client requires some configuration to connect to SGD. Not only that, different configurations might be needed in different situations, for example because the user is in the office or working at home. To be able to manage multiple Client configurations, version 4.3 introduces client profiles as the method for storing a group of SGD Client settings. Each client profile enables you to configure the following:

- The URL to connect to SGD
- The operating mode of the SGD Client, whether Webtop mode or Integrated mode
- Whether automatic logins are enabled
- Whether the SGD Client starts automatically when the user logs in to their client device
- Proxy server configuration, whether the settings are configured manually in the profile or determined automatically from the web browser
- Reconnection settings for controlling what happens when the SGD Client loses its connection to SGD
- Logging settings for controlling what information is written to the SGD Client log file
- The path to the PDF viewer used for PDF printing on Solaris OS, Linux, and Mac OS X clients

SGD Administrators have full control over client profiles. On an Administrator's webtop there is a new administration tool, Profile Editor. With the Profile Editor, Administrators can create and edit client profiles for organization, organizational

unit (OU) objects, and for profile objects in the Tarantella System Objects organization. By defining client profiles for these objects, Administrators can deploy common default SGD Client configurations to users.

Administrators can control whether users can create and edit their own client profiles. User profile editing can be enabled globally, for an organization, for an OU, or for individual users. By default, user profile editing is enabled. Users create and edit profiles from the Edit button on their webtop.

SGD has a system-wide default profile that is configured to give users the standard webtop behavior available in previous releases. Administrators can edit this profile.

When the SGD Client connects to SGD, the profile configured for the user is copied from SGD to the client device. If a user edits their profile, the changes are stored *only* on the client device.

Mobile Proxy Server Configuration

When connecting to SGD from different locations, the SGD Client often needs different client proxy server settings. Ensuring that users have the correct proxy settings can also be difficult to administer. Version 4.3 introduces mobile proxy server configuration. With mobile proxy server configuration, the SGD Client uses the settings in the client profile to determine the proxy server settings. The proxy server settings can be specified as follows:

- **Manually.** The proxy settings are stored in the client profile itself.
- **Automatically.** The proxy settings are obtained from the user's default web browser.

If the SGD Client is running in Integrated mode and configured to use the web browser settings, the SGD Client obtains the proxy settings by loading the URL specified in the profile in the user's default web browser. As the SGD Client caches the settings it obtains, the SGD Client can be configured to use the settings in the cache so that the user's default web browser only has to be started once.

Note – To determine the proxy settings from a web browser, the web browser must have Java technology enabled.

Enhanced Command Line for the SGD Client

The command line for the SGD Client on all platforms has been enhanced to support client profiles. You can use arguments to specify the following:

- The profile to use.

- The URL to connect to SGD. This overrides the URL in the profile.
- The preferred language to use.

With the enhancements to the command line, you can create your own scripts for starting the SGD Client and for running single applications.

Manually Installable SGD Client

To support running the SGD Client in Integrated mode, or in environments that have web browsers without Java technology enabled, you can download and install the SGD Client manually. You download the SGD Client from an SGD server at `http://`*server.example.com*, where *server.example.com* is the name of an SGD server. Click Install the Sun SGD Client to install the SGD Client.

New X Server

This release includes a new X server, based on X11R6.8.2. The new X server delivers significant speed and bandwidth improvements when compared to version 4.2.

The updated server supports the following X extensions:

- `BIG-REQUESTS`
- `BLINK`
- `DAMAGE`
- `DEC-XTRAP`
- `DOUBLE-BUFFER`
- `Extended-Visual-Information`
- `GLX`
- `MIT-SCREEN-SAVER`
- `MIT-SHM`
- `MIT-SUNDRY-NONSTANDARD`
- `NATIVE-WND`
- `RDP`
- `RECORD`
- `RENDER`
- `SCO-MISC`
- `SECURITY`
- `SGI-GLX`

- SHAPE
- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES
- XFree86-Bigfont
- XTEST
- XTTDEV

The new X server also includes support for some additional X fonts. The Speedo font is no longer available.

New X Security Extension Attribute

X application objects have a new X Security Extension attribute (`--securityextension`) that enables the X Security Extension for an application. If you need to run an X application from an application server that might not be secure, enable the X Security Extension and run the application in untrusted mode. This restricts the operations that the X application can perform in the X server and protects the display. X security only works with versions of SSH that support the `-Y` option. For OpenSSH, this is version 3.8 or later.

PDF Printing for UNIX Platform, Linux, and Mac OS X Clients

The SGD Client on UNIX platform, Linux, and Mac OS X client devices now supports PDF printing. On these clients, printing to an SGD PDF printer causes the document to be displayed in a PDF viewer where the file can be saved or printed. By default SGD supports the following PDF viewers.

Client Platform	Default PDF Viewer
Solaris OS on SPARC technology platforms	Adobe Reader (`acroread`)
Solaris OS on x86 platforms	GNOME PDF Viewer (`gpdf`)
Linux	GNOME PDF Viewer (`gpdf`)
Mac OS X	Preview.app

To be able to use a default viewer, the application must be on the user's PATH.

If an alternative PDF viewer is preferred, the *full path* to the alternative viewer can be specified in the client profile used by the SGD Client.

Note – When selecting a PDF printer on UNIX platform, Linux, and Mac OS X client devices, there is no difference between the "Universal PDF Printer" and "Universal PDF Viewer" printers as the document is always displayed in a PDF viewer.

PDF printing on Microsoft Windows client devices is unchanged.

Client Drive Mapping for UNIX Platform and Linux Applications

Client drive mapping (CDM) is now available for UNIX platform and Linux applications.

When you enable client drive mapping in the Administration Console, this enables client drive mapping for UNIX platform, Linux, and Windows applications.

The attributes for managing access rights to client drives available for organization, organizational unit and user profile objects apply only to Windows client devices regardless of whether they are connected to Windows, UNIX platform, or Linux applications.

The drives that are mapped for UNIX platform, Linux, and Mac OS X client devices are controlled by entries in the user's configuration file, `$HOME/.tarantella/native-cdm-config`.

For client drive mapping to be available for UNIX platform and Linux applications, the following conditions must be met:

- The SGD Enhancement Module must be installed and running on the UNIX platform or Linux application server. Currently you have to manually start the client drive mapping service with the `/opt/tta_tem/bin/tem startcdm` command.
- The application server must have an Network File System (NFS) server installed and running. The NFS server must export a directory to be used for client drive mapping. By default, this is `/smb`. It is possible to specify a different directory in the `/opt/tta_tem/etc/client.prf` file. The entry in this file has the format `NFS_server/mount/mountpoint`.
- Client drive mapping must be enabled in the array.
- The SGD client drive mapping service must be started in the array using the `tarantella start cdm` command.

- The access rights to client drives must be configured using the Administration Console (for Windows clients) and in the user's configuration file (UNIX platform, Linux, and Mac OS X clients).

When client drive mapping is enabled, the user's client drives or file systems are available by default in the `My SGD drives` directory in the user's home directory. The `My SGD drives` directory is a symbolic link to the NFS share that is used for client drive mapping.

Support for Serial Ports in Windows Applications

Users running Windows applications on a Windows Terminal Server can now access the serial ports on their client device.

To be able to access a serial port, the following conditions must be met:

- COM port mapping must be enabled in the Terminal Services Configuration (it is by default).
- Serial port mapping must be enabled in the Global Settings ⇒ Client Device tab of the Administration Console (it is by default).
- Access to serial ports must enabled for either an organization, an organizational unit or a user profile object. Access permissions can be inherited.
- SGD clients must be able to enumerate the serial ports on client devices. The *Sun Secure Global Desktop 4.4 Administration Guide* has details of how to map serial ports.

Users must have read-write access to the serial ports that they want to access.

Serial port mapping is available to the SGD Client running on Windows, Solaris platform, and Linux client devices.

Support for the Remote Desktop on Microsoft Windows XP Professional

Microsoft Windows XP Professional includes the Remote Desktop feature that enables you to access a computer using the Remote Desktop Protocol. You can now use SGD and Remote Desktop, for example, to give users to access their office PC when they are out of the office. Only full Windows desktop sessions are supported.

You can also install the SGD Enhancement Module on Microsoft Windows XP Professional client devices to provide support for client drive mapping. Advanced load balancing and seamless windows are not supported.

Support for Connections to the Console Session With Windows Server 2003 Terminal Services

The SGD Terminal Services Client (`ttatsc`) now supports an additional `-console` option that enables you to connect to the console session with Windows Server 2003 Terminal Services.

You can specify this option with the Arguments for Protocol (`--protoargs`) attribute of the Windows application object.

Initial Connection Security

The initial connection between an SGD Client and an SGD server is now secured with SSL. However, after the user logs in, the connection is downgraded to a standard connection. To be able to use SSL permanently for connections to SGD, you must enable SGD security services.

TCP Port 5307 is used for SSL-based connections between SGD Clients and SGD. You might have to open this port in your firewall to allow SGD Clients to connect.

SGD has an array routes feature that enables you to configure server-side SOCKS proxy servers. You configure array routes with the following command:

```
$ tarantella config edit \
--tarantella-config-array-netservice-proxy-routes route...
```

If a route includes the `:ssl` option, you must configure the SGD SSL Daemon to accept unencrypted connections using the SSL Accelerator Support attribute on the Secure Global Desktop Server Settings ⇒ Security tab of the Administration Console, or with the following command:

```
$ tarantella config edit --security-acceptplaintext 1
```

Protecting Clients Against Unauthorized Servers

As the SGD Client can now start and log in automatically, it is vital that users only connect to an SGD server that is trusted. In this release, users must explicitly authorize the connection to SGD.

When a user connects to SGD for the first time, they see an Untrusted Initial Connection warning message that asks them whether they really want to connect to the SGD server. The message displays the host name and fingerprint of the security

certificate for the server they are connecting to. Users should check these details *before* clicking Yes. Once a user agrees to the connection, they are not prompted again unless there is a problem.

To ensure that users only connect to SGD servers that are trusted, SGD Administrators must do the following:

- Provide users with a list of host names and fingerprints for the servers that are trusted. Use the `tarantella security fingerprint` command on each member of the array to obtain a list of fingerprints.
- Explain to users the security implications of agreeing to connect to server.

In a fresh installation, each SGD server has its own self-signed security certificate. Administrators must obtain and install a valid X.509 certificate for each SGD server.

Controlled Copy And Paste

SGD Administrators now have control over copy and paste operations in Windows and X application sessions. Administrators can configure copy and paste as follows:

- Copy and paste for SGD as a whole can be enabled or disabled.
- Copy and paste can be enabled or disabled for organization, organizational unit, or user profile objects. This gives Administrators control over who is allowed to copy and paste.
- Applications can be assigned a Clipboard Security Level. Data can only be copied if the target application (the application *receiving* the data) has the same Clipboard Security Level or higher as the source application. This enables Administrators to secure the data available through particular applications.
- The SGD Client can be assigned a Clipboard Security Level. Data can only be copied to applications running on the client device if the SGD Client has the same Clipboard Security Level or higher as the source application. This enables Administrators to secure the flow of data outside of SGD.

If a user attempts a copy and paste operation that is not permitted, for example because of differing security levels, they paste the following message instead of the copied data:

```
Sun SGD Software: Copied data not available to this application
```

Support for SecurID for Application Server Authentication

As well as using RSA SecurID to authenticate users to SGD, you can use SecurID for application server authentication when launching X and character applications.

To use SecurID authentication, first ensure that users can log in to the application server using SecurID before introducing SGD. When you are ready to use SecurID authentication, configure the application to use the `securid.exp` login script.

Localized User Interface

Version 4.3 contains localized user interfaces for the following languages:

- French
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

By visiting a different URL, or selecting a language on the SGD Web Server Welcome Page (`http://`*server.example.com*, where *server.example.com* is the name of an SGD server), users can run a webtop in their preferred language. The SGD Client can also be started in a preferred language.

The Administration Console tool is localized into the same languages as the user interface.

Translated Documentation

The following table lists the translations of SGD Documentation that are available.

Language	Release Notes	Installation Guide	Administration Guide	Reference Manual	User Guide
French	Yes	Yes	No	No	Yes
Japanese	Yes	Yes	Yes	Yes	Yes
Korean	Yes	Yes	No	No	Yes
Simplified Chinese	Yes	Yes	No	No	Yes
Traditional Chinese	Yes	Yes	No	No	Yes

Language Support in Expect Scripts

The Expect scripts used to start applications on application servers are enhanced to support system prompts in different languages. By default, the languages supported by SGD are supported.

To enable the Expect scripts to work with system prompts in different languages, a new Prompt Locale (`--hostlocale`) attribute on application server objects enables you to specify the locale of the application server.

Changes in Version 4.40

This section describes the changes since the Sun Secure Global Desktop Software 4.31 release.

Changes to Supported Installation Platforms

For this release, the following changes to the supported installation platforms for SGD are applicable:

- Solaris 10 OS Trusted Extensions on SPARC and x86 platforms is now supported. See "Support for Solaris 10 OS Trusted Extensions" on page 20 for more details.
- Fedora Linux 7 (Intel x86 32-bit) is now supported. Fedora Core 6 is no longer a supported platform.

See Chapter 1 for more information about supported platforms for this release.

Retirement of Classic Clients

SGD version 4.31 was the last release to contain the Java technology clients, the SGD Native Clients and the classic webtop. The 4.40 release does not contain these clients.

As a result of this change, for this release of SGD, you cannot configure applications to display in a web browser window. The `webtop` and `newbrowser` options for the Window Type attribute (`--displayusing`) have been removed.

Login and Authentication Sequence

As a security measure to prevent denial-of-service attacks, the sequence of events when you log in to SGD has changed, as follows:

- In SGD version 4.31, the SGD Client was started *before* the login screen was shown.
- For SGD version 4.40, the SGD Client is not started until *after* the user successfully authenticates at the login screen.

Start up of the SGD Client is indicated by an icon in the desktop task bar. See the *Sun Secure Global Desktop 4.4 Installation Guide* for more details about logging in to SGD.

You can no longer deny a connection to SGD based on the client's IP address.

Server Certificates and Multiple External DNS Names

In previous releases, the `--tarantella-config-ssldaemon-certificates` attribute was used to associate an X.509 certificate with an external DNS name for an SGD server.

This attribute is no longer supported. In this release, you can specify external DNS names as subject alternative names when you generate a CSR.

See "Subject Alternative Names for Server Certificates" on page 20 for more details.

Web Services Changes

The following web services changes have been implemented for this release:

- Authentication model changes
- Renaming of methods
- New web service operations
- Document/Literal SOAP message encoding
- Querying device data

Authentication Model Changes

In the 4.31 release, the `startSession` and the `authenticateSession` methods were used to authenticate a user session.

For the 4.40 release, creating and authenticating a user session have been combined into a single method, `authenticate`.

The `startSession` and `authenticateSession` methods are not available for the 4.40 release.

Renaming of Methods

Some overloaded methods were present in the 4.31 release. These methods were distinguished by the number and type of their parameters. All such overloaded methods have been renamed for the 4.40 release. Additionally, the mandatory parameters for the `setSessionIdentity` method have changed for the 4.40 release.

The following table lists the method name changes for this release.

Interface Name	Method Name in Version 4.31	Method Name in Version 4.40
`ITarantellaDatastore`	`modify(String, String, String[])`	`modifyReplace (String, String, String[])`
`ITarantellaEvent`	`adminSendClientSideMessage (String, String, String, String, String)`	`adminBroadcastClientSideMessage (String, String, String, String, String)`
`ITarantellaExternalAuth`	`setSessionIdentity (String, String)`	`setSessionIdentity (String, String, String)`
`ITarantellaPrint`	`printJobs(String)`	`printAllJobs(String)`
`ITarantellaWebtopSession`	`authenticateSession(String, String, String)`	`authenticate(String, String, String, String)`
`ITarantellaWebtopSession`	`authenticateSession(String, String, String, Item[], Item[])`	`authenticateExt(String, String, String, String, Item[], Item[])`
`ITarantellaWebtopSession`	`setTCCConfiguration (String, String, String, String, String, Item[])`	`setTCCConfigurationOverrides (String, String, String, String, String, Item[])`
`ITarantellaWebtopSession`	`startSession(*)`	No equivalent

New Web Service Operations

The following table lists the new web service operations.

Interface Name	Method Name	Description
ITarantellaDatastore	deleteObjects	Delete several objects from the SGD datastore.
	searchStart	Clean up server side resources for a given search.
	searchNext	Retrieve the next subset of search results.
	searchEnd	Start a datastore search returning a subset of results.
ITarantellaEmulatorSession	adminCount	Count the number of matching application sessions a search would return.
	adminSearchEnd	Clean up server side resources for a given search.
	adminSearchNext	Retrieve the next subset of search results.
	adminSearchStart	Start a search returning a subset of results.
	endSessions	End multiple application sessions.
ITarantellaPrint	adminCount	Count the number of matching print jobs a search would return.
	adminSearchEnd	Clean up server side resources for a given search.
	adminSearchNext	Retrieve the next subset of search results.
	adminSearchStart	Start a search, returning a subset of results.
ITarantellaWebtopSession	associateTCC	Associate a user session with an existing TCC connection.
	authenticate	Authenticate a user session.
	authenticateExt	Authenticate a user session.
	createView	Create a new view of an existing user session.
	adminEndSessions	End multiple user sessions.
	adminCount	Count the number of matching user sessions a search would return.
	adminSearchEnd	Clean up server side resources for a given search.
	adminSearchNext	Retrieve the next subset of search results.
	adminSearchStart	Start a search, returning a subset of results.
ITarantellaUtility	SearchEnd	Clean up server side resources for a given search.
	SearchNext	Retrieve the next subset of search results.
	SearchStart	Start a search, returning a subset of results.

Document/Literal SOAP Message Encoding

The SOAP message encoding format used for SGD web services has changed from RPC/Encoded to Document/Literal.

To list the SGD web services, go to http://*server.example.com*/axis/services, where *server.example.com* is the name of an SGD server. Click on the wsdl link to see the Web Services Description Language (WSDL) listing for an SGD web service.

The WSDL listings for the RPC/Encoded versions of the web services are still included on this page. Do not use the RPC/Encoded versions for developing your own applications. These versions of the web services will be deprecated in future releases.

Querying Device Data

The `adminLookupSession` operation now returns device information. You can use this operation to query the `--scottarawdevicedata` and `--scottadeviceaccessibledata` device data attributes.

The returned device information can be used as a diagnostic tool.

Flushing the Kerberos Cache

A new setting for the `tarantella cache` command enables you to refresh the current Kerberos configuration settings for an SGD server.

The new option, krb5config, is used as follows:

```
$ tarantella cache --flush krb5config
```

This setting enables you to update the Kerberos configuration for an SGD server without having to restart the server. This feature is used for Active Directory authentication only.

`tem status` Command

For users of the SGD Enhancement Module, a new command is available.

The `tem status` command provides status information for load balancing, UNIX platform audio, and client drive mapping services for the SGD array. The command lists the installed modules and indicates whether they are running or not.

SGD Client Does Not Assume Java Technology by Default

The SGD Client can be started from the command line using the `tcc` command on Microsoft Windows client platforms, or the `ttatcc` command on UNIX, Linux, or Mac OS X client platforms.

In this release, by default, when you start the SGD Client from the command line or in Integrated mode, the SGD Client assumes that the client device does not have Java technology enabled. A new `-use-java` argument for the `tcc` and `ttatcc` commands configures the SGD Client to use Java technology.

In previous releases, by default, the SGD Client assumed Java technology was enabled. A `-no-java` argument for the `tcc` and `ttatcc` commands was available to override this behavior. This argument has now been deprecated.

The available arguments for the `tcc` and `ttatcc` commands are described in the *Sun Secure Global Desktop 4.4 Administration Guide*.

SGD Client Logs Client Device Information

The SGD Client now logs information on client devices. Device access data and error messages are logged for printing, serial port, client drive mapping, audio and smart card devices.

The client device information is written to the SGD Client log file and is displayed on the Detailed Diagnostics page of the webtop.

Renamed Command Line Arguments

Several attributes have been renamed to give shorter attribute names. This prevents errors when typing these attributes on the command line.

The following table lists the attribute names that have been renamed.

Attribute Name in Version 4.31	Attribute Name in Version 4.40
`--tarantella-config-login-thirdparty-searchens`	`--login-thirdparty-ens`
`--tarantella-config-login-thirdparty-allownonens`	`--login-thirdparty-nonens`

Attribute Name in Version 4.31	Attribute Name in Version 4.40
`--tarantella-config-ldap-thirdpartyldapcandidate-useens`	`--login-ldap-thirdparty-ens`
`--tarantella-config-ldap-thirdpartyldapcandidate-useprofile`	`--login-ldap-thirdparty-profile`
`--tarantella-config-xpeconfig-timezonemapfile`	`--xpe-tzmapfile`

Windows NT Domain Attribute

The Windows NT Domain attribute has been renamed to Domain Name. This attribute specifies the domain to use for the application server authentication process.

The following objects have this attribute:

- Application server
- Windows application
- User profile

PDF Printers Renamed

The names of the SGD PDF printers have changed as shown in the following table.

Printer Name in Release 4.31	Printer Name in Release 4.4
Universal PDF	Universal PDF Printer
Print to Local PDF File	Universal PDF Viewer

Window Closure Warning

For application objects configured with a Window Type setting of Independent Window, a warning dialog is now shown when the application window is closed. The dialog prompts you to confirm that you want to end the application session.

SOCKS Proxy Removed From Client Profile

You can no longer configure SOCKS proxy servers using the SGD Client profile.

You can still configure SOCKS proxy servers using the array routing feature. Use the following command:

```
$ tarantella config edit \
--tarantella-config-array-netservice-proxy-routes \
"192.168.10.*:CTSOCKS:taurus.indigo-insurance.com:8080"
```

With this configuration, clients with IP addresses beginning `192.168.10` connect using the SOCKS proxy server `taurus.indigo-insurance.com` on TCP port 8080.

Administration Tools Removed From The Administrator Webtop

The Object Manager, Array Manager, Session Manager, and Configuration Wizard administration tools are no longer displayed on the Administrator's webtop. These administration tools have been replaced by a browser-based administration tool called the Administration Console. See "SGD Administration Console" on page 15 for more details.

The Configuration Wizard is still included in the SGD distribution, as an example web application. To display the Configuration Wizard, go to http://*server.example.com*`/sgd/admin/configmgr/index.jsp`, where *server.example.com* is the name of an SGD server.

Session Manager is still included in the SGD distribution, as an example web application. To display Session Manager, go to http://*server.example.com*`/sgd/admin/sessmgr/index.jsp`, where *server.example.com* is the name of an SGD server.

Login Script Changes

The login scripts in the */install-dir*`/var/serverresources/expect` directory have been rationalized. Some scripts have been renamed and others have been merged.

If you are using SecurID for application server authentication, objects now use the `securid.exp` script, rather than the `securid/unix.exp` script. For backward compatibility, a symbolic link now exists from `securid/unix.exp` to the new `securid.exp` script.

Enabling Input Methods for Locales

An input method (IM) is a program or operating system component that enables users to enter characters and symbols not found on their keyboard. On Microsoft Windows platforms, an IM is called an input method editor (IME).

When running applications, SGD enables an IM if either the TTA_PreferredLocale, TTA_HostLocale, or the LANG (from the application environment overrides) environment variables are set to a locale that requires an IM. The locales that require an IM are controlled by the IM_localeList variable, which is defined in the `vars.exp` login script.

By default, an IM is enabled for all Japanese, Korean, and Chinese locales. To enable an IM in other locales, you must edit `vars.exp` and add the locale to the IM_localeList variable.

SGD Client Termination Timeouts

If an application is terminated because the SGD Client exits unexpectedly, an additional value of 20 minutes is added to the following timeouts:

- T**imeout for User Session Resumability** – For applications configured to be resumable during the user session
- **Timeout for General Resumability** – For applications configured to be generally resumable

Changes in Version 4.31

This section describes the changes since the Sun Secure Global Desktop Software 4.30 release.

SecurID Authentication on Solaris x86 Platforms

In version 4.31, you can use SecurID authentication when SGD is installed on Solaris x86 platforms.

Support for Multiple SGD Servers in Integrated Mode

In version 4.30, it is possible to connect only to one SGD server when the SGD Client is in Integrated mode. In version 4.31, Integrated mode can be used with multiple SGD servers. In the desktop Start or Launch menu, a login link is available for each SGD server.

Array Routes

SGD has an array routes feature that enables you to configure server-side SOCKS proxy servers. You configure array routes with the following command:

```
$ tarantella config edit \
--tarantella-config-array-netservice-proxy-routes route...
```

Array routes are enhanced so that you can now configure a direct connection type. Use `CTDIRECT` as the connection type to specify the clients that can connect without using a proxy server.

The following is an example array route configuration:

```
$ tarantella config edit \
--tarantella-config-array-netservice-proxy-routes \
"192.168.5.*:CTDIRECT:" \
"192.168.10.*:CTSOCKS:taurus.indigo-insurance.com:8080"
```

With this configuration, clients with IP addresses beginning `192.168.5` have a direct connection. Clients with IP addresses beginning `192.168.10` connect using the SOCKS proxy server `taurus.indigo-insurance.com` on TCP port 8080.

SGD Start-up Scripts

In version 4.31, the start-up scripts that ensure SGD services stop and start when an SGD server is rebooted are renamed and restructured. The `*Tarantella` and `*TarantellaWebserver` scripts are replaced by a single script named `*sun.com-sgd-base`. The `*tem` script for the SGD Enhancement Module is now named `*sun.com-sgd-em`.

Untrusted Initial Connection Message

The Untrusted Initial Connection warning message that displays when users first connect to an SGD server is enhanced. Users can now view the server's security certificate from this message.

Windows Key Disabled

By default, the Windows key is now disabled in SGD Windows Terminal Services sessions. The Windows key is honored in local Windows sessions only. To display the Windows Start menu in an SGD Terminal Services Session, press Alt+Home.

The SGD Terminal Services Client (`ttatsc`) now supports an additional `-windowskey on|off` option that enables you to enable support for the Windows key. You can specify this option with the Arguments for Protocol (`--protoargs`) attribute on the Windows application object.

Changes in Version 4.30

This section describes the changes since the Sun Secure Global Desktop Software 4.20 release.

Single Installable Package

Version 4.3 introduces a single package for installing SGD. When you install SGD, you install all the packages that previously had to be installed separately, including the font packages. The license keys installed in the array control the SGD components that can be used.

SSL Daemon Always Running

As the initial connection to SGD is now always secure, this means that the SGD SSL Daemon is always running even if SGD security services are not enabled.

User Preferences File on UNIX Platform, Linux, and Mac OS X Client Devices

In previous releases, a user preferences file was used to configure the SGD Client on UNIX platform, Linux, and Mac OS X client devices. With the introduction of profiles, this file is no longer used.

Window Close Action (`--windowclose`) Attribute

In previous releases, the Window Close Action (`--windowclose`) attribute was only available to X applications that were configured to display using client window management. The use of this attribute is extended to include X, Windows, and character applications that are configured to display using an independent window.

The change means that closing an independent window might end or suspend the application session. The default is to end the session.

Support for PAM for UNIX Platform User Authentication

SGD now supports Pluggable Authentication Modules (PAM) for UNIX platform user authentication. The change affects the following UNIX authentication mechanisms:

- Search Unix ID in Local Repository (ENS)
- Use Default User Profile (UNIX User)
- Search Unix Group ID in Local Repository (UNIX Group)

SGD uses PAM for user authentication, account operations and password operations.

When you install SGD on Linux platforms, Setup automatically creates PAM configuration entries for SGD by copying the current configuration for the `passwd` program and creating the `/etc/pam.d/tarantella` file. On Solaris OS platforms, you can add a new entry for SGD (`tarantella`) in the `/etc/pam.conf` file if required.

Using PAM gives SGD Administrators more flexibility and control over UNIX platform user authentication, for example by adding new login tests, account limits, or valid password checks.

PDF Printing

As a result of the changes introduced in this release to support PDF printing on UNIX platform, Linux, and Mac OS X client devices, the Display Adobe Reader Print dialog (`--pdfprompt`) attribute is removed.

This change means that when users print with the Universal PDF Printer printer on Windows clients, the print job is automatically sent to the client's default printer. To be able to choose the client printer where a print job is sent, users must now select the Universal PDF Viewer printer.

Client Certificates for Active Directory Authentication

For Active Directory authentication, a Client Certificates checkbox is available in the Authentication Wizard. If Active Directory is configured to require a client certificate and you created and installed a client certificate for SGD, then you no longer need to configure the username and password of a privileged user.

SGD Certificate Store

The password used for the SGD certificate store, */install-dir*`/var/info/certs/sslkeystore`, is no longer hard-coded to `123456`. Instead, each store now has a random password, which is stored in */install-dir*`/var/info/key`. Use this password with the `-storepass` and `-keypass` options when using the `keytool` application.

Licensing

Version 4.2 contained the following changes to licensing:

- Activation license keys are no longer required to enable an array.
- Named user licensing is no longer available.
- Maintenance and Right to upgrade license keys are no longer available.

If you upgrade from an earlier version, your existing product license keys are automatically converted and your existing Maintenance and Right to Upgrade license keys are deleted.

Application Connection Methods

From version 4.1, SGD no longer supports the `rlogin` and `rcmd` connection methods for starting applications. If you upgrade from an earlier version, you must change the connection method for any applications that use these methods.

Simultaneous Webtop Connections Attribute

From version 4.1, SGD uses a different attribute for the Maximum Simultaneous User Sessions setting (`--tuning-maxconnections`). If you upgrade from an earlier version, the default setting for this attribute is applied.

Mainframe (3270) Applications

From version 4.0, SGD uses a different emulator for mainframe (3270) applications. 3270 character and 3270 X application objects are no longer available and are replaced by a single 3270 application object. As the new 3270 application object has several new attributes, it is not possible to upgrade existing 3270 application objects. If you upgrade from an earlier version, your existing 3270 character and 3270 X applications are deleted when you upgrade. You must reconfigure these applications.

CHAPTER 3

Support Statements, Known Issues, Bug Fixes, and Documentation Issues

This chapter contains support information for SGD.

Topics in this chapter include the following:

End-Of-Support Statements

The following table lists the end-of-support dates for SGD products.

Software and Version	End of Full Support	End of Limited Support	End of Service Life
Sun Secure Global Desktop Software 4.3	April 29, 2009	April 29, 2013	April 29, 2013
Sun Secure Global Desktop Software 4.2	November 8, 2008	November 8, 2012	November 8, 2012
Secure Global Desktop Enterprise Edition 4.1			March 31, 2007
Secure Global Desktop Enterprise Edition 4.0			March 31, 2007
Secure Global Desktop Software Appliance 4.0			March 31, 2007

Software and Version	End of Full Support	End of Limited Support	End of Service Life
Secure Global Desktop Enterprise Edition 3.44*			December 31, 2007
Secure Global Desktop Enterprise Edition 3.42			March 31, 2007
Tarantella Enterprise 3 (including TASP)			March 31, 2007

* Japanese only

For details of the Sun End of Service Life (EOSL) Policy, see `http://www.sun.com/service/eosl/`.

Customers with a valid support agreement can upgrade to the latest version of SGD free of charge.

Known Bugs and Issues

This section lists the known bugs and issues with SGD version 4.40.

602423 - Return Key and Keypad Enter Key Issues

Problem: SGD X and character emulators cannot distinguish between the Return key and the keypad Enter key on the user's client keyboard.

Cause: A known issue.

Solution: By default, the SGD Client maps the keypad Enter key to Return in both X and character application sessions. With additional configuration, this behavior can be changed.

To change the behavior of the keypad Enter key in a *character application* session, you need to set up a keymap for your character application object (`--keymap`) and add a mapping for `KPENTER`, for example:

```
KPENTER="hello"
```

To change the behavior of the keypad Enter key in a *Windows* or *X application* session, you need to modify your X keymap (for example, `xuniversal.txt`) and add a mapping for the `KP_Enter` key, for example:

```
92 KP_Enter KP_Enter NoSymbol NoSymbol 0x801c
```

Caution – The X keymap is a global user resource, so all applications for that user might be affected by this change. If any of these applications do not handle `KP_Enter`, then you might need to consult your X or Windows application vendor for assistance.

6443840 - Automatic Proxy Server Configuration Scripts Fail

Problem: Proxy server automatic configuration scripts can specify a list of proxy servers to try. If the first proxy server in the list is unavailable, the browser tries the other proxy servers in turn until it finds one that is available.

If you are using Microsoft Internet Explorer with Sun Java Plug-in tool version 1.5.0, only the first proxy server in the list is used. If that proxy server is not available, the connection fails.

Cause: A known issue.

Solution: Use Sun Java Plug-in tool version 1.6.0.

6448990 - Backslash and Yen Keys Problems

Problem: When using Japanese PC 106 or Sun Type 7 Japanese keyboards with Windows applications running through SGD, the Yen and Backslash keys produce the same result.

Cause: A known issue with key handling.

Solution: Modify the Xsun keytable or the Xorg keytable on the client device.

For example, change the `/usr/openwin/etc/keytables/Japan7.kt` file as follows:

```
...
#137     RN       XK_backslash     XK_bar  XK_prolongedsound
137     RN       XK_yen           XK_bar  XK_prolongedsound
...
#39      RN       XK_0     XK_asciitilde   XK_kana_WA       XK_kana_WO
39      RN       XK_0     XK_0            XK_kana_WA       XK_kana_WO
...
```

For example, change the `/usr/X11/lib/X11/xkb/symbols/sun/jp` file as follows:

```
...
# key <AE13> { [ backslash, bar      ], [ prolongedsound    ]      };
  key <AE13> { [ yen, bar       ], [ prolongedsound     ]       };
...
# key <AE10> { [ 0, asciitilde      ], [ kana_WA, kana_WO   ]      };
  key <AE10> { [ 0, 0], [ kana_WA, kana_WO   ]       };
...
```

After making these changes, you must restart `dtlogin`:

```
# /etc/init.d/dtlogin stop
# /etc/init.d/dtlogin start
```

6456278 - Integrated Mode Does Not Work for the Root User

Problem: On Solaris 10 x86 platforms, enabling Integrated mode when you are logged in as the `root` user does not add applications to the Solaris 10 Launch menu. You might also see the following warning:

```
gnome-vfs-modules-WARNING **: Error writing vfolder configuration
file "//.gnome2/vfolders/applications.vfolder-info": File not found.
```

Cause: A known issue with the Gnome Virtual File System (VFS).

Solution: No solution is currently available.

6458111 - Gnome Main Menu Crashes Using Integrated Mode

Problem: On client devices running SUSE Linux Enterprise Server 10, the Gnome Main Menu crashes when using the SGD Client in Integrated mode. The crash usually occurs on login or logout.

Cause: A known problem with the Gnome Main Menu applet on SUSE Linux Enterprise Server 10 (Novell bug reference 186555).

Solution: Install the latest version of the `gnome-main-menu.rpm` package for SUSE Linux Enterprise Server 10.

Alternatively, disabling the Recently Used Applications functionality improves the stability of the Gnome Main Menu. Run the following commands on the client device:

```
$ gconftool-2 --set --type=list --list-type=int \
/desktop/gnome/applications/main-menu/lock-down/showable_file_types [0,2]
$ pkill main-menu
$ pkill application-browser
```

6461864 and 6476661 - Automatic Login and Integrated Mode Fails With the Gnome Desktop

Problem: After enabling Automatic Client Login or Integrated mode, the SGD Client does not start automatically when you log in to the Gnome Desktop and the Start menu is not updated with webtop content when you log in to SGD. This problem affects SUSE Linux Enterprise Server 9 and Red Hat Enterprise Linux 4.

Cause: The directories containing the `.menu` files are not monitored and so changes to the Start menu are not detected.

Solution: The workaround is run the `pkill gnome-panel` command to restart the gnome-panel and pick up new menu information.

Note – You must run the `pkill gnome-panel` command to update the menu *each time* the menu changes.

6468716 - Keyboard Does Not Work in Gnome Sessions

Problem: After starting a Gnome session on Solaris 10 OS on Sparc platforms, users are unable to input anything with the keyboard. The mouse, however, does work.

Cause: A known bug with remote Gnome sessions. The Sun Microsystems bug reference is 6239595.

Solution: This problem was fixed in patch number 119542. This patch was also included in a cumulative patch ID 122212 for the Gnome Desktop.

The workaround is to create a Gnome configuration file `/etc/gconf/gconf.xml.defaults/apps/gnome_settings_daemon/keybindings/%gconf.xml` with the following content:

```
<?xml version="1.0"?>
<gconf>
<entry name="volume_up" mtime="1110896708" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="volume_mute" mtime="1110896705" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="volume_down" mtime="1110896702" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="help" mtime="1110896698" type="string">
<stringvalue></stringvalue>
</entry>
</gconf>
```

6470197 - Compiling SGD Web Server Modules Fails

Problem: When you compile your own Apache modules for use with the SGD Web Server, the compilation fails because of a missing egcc compiler.

Cause: The configuration file for the Apache eXtenSion tool (`apxs`) that is used to build extension modules for the SGD Web Server uses the egcc compiler and this might not be available on your system.

Solution: Either modify the `apxs` configuration file to use a compiler that is available on your system, or create a symlink for `egcc` that links to the compiler on your system. The `apxs` configuration file is located at */install-dir*/webserver/apache/*version*/bin/apxs.

6476194 - No KDE Desktop Menu Item for the SGD Client

Problem: Shortcuts for the SGD Client do not display on the KDE Desktop Menu on SUSE Linux Enterprise Server 10.

Cause: SUSE-specific configuration of the KDE menu system means that if a menu contains only one application entry, then that single application is used in the main menu instead of the menu. If menu entry is a sub-menu, the sub-menu does not display at all. This causes the Login menu for the SGD Client in Integrated mode not to display.

Solution: The workaround is to add the following line to the `[menus]` section of the `$HOME/.kde/share/config/kickerrc` file:

```
ReduceMenuDepth=false
```

Then run the following command for the KDE panel to immediately pick up the changes:

```
# dcop kicker kicker restart
```

All subsequent KDE sessions automatically use this setting.

6477187 - Client Drive Mapping Fails Without the Client for Microsoft Networks

Problem: Client drive mapping fails if the Client for Microsoft Networks is not enabled on a Microsoft Windows application server.

Cause: The Client for Microsoft Networks must be enabled to allow remote access to files and folders.

Solution: Enable the Client for Microsoft Networks.

▼ How to Enable the Client for Microsoft Networks

1. **In the Control Panel, double-click Network Connections.**
2. **Right-mouse click the network card and select Properties.**
3. **On the General tab, check the box next to Client for Microsoft Networks.**
4. **Click OK.**

6481312 - Upgrading Resets the Available Connection Types

Problem: After upgrading to version 4.40, a server that was configured to accept only secure connections now accepts standard and secure connections.

Cause: A known issue.

Solution: Reconfigure the server to accept only secure connections. In the Administration Console, display the Secure Global Desktop Servers ⇒ Security tab for the SGD server and deselect the Standard check box in the Connection Types field. Alternatively, run the following command:

```
$ tarantella config edit --security-connectiontypes ssl
```

6482912 - SGD Client Not Installed Automatically

Problem: Using Internet Explorer 7 on Microsoft Windows Vista platforms, the SGD Client cannot be downloaded and installed automatically. The SGD Client can be installed manually and can be installed automatically using another browser, such as Firefox.

Cause: Internet Explorer has a Protected Mode that prevents the SGD Client from downloading and installing automatically.

Solution: Add the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

6493374 - Non-ASCII Characters in Input Method Windows

Problem: Users in Simplified Chinese and Traditional Chinese locales cannot display non-ASCII characters in the candidate and status windows of the input method when running applications on a Solaris OS application server. This affects Solaris 8, 9, 10 and 10u1 OS platforms.

Cause: Missing font path configuration on the SGD server.

Solution: If the application server is running on Solaris10 or Solaris10u1, do one of the following:

- For SPARC platforms, install patches 120410,120412 and 120414.
- For x86 platforms, install patches 120411,120413 and 12041.
- Upgrade to Solaris 10u2 or higher.

If the application server is running on Solaris 8 or Solaris 9, do one of the following:

- **Simplified Chinese.** Set Environment Variables as "LANG=zh;LC_ALL=zh" in the Applications ⇒ Launch tab of the Administration Console.
- **Traditional Chinese.** Set Environment Variables as "LANG=zh_TW;LC_ALL= zh_TW" in the Applications ⇒ Launch tab of the Administration Console.

6542943 – Firefox Fails Using Sun Java Plug-In Tool Version 1.5

Problem: The Firefox web browser terminates unexpectedly when using Sun Java Plug-in tool version 1.5.0.

Cause: The path to the Java virtual machine (JVM) software changed with release 1.5.0 of the Sun Java Plug-in tool.

Solution: Ensure that there is a symbolic link from the Firefox plug-ins directory to the JVM location at `/usr/local/`*jre-version*`/plugin/i386/ns7/libjavaplugin_oji.so`, where *jre-version* is the Java Runtime Environment (JRE™) software version.

6555834 – Java Technology is Enabled For Browser But Is Not Installed On Client Device

Problem: If Java technology is enabled in your web browser settings, but a Sun Java Plug-in tool is not installed on the client device, the SGD webtop does not display. The login process halts at the splash screen.

Cause: SGD uses the web browser settings to determine whether to use Java technology.

Solution: Install the Sun Java Plug-in tool and create a symbolic link from the web browser plug-ins directory to the location of the JVM. Refer to your web browser documentation for more information.

6591516 - Webtop Page Transitions Not Working in Internet Explorer

Problem: With certain versions of Symantec Client Firewall, such as Version 8.7.4.79, you might experience login problems when using Internet Explorer. The log in process halts at the splash screen and the SGD webtop is not shown.

Cause: The firewall intercepts some JavaScript operations.

Solution: Configure the SGD server as a safe host. Refer to your Symantec documentation for more information.

6592560 – Administration Console Online Help Not Available Over HTTPS

Problem: The online help for the Administration Console is disabled when HTTPS connections to the SGD Web Server are enabled.

Cause: The Administration Console uses the JavaHelp™ software to display the online help. Additional configuration is required to run JavaHelp over an HTTPS connection.

Solution: Import the certificate used to secure the SGD Web Server into the JDK™ software keystore. Use the Java software `keytool` application as follows:

```
$ keytool -import -keystore -storepass changeit \
/install-dir/bin/jdk-version/jre/lib/security/cacerts \
-file /install-dir/var/tsp/ca.pem
```

Where *changeit* is the password for the keystore and *jdk-version* is the version of the JDK installed on the SGD server.

If you have more than one certificate in your `ca.pem` file, separate each certificate and add them individually.

6598048 – French Canadian Keyboard Not Mapped Correctly for Windows Applications

Problem: When using a Canadian French (legacy) keyboard layout with Windows applications, some French characters are printed incorrectly.

Cause: A known issue with Canadian French (legacy) keyboard layouts.

Solution: No known solution. A compatible keymap file is not supplied with SGD at present.

6605404 – Tomcat Resource File Location Change

Problem: After upgrading to version 4.40, you might experience problems configuring secure SOAP connections.

Cause: The `Resources.properties` resource file has been relocated for this release. This file is needed when securing SOAP connections to the Tomcat JSP container. The location of this file for version 4.31 was as follows:

/install-dir/webserver/tomcat/version/webapps/sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/apis/Resources.properties

The location of this file for version 4.40 is as follows:

/install-dir/webserver/tomcat/version/shared/classes/com/tarantella/tta/webservices/client/apis/Resources.properties

Solution: Locate and edit the `Resources.properties` file. Restart the Tomcat JSP container.

6609001 – Cannot Detach a Stopped Secondary Server Using the Administration Console

Problem: If a secondary server is down, you cannot remove it from the SGD array using the Administration Console. Detach operations using the `tarantella array detach` command are not affected.

Cause: In this release, using the Administration Console to detach a secondary server that is down is not supported.

Solution: Restart the secondary server that is down and use the Administration Console to detach it from the SGD array. Alternatively, use the `tarantella array detach` command to remove the secondary server that is down.

6609518 – Array Joining When Running the Administration Console From a Secondary Server

Problem: You cannot add a new secondary server to an SGD array when the Administration Console is running on an existing secondary server.

Cause: In this release, it is not possible to supply credentials for more than one secondary server.

Solution: Run the Administration Console on the primary server, or on the server that is to be joined into the array.

6610760 – Custom PDF Printer Settings Not Applied For Windows Applications

Problem: Custom PDF printer settings are not applied when printing from Windows applications.

For example, if you *enable* the SGD Universal PDF Printer and Universal PDF Viewer printers for an OU object. Then, you override the parent objects setting and *disable* the Universal PDF Printer and Universal PDF Viewer printers for a user in the OU. The custom printer settings are not inherited by the user.

Cause: A known issue when inheriting PDF printer settings.

Solution: No known solution. Configure PDF printer settings at OU or organization level wherever possible, rather than at user level.

6611502 – Errors When Creating and Modifying Objects From a Secondary Server

Problem: Creating or modifying objects when running the Administration Console on a secondary SGD server returns the following error message: “Object could not be created”.

Cause: The creation or modification of the object is successful, but the Administration Console proceeds before the replicated data has come back from the primary server.

Solution: Wait for a couple of seconds and then repeat the operation.

Sun Type 7 Japanese Keyboard Issues

Problem: Users with Sun Type 7 Japanese keyboards cannot input characters correctly using SGD.

Cause: Missing Solaris OS keytable on the client device.

Solution: Install the appropriate patch to install the keytable on the client device:

Platform	Patch
Solaris 10 OS on SPARC platforms	121868
Solaris 9 OS on SPARC platforms	113764
Solaris 8 OS on SPARC platforms	111075
Solaris 10 OS on x86 platforms	121869
Solaris 9 OS on x86 platforms	113765
Solaris 8 OS on x86 platforms	114539

Start Menu Items Not Sorted Alphabetically

Problem: When using the SGD Client in Integrated mode on Microsoft Windows client devices, users might notice that the Start menu entries are not sorted alphabetically.

Cause: This is caused by a Windows feature that adds new items to end of a menu rather than preserving the alphabetical sorting.

Solution: See Microsoft KB article 177482 for details.

No Launch Menu Entries on Sun Java Desktop Systems

Problem: On Sun Java Desktop Systems, users might find that Launch menu entries are not created for SGD when they enable Integrated mode. The Launch menu entries are added when they log out of their desktop and log in again.

Cause: A known issue with the Gnome panel.

Solution: The solution is to install the following patches:

- 119906 for Solaris OS on SPARC technology platforms
- 119907 for Solaris OS on x86 platforms

The workaround is to log out of the desktop and log in again.

Bug Fixes in Version 4.40

The following table lists the significant bugs that are fixed in the 4.40 release.

Reference	Description
2144612	Active Directory authentication does not failover to the next global catalog.
2147536	`ttaxpe` command does not exit if an incorrect password is entered.
2148699	CDM fails with multiple external DNS names.
2148700	SGD Client fails when an X application opens a specific window.
2148811	Printer preferences on Terminal Services not set permanently with Zebra bar code printer.
2149630	Korean keyboard does not work correctly with SSGD 4.30.915.
2150849	Intermittent problems with serial COM port redirection.
2151274	Accented characters fail in French locale windows.
6469935	SGD Client should be able to match hostname to DNS item in certificate subjectAltName extension.
6478585	Java virtual machine SSL key and certificate store destroyed on upgrade.
6520742	The `tarantella security peerca --show` command fails on primary SGD server.
6525004	Extend client device access logging in the SGD Client.
6527507	Better error reporting for web service failures.
6532425	UNIX CDM fails if `tta_tem` is installed in non-standard directory.
6532764	LDAP failover is not seamless when multiple LDAP servers are configured.
6537643	SGD Client crashes if application exited while dialog displayed.
6541478	SGD session hangs if audio played from SGD while local audio is playing on Sun Ray Client.
6541914	CDM does not work in Windows Vista in certain scenarios.
6542533	Webtop does not update to display launched applications in Safari on MacOS X 10.4.9.
6544350	Webtop print controls are unstable in an array.
6546840	Integrated mode is not enabled on SUSE Linux Enterprise Server 9.
6547337	Using `-preferredlanguage` option for `ttatcc` command does not open page in appropriate locale.
6550172	Launch fails if offline server selected in a load balanced group.

Reference	Description
6552038	Improvements to `ttaxpe` debug logging.
6553252	SGD Client exits with segmentation faults and is terminated by Electric Fence application.
6558691	Secondary licenses are removed when primary stopped or array breaks apart.
6561306	Check `ssh` version before updating `ssh` arguments.
6563481	Improve error messages in `execpe` log files.
6571826	Command line for creating 3270 and 5250 objects does not accept all arguments correctly.
6574469 6574471	Update Java Platform, Standard Edition to 1.6.0_01 or later (third party) for Solaris and Linux platforms.
6583316	CDM cannot be disabled on a per-client basis for SGD clients.
6583333	`ssh` launch failure when `sshhelper` is setuid, and SGD user has no home directory.
6597576	SGD Enhancement Module for Linux platforms does not get installed in non-default path.
6598686	Application title is garbaged on locales.
6601084	In Integrated mode, the folder specified in the “Start In” box is invalid.

Bug Fixes in Version 4.31

The following table lists the significant bugs that are fixed in the 4.31 release.

Reference	Description
2140625	Time zone redirection is fixed for clients on UNIX platforms.
2145026	Licensing information is not copied to all the secondaries until after a restart.
2145602	X application launch is slow or times out. Possible error in the Input Method handling in the `procs.exp` script.
2145932	Windows key functionality is being held when returning to SGD session.
2146043	Using client drive mapping, you cannot overwrite a larger file.
2146285	Tomcat fails and icons do not appear on the webtop.
6440254	The proxy server authentication dialog does not display realm information.
6443192	Upgrading using the `pkgadd` command on Solaris OS reports hundreds of file conflicts.

Reference	Description
6443840	The SGD Client does not understand proxy failover from proxy server configuration (PAC) files.
6474180	The `HARD_SERVER_LIMIT` of the SGD Web Server is increased to 1024.
6480225	In Integrated mode, applications fail to resume on UNIX client platforms.
6494450	Client drive mapping cannot handle files larger than 2 gigabytes.
6499639	A recursive directory request causes a segmentation fault when using client drive mapping on UNIX and Linux platforms.
6503627	The `xfrbelgian.txt` keyboard map file contains a mistake.
6518152	Start menu is not updated on a using Integrated mode on Microsoft Windows Vista client devices.
6518638	The `tarantella print cancel` command deletes all print jobs instead of just the selected job.
6525384	XRDP does not work with SGD.
6528037	Page Not Found displays on the webtop when a group containing hosts is deployed by mistake to a webtop.
6506222	A user's `.Xdefaults` file is not used when launching an application.

Bug Fixes in Version 4.30

This section lists the significant bugs that are fixed in the 4.30 release. The bug fixes are divided into the following areas:

Administration Tools

The following bugs with the SGD administration tools are fixed.

Reference	Description
6433525	`/usr/bin` owner is changed to ttasys on startup.
6436735	The `tarantella object new_xapp` command does not accept the `--accel` argument.
6437203	Object Manager shows a warning message after renaming an ENS object.
6445405	Shadowing from the command line takes an invalid session ID.
6447937	X authority cookies must not be passed using environment.
6450323	Attributes cannot be specified in object creation but can be set in object edit.
6451537	`tarantella license` commands and Array Manager display obsolete software components.

Application Launch

The following bugs with launching applications are fixed.

Reference	Description
6357003	The Native Client cannot launch a web browser on Solaris OS.
6357022	Native Client shifts up the full-screen webtop on Java Desktop System.
6392279	X authorization issue causes launch failure.
6401949	With `optimizelaunch` enabled in the `unix.exp` login script, the expired password handler does not work.
6405808	The filtering script (`runsubscript.exp`) is not being called during the launch process.
6416951	Error message is displayed when a new browser window application is ended with the X button.
6419574	The authentication dialog returns corrupted data if the password has more than eight characters.
6427189	Launch failure occurs when the host is not known to SSH.
6434660	Password expiry handling on application launch is broken.
6447551	There should only be one ttacpe process created for each webtop session.
6455378	Launch failure when SSH used over `su` for an application running on the SGD host.

Reference	Description
6464809	# characters in system login banner cause automated launch process to fail.
6470173	Add support for SecurID ACE agent for PAM.
6475303	Custom Certificate Authority certificates are not recognized and cause a prompt when launching in-place applications.
6476180	Root window stays around when logging out of a kiosk Gnome session.

Clients and Webtop

The following bugs with the SGD clients and webtop are fixed.

Reference	Description
6408157	Local X server application does not launch from the JSP software webtop.
6417140	The webtop frame is blank after launching an application.
6417575	UNIX Native Client using a proxy server: log in, log out, log in again and the Native Client hangs.
6417631	UNIX Native Client: redraw problems with kiosk applications.
6424776	SGD Client produces errors and exits when logging out of the webtop.
6432133	The SGD Native Client causes a segmentation fault if you close the connection progress window.
6465959	When SGD restarts, the SGD Client spins and sends out hundreds of network packets.
6468173	On Sun Ray thin clients, the wait cursor is no longer set permanently.

Emulation

The following emulation bugs are fixed.

Reference	Description
6381531	Edited `colormap.txt` intermittently ignored when security is enabled.
6386091	SGD Native Client for Windows and Citrix ICA X Client: possible key event incompatibility.
6415498	Character terminal session closes unexpectedly when function keys are pressed.

Reference	Description
6417698	Scalable windows applications do not toggle when scroll lock pressed on Java Desktop System on Solaris 10 OS.
6426355	`ttaxpe` exits with a segmentation fault.
6427789	Copy (ctrl+insert) causes X applications to hang.
6433273	Using the Native Client on Solaris OS, kiosk mode does not display correctly.
6435437	Child window sometimes comes up below the parent window using seamless windows.
6435489	Performance improvements for Windows applications.
6435527	Segmentation fault in the ttaxpe when running the HP monitoring tool.
6445467	Windows Logo keys do not work in a Terminal Services session.
6446469	Problems with the French locale and keymap.
6467368	Letter repeated twice in Remote Desktop Protocol session.
6471395	Timezone redirection fails to set correct time during daylight saving time. Time always out by one hour.
6472959	ESC-NumLock does not work as expected from Solaris OS client and Sun Ray thin clients.

Installation and Upgrade

The following installation and upgrade bugs are fixed.

Reference	Description
6355269	The default configuration for a Java Desktop System session loses some important configuration parameters.
6368390	Upgrade from 4.20.909 to later builds requires a maintenance or right to upgrade license.
6368675	Root certificates for secure LDAP servers are not retained during an upgrade.
6396629	Install fails during bean creation and server does not start.
6407985	SGD incorrectly handles large amount of free disk space at install.
6430913	Web server configuration file (`httpd.conf`) is not upgraded correctly.
6446020	Unable to uninstall SGD if the external DNS name is incorrect.
6453638	Cannot log in to an SGD server after an upgrade.
6462429	SGD is uninstalled even though user selects No.

Internationalization and Localization

The following internationalization and localization bugs are fixed.

Reference	Description
6354105	In Configuration Wizard, the application list shows corrupt strings with multi-byte characters.
6355226	The Connection Progress dialog cannot display multi-byte characters.
6357040	Cannot copy and paste from Microsoft Windows to Solaris OS.
6357075	Cannot copy and paste from Microsoft Windows to Microsoft Windows.
6357606	Cannot copy and paste from Java Desktop System to Common Desktop Environment.
6362374	Client drive mapping daemon crashes with a localized `native-cdm-config` file.
6419511	Windows applications should have Unicode as the Euro symbol default.
6419523	Server LANG environment overrides client locale setting.
6447594	Client window mode should be accessed with an IP address instead of UNIX platform socket
6450008	Cannot generate an apostrophe with a Swedish keyboard.

Other

The following miscellaneous bugs are fixed.

Reference	Description
6375600	Authentication fails with ActivCard - Cyberflex 64k Smart Card (also bug ref 607218).
6384746	Able to read Common Gateway Interface Files (`.cgi`) files using a web browser.
6390126	A large number of users logging in in quick succession hangs the SGD server.
6393623	New browser window gets launched when new browser windows applications are launched with the CTRL key pressed.
6407855	SGD server exits with error code 129, signal 0.
6408159	New blank browser window opens on exiting the application opened in new browser window mode.
6409117	SGD Enhancement Module for Solaris OS x86 platforms appears to fail.

Reference	Description
6409765	Error copying large files from client to server over a slow network in RDP sessions.
6410161	Using telnet to connect to localhost port 1023 causes the Protocol Engine Manager to use 100% CPU.
6416384	RDP-based audio output stops playing when using a Sun Ray thin client.
6418965	Client window manager applications display Minimize and Maximize buttons that are not present in original application.
6430243	SGD Apache includes development private paths and configurations.
6430396	Unable to copy paste to and from a WCP IWM session from the classic webtop.
6436155	Setting the keepalive to 0 causes keepalives to be sent continuously.
6442142	Quitting Gnome session causes ttaxpe to use 100% CPU.
6446271	SGD Web Server starts but remains attached to the console.
6466415	Secure LDAP does not work without security licenses installed.

Printing

The following printing bugs are fixed.

Reference	Description
6376221	Printer properties (such as paper size) do not appear to be stored between RDP sessions.
6406292	Driver name duplicated if printing is configured at OU and user level.
6421283	Windows Native Client detects `DEFAULT_PRINTER_UNKNOWN` when no printer is configured on the client device.
6427852	Login delay induced by inaccessible network printer attached to client device.

Security

The following security bugs are fixed.

Reference	Description
6419520	LDAP searches of Active Directory contacts AD servers in other regions for information.
6446338	The prompt for password change does not appear after a password expires.
6446437	Cannot create an array after enabling SSL connections between array members.
6457984	Validate user input to the login box to prevent cross-site scripting attacks.
6468699	SSL daemon core dumps due to `sigsegv`, signal 11.
6469123	OpenSSL security patch secadv_20060905.txt needs to applied.
6476728	OpenSSL security patch secadv_20060928.txt needs to be applied.
6478735	Fixed a vulnerability with the SGD Cascading Stylesheets.

Server

The following bugs with SGD servers and arrays are fixed.

Reference	Description
6379743	`tarantella status` command report is incorrect when SSL connections between array members is enabled.
6392365	Array problems when one of the array members is not contactable.
6393745	Cannot successfully promote a secondary server to a primary if the primary server is down.
6445200	Array behavior when joining and detaching members of an array that is licensed.

User Authentication

The following bugs with user authentication are fixed.

Reference	Description
6383417	If the `krb5.conf` file has errors, user login hangs and the server continuously writes exceptions to `jserver.log`.
6400123	Ambiguous login is not allowed if invalid credentials are provided the first time.
6415709	Active Directory authentication fails silently if one tree of a forest is not configured in the `krb5.conf` file.
6439688	SGD Native Client for Windows does not display an error message if an Active Directory password change fails.
6454261	Expect script updated for German Solaris OS applications.
6460263	Oberthur AuthentIC card is not recognized when using SGD (fixed for Windows Clients only).
6465569	Active Directory PKI infrastructure does not failover to the next global catalog server.
6471877	SecurID login authority does not work correctly.

Web Services

The following bugs with SGD web services are fixed.

Reference	Description
6391262	Anonymous users can create and edit webtop groups. This information is stored on disk and not cleaned up.
6427185	SGD Web Server exposes too much information.

Documentation Issues in Version 4.40

This section lists the known documentation issues for release 4.40.

Assigned User Profiles Tab Changes

The tables in the Applications ⇒ Assigned User Profiles tab of the Administration Console have changed as follows:

- **Effective User Profiles table.** The Repository column in this table has been removed. User profiles from the local repository are listed in the Local Assignments area of this table. Users and groups from an LDAP directory are listed in the LDAP Assignments area of this table. The LDAP Assignments area of this table is only shown if the Local + LDAP setting is selected for the Repository field in the User Profiles tab. You can click the Load LDAP Assignments link to refresh this area of the table.
- **Editable Assignments table.** The Repository column in this table has been renamed to "Assignment Type".

The "Assigned User Profiles Tab" section on page 119 of the *Sun Secure Global Desktop 4.4 Reference Manual* does not document these changes.

Tomcat Resource File Location Change

The `Resources.properties` resources file has been relocated for version 4.40. This file is needed when securing SOAP connections to the Tomcat JSP container.

The location of this file for release 4.40 is as follows:

/install-dir`/webserver/tomcat/`*version*`/shared/classes/com/tarantella/tta/webservices/client/apis/Resources.properties`

Details of the file location change are missing from the released documentation.

Automatic Timeout of Idle User Sessions

Details of how to configure the user session idle timeout are missing from the released documentation.

This attribute specifies a value for automatic timeout of inactive user sessions. User sessions are suspended if there has been no application session or webtop activity for the specified period.

You can specify this attribute using the following command:

```
$ tarantella config edit \
--tarantella-config-array-webtopsessionidletimeout secs
```

Replace *secs* with the timeout value, measured in seconds.

A setting of 0 turns off the user session idle timeout feature. This is the default setting.

Window Type (`--displayusing`) Command Options

Page 214 of the *Sun Secure Global Desktop 4.4 Reference Manual* incorrectly states that the following command-line options are available when specifying the Window Type (`--displayusing`) attribute:

- `webtop`
- `newbrowser`

These options have been deprecated for the 4.40 release.

Errors When Creating and Modifying Objects From a Secondary Server

Problems might be experienced in creating or modifying objects when running the Administration Console on a secondary SGD server. This is due to the Administration Console not waiting long enough for data replication from the primary server to complete before proceeding.

The Administration Console can be configured to wait for a certain period of time after an object has been created or modified. The time period is defined by the `com.sun.tta.confmgr.ArraySyncPeriod` setting in the `web.xml` configuration file for the Administration Console. The `web.xml` file is located in the `/`*install-dir*`/webserver/tomcat/`*version*`/webapps/sgdadmin/WEB-INF/` directory on an SGD server.

Details of this setting are missing from the released documentation.

Creating Entries in the Password Cache

The following information about using the Adminstration Console to create entries in the password cache is missing from the released documentation.

The Global Settings ⇒ Caches ⇒ Passwords tab is used to manage password cache entries. You can also add password cache entries at this tab, using the Create New Password Cache Entry page. This is equivalent to using the `tarantella passcache new` command.

It is important that you enter a valid name in the User Identity or Server fields on the Create New Password Cache Entry page. The Administration Console supports several ways that you can enter a name in the User Identity or Server field, as follows:

- **Browse button.** If the selected User Identity Type option is Local or LDAP/Active Directory, you can use the Browse button next to the User Identity or Server field to browse for object names. Using the Browse button in this way avoids errors when typing in object names.
- **Full Name.** Type the *full name* into the field. For example, you can type in the full name for an application server from the local repository as follows:

  ```
  .../_ens/o=appservers/cn=boston
  ```

- **Partial Name.** Type a *partial name*, without the namespace prefix, into the field. Depending on the selected User Identity Type option, the Administration Console adds the relevant namespace prefix when the password cache entry is saved. For example, you can type in the partial name for a user identity from the UNIX repository as follows:

  ```
  o=organization/cn=indigo-jones
  ```

  The Administration Console adds the `.../_user` namespace prefix when the password cache entry is saved.

  The following table shows the namespace prefixes that the Administration Console adds for the selected User Identity Type option.

User Identity Type	Namespace Prefix
Local	`.../_ens`
UNIX (User/Group)	`.../_user`
Windows Domain Controller	`.../_wns`
LDAP/Active Directory	`.../service/sco/tta/ldapcache`
SecurID	`.../service/sco/tta/securid`
Anonymous	None
Third Party	`.../service/sco/tta/thirdparty`

  If you specify a partial name in the Server field, the Adminstration Console adds the `.../_ens/o=appservers` namespace prefix when the password cache entry is saved.

LDAP names must be typed in using the SGD naming format. The following example shows a partial name for a user identity from an LDAP repository:

```
dc=com/dc=example/cn=indigo-jones
```

This name is converted to the correct LDAP format when the password cache entry is saved, as follows:

```
.../_service/sco/tta/ldapcache/cn=indigo-jones,dc=example,dc=com
```

Corrections to the "Securing the SOAP Connections to an SGD Server" Page

The "Securing the SOAP Connections to an SGD Server" page in the *Sun Secure Global Desktop 4.4 Administration Guide* contains errors.

In Step 2, the following paragraph is incorrect:

"You must add the X.509 certificate for each SGD server in the array. The certificate for each server is stored in `/opt/tarantella/var/tsp/cert.pem`."

The corrected paragraph is as follows:

"You must add the X.509 certificates to enable the SGD server to be able to form a trusted certificate chain. The certificate chain for each server is stored in `/opt/tarantella/var/tsp/ca.pem`."

The paragraph describing the `keytool` command line is incorrect. The corrected paragraph is as follows:

```
$ keytool -import -keystore -storepass changeit \
/install-dir/bin/jdk-version/jre/lib/security/cacerts \
-file /install-dir/var/tsp/ca.pem -alias hostname
```

Where *changeit* is the password for the keystore, *jdk-version* is the version of the JDK installed on the SGD server, and *hostname* is a name used to identify the certificate.

If you have more than one certificate in your `ca.pem` file, separate each certificate and add them individually.