



Sun Secure Global Desktop 4.5 Gateway Administration Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 820-6691-10
April 2009, Revision 01

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

Copyright 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, JavaServer Pages, JSP, JVM, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Adobe is the registered trademark of Adobe Systems, Incorporated.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun Java, JavaServer Pages, JSP, JVM, et Solaris sont des marques déposées ou enregistrées de Sun Microsystems, Inc. ou ses filiales aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Adobe est une marque enregistrée de Adobe Systems, Incorporated.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont regis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont regis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Adobe PostScript

Contents

Preface xi

1. Installing the SGD Gateway 1

About the SGD Gateway 1

System Requirements 2

Known Issues 2

Performing the Installation 3

▼ How To Install the SGD Gateway 3

2. Configuring the SGD Gateway 7

Deploying the SGD Gateway 7

Basic Deployment 7

Load-Balanced Deployment 9

SGD Gateway Configuration Tasks 12

Client Device to SGD Gateway Connections 12

▼ How to Configure the Ports and Connections for the SGD Gateway 12

▼ How to Install an SSL Certificate for Client Connections Into the Client Keystore 13

SGD Gateway to SGD Server Connections 14

▼ How to Install SGD Server Certificates 14

▼	How to Install SGD Gateway Certificates on the SGD Array	16
▼	How to Configure SGD Client Connections	17
	Client Device to Load Balancer Connections	17
	Load Balancer to SGD Gateway Connections	17
	Controlling the SGD Gateway	18
	Starting the SGD Gateway	18
	Stopping the SGD Gateway	18
	Restarting the SGD Gateway	19
	Removing the SGD Gateway	19
▼	How To Remove the SGD Gateway	19
A.	SGD Gateway Architecture Overview	21
	SGD Gateway Architecture	21
	Components of the SGD Gateway	25
	About Routing Tokens	25
	Keystores Used By the SGD Gateway	26
	Routing Proxy Configuration File	27
	Apache Web Server Configuration Files	27
	Configuring Reverse Proxying and Load Balancing	28
	Apache Modules Used by the SGD Gateway	28
	Supported Cipher Suites	29
B.	Command-Line Reference	31
	The <code>gateway</code> Command	31
	Syntax	31
	Description	32
	Examples	32
	<code>gateway start</code>	33
	Syntax	33

Description	33
Examples	33
gateway stop	33
Syntax	33
Description	33
Examples	34
gateway restart	34
Syntax	34
Description	34
Examples	34
gateway config	34
Syntax	34
Description	35
Examples	35
gateway config create	35
Syntax	35
Description	36
Examples	36
gateway config list	36
Syntax	37
Description	37
Examples	37
gateway config edit	38
Syntax	38
Description	38
Examples	39
gateway config enable	39
Syntax	39

Description	40
Examples	40
gateway config disable	40
Syntax	40
Description	41
Examples	41
gateway server	41
Syntax	41
Description	42
Examples	42
gateway server add	42
Syntax	42
Description	42
Examples	43
gateway server remove	43
Syntax	44
Description	44
Examples	44
gateway server list	44
Syntax	44
Description	44
Examples	45
gateway status	45
Syntax	45
Description	45
Examples	45
gateway version	45
Syntax	45

Description	46
Examples	46
gateway sslcert	46
Syntax	46
Description	46
Examples	46
gateway sslcert export	47
Syntax	47
Description	47
Examples	47
gateway sslcert print	47
Syntax	47
Description	47
Examples	48
gateway sslkey	48
Syntax	48
Description	48
Examples	48
gateway sslkey import	49
Syntax	49
Description	49
Examples	50
gateway sslkey export	50
Syntax	50
Description	50
Examples	51
gateway cert export	51
Syntax	51

Description	51
Examples	51
gateway key import	52
Syntax	52
Description	52
Examples	53
gateway setup	53
Syntax	53
Description	53
Examples	54
gateway uninstall	54
Syntax	54
Description	54
Examples	54
The tarantella gateway Command	54
Syntax	55
Description	55
Examples	55
tarantella gateway add	56
Syntax	56
Description	56
Examples	56
tarantella gateway list	57
Syntax	57
Description	57
Examples	57
tarantella gateway remove	57
Syntax	57

Description	57
Examples	58
The <code>--security-gateway</code> Attribute	58
C. Advanced Configuration	61
Tuning the SGD Gateway	61
Changing the Maximum Number of AIP Connections	62
Calculating the Number of AIP Connections	62
Changing the Maximum Number of HTTP Connections	63
Changing the JVM Memory Size	63
Calculating the JVM Memory Size	64
Configuring HTTP Redirection	64
Changing the Binding Port for the SGD Gateway	65
Enabling the Balancer Manager Application	65
Using Unencrypted Connections to the SGD Array	66
Using Unencrypted Incoming Connections to the SGD Gateway	67
The Reflection Service	67
Enabling the Reflection Service	68
▼ How to Enable Unauthorized Access to the Reflection Service	68
▼ How to Enable Authorized Access to the Reflection Service	69
Using the Reflection Service	71
About the RESTful Web Services	72
Examples of Using the Reflection Service	73
D. Troubleshooting the SGD Gateway	75
Logging and Diagnostics	75
About SGD Gateway Logging	75
Changing the Logging Level	76
Log File Locations	76

Displaying SGD Gateway Process Information	77
Checking the Configuration From the Command Line	77
SGD Gateway Error Messages	78

Preface

The *Sun Secure Global Desktop 4.5 Gateway Administration Guide* provides instructions for installing, configuring, and operating the Sun Secure Global Desktop Gateway (SGD Gateway). The document is written for system administrators.

How This Book Is Organized

[Chapter 1](#) describes how to install the SGD Gateway.

[Chapter 2](#) describes how to configure the SGD Gateway for your network.

[Appendix A](#) describes the architecture of the SGD Gateway.

[Appendix B](#) describes how to configure and control the SGD Gateway from the command line.

[Appendix C](#) covers advanced configuration of the SGD Gateway, including how to configure and use the reflection service of the SGD Gateway.

[Appendix D](#) includes troubleshooting information, to help you to diagnose and fix problems with the SGD Gateway.

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, which is at
<http://docs.sun.com>

This document does, however, contain information about specific SGD commands.

Shell Prompts

Shell	Prompt
C shell	<i>machine-name%</i>
C shell superuser	<i>machine-name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Typographic Conventions

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

Note – Characters display differently depending on browser settings. If characters do not display correctly, change the character encoding in your browser to Unicode UTF-8.

Related Documentation

The following table lists the documentation for this product. The online documentation is available at:

<http://docs.sun.com/app/docs/coll/1706.4>

Application	Title	Part Number	Format	Location
Release Notes	<i>Sun Secure Global Desktop 4.5 Release Notes</i>	820-6687-10	HTML PDF	Online Software CD and online
Installation	<i>Sun Secure Global Desktop 4.5 Installation Guide</i>	820-6688-10	HTML PDF	Online Software CD and online
Administration	<i>Sun Secure Global Desktop 4.5 Administration Guide</i>	820-6689-10	HTML PDF	Online
User	<i>Sun Secure Global Desktop 4.5 User Guide</i>	820-6690-10	HTML PDF	Online

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

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:

docfeedback@sun.com

Please include the following document title and part number in the subject line of your email:

Sun Secure Global Desktop 4.5 Gateway Administration Guide, part number 820-6691-10.

Installing the SGD Gateway

Following a brief introduction to the SGD Gateway, this chapter describes how to install the SGD Gateway software. The chapter also includes details of system requirements for the SGD Gateway.

This chapter includes the following topics:

- “About the SGD Gateway” on page 1
- “System Requirements” on page 2
- “Performing the Installation” on page 3

About the SGD Gateway

The SGD Gateway is a proxy server designed to be deployed in front of an SGD array in a demilitarized zone (DMZ). This enables the SGD array to be located on the internal network of an organization. Additionally, all connections can be authenticated in the DMZ before any connections are made to the SGD servers in the array.

Using the SGD Gateway is an alternative to running your SGD servers with firewall traversal, also called firewall forwarding.

The SGD Gateway manages load balancing of Hypertext Transfer Protocol (HTTP) connections, so you do not need to use the JavaServer Pages™ (JSP™) technology load balancing page included with SGD.

System Requirements

The supported installation platforms for the *SGD Gateway host* are shown in the following table.

Operating System	Supported Versions
Solaris™ Operating System (Solaris OS) on SPARC platforms	10
Solaris OS on x86 platforms	10
OpenSolaris on x86 platforms	Latest version
Red Hat Enterprise Linux (Intel x86 32-bit)	5
SUSE Linux Enterprise Server (Intel x86 32-bit)	10

The following requirements apply for the *SGD servers* used with the SGD Gateway:

- **Secure mode.** The SGD servers used with the SGD Gateway must be running in secure mode. Firewall traversal is not supported, so you cannot use the `tarantella security enable` command to configure secure mode automatically.

See “Setting Up Secure Client Connections (Manual Configuration)” in Chapter 1 of the *Sun Secure Global Desktop 4.5 Administration Guide* for details of how to secure an SGD server.

Firewall traversal is covered in “Using Firewall Traversal” in Chapter 1 of the *Sun Secure Global Desktop 4.5 Administration Guide*.

- **Integrated mode.** SGD Clients must not be configured to access the SGD servers in Integrated mode.
- **SGD version.** The SGD servers must be running version 4.50 of SGD.
- **Clock synchronization.** It is important that the system clocks on the SGD servers and the SGD Gateway are in synchronization. Use Network Time Protocol (NTP) software, or the `rdate` command, to ensure that the clocks are synchronized.

For more information on SGD server system requirements, see the *Sun Secure Global Desktop 4.5 Installation Guide*.

Known Issues

See the *Sun Secure Global Desktop 4.5 Release Notes* for details of the known issues with this release of the SGD Gateway.

Performing the Installation

On Solaris OS platforms, install the SGD Gateway with the `pkgadd` command.

On Linux platforms, install the SGD Gateway with the `rpm` command.

By default, SGD is installed in the `/opt/SUNWsgdg` directory. You can change the installation directory, as follows:

- **Solaris OS platforms** – The installation program asks you for the installation directory when you install the software
- **Linux platforms** – You can choose a different installation directory, by using the `--prefix` option with the `rpm` command when you install the software

▼ How To Install the SGD Gateway

1. Save the SGD Gateway package to a temporary directory on the host.

If you are installing from the CD-ROM, the package is in the `gateway` directory.

Alternatively, download the installation program from an SGD web server at `http://server.example.com`, where `server.example.com` is the name of an SGD server. When the SGD web server Welcome Page is displayed, click Install the Sun Secure Global Desktop Gateway.

These are the package files:

- `SUNWsgdg-version.sol-x86.pkg` for Solaris OS on x86 platforms
- `SUNWsgdg-version.sol-sparc.pkg` for Solaris OS on SPARC technology platforms
- `SUNWsgdg-version.i386.rpm` on Linux platforms

where `version` is the SGD Gateway version number.

2. Log in as superuser (root) on the host.

3. Install the SGD Gateway.

If the package file is compressed, you must expand it before installing.

To install on Solaris OS on x86 platforms:

```
# pkgadd -d /tmpdir/SUNWsgdg-version.sol-x86.pkg
```

To install on Solaris OS on SPARC technology platforms:

```
# pkgadd -d /tmpdir/SUNWsgdg-version.sol-sparc.pkg
```

Note – On Solaris OS platforms, if the installation fails with a `pwd: cannot determine current directory!` error message, change to the `/tmpdir` directory and try again.

To install on Linux platforms:

```
# rpm -Uvh /tmpdir/SUNWsgdg-version.i386.rpm
```

4. Verify that the SGD Gateway package is registered in the package database.

On Solaris OS platforms:

```
# pkginfo -x SUNWsgdg
```

On Linux platforms:

```
# rpm -qa | grep -i SUNWsgdg
```

5. Run the SGD Gateway setup program.

```
# /opt/SUNWsgdg/bin/gateway setup
```

The SGD Gateway setup program presents the following settings that you can accept or change:

- **SGD Gateway port settings.** The interface and port used by the SGD Gateway for incoming connections. By default, the SGD Gateway listens on port 443 on all interfaces.
- **Network entry point.** The Internet Protocol (IP) address, or Domain Name System (DNS) name, and the port that client devices use to connect to the SGD Gateway. This is not always the same as the address of the SGD Gateway. Depending on the configuration of your network, this can be the address of a load balancer or other external device.

For example, if users connect directly to an SGD Gateway at `gateway1.example.com`, type `gateway1.example.com:443` for the network entry point.

If users connect to the SGD Gateway through a load balancer at `lb.example.com`, type `lb.example.com:443` for the network entry point.

- **Secure connections.** Whether to secure the connections between the SGD Gateway and the SGD servers in the array. By default, the SGD Gateway uses secure connections. To use secure connections, the SGD servers in the array must be running in secure mode.

Note – These settings can be changed later, by using the `gateway config create` command. See [“How to Configure the Ports and Connections for the SGD Gateway”](#) on page 12.

After installing the software, you must perform additional configuration of the SGD Gateway. See [Chapter 2](#) for details of what you need to do.

Configuring the SGD Gateway

This chapter describes how to configure the SGD Gateway for typical deployment scenarios. How to start and stop the SGD Gateway is also covered in this chapter, along with instructions on how to remove the SGD Gateway software.

This chapter includes the following topics:

- [“Deploying the SGD Gateway” on page 7](#)
- [“SGD Gateway Configuration Tasks” on page 12](#)
- [“Controlling the SGD Gateway” on page 18](#)
- [“Removing the SGD Gateway” on page 19](#)

Deploying the SGD Gateway

This section describes the following SGD Gateway deployment scenarios:

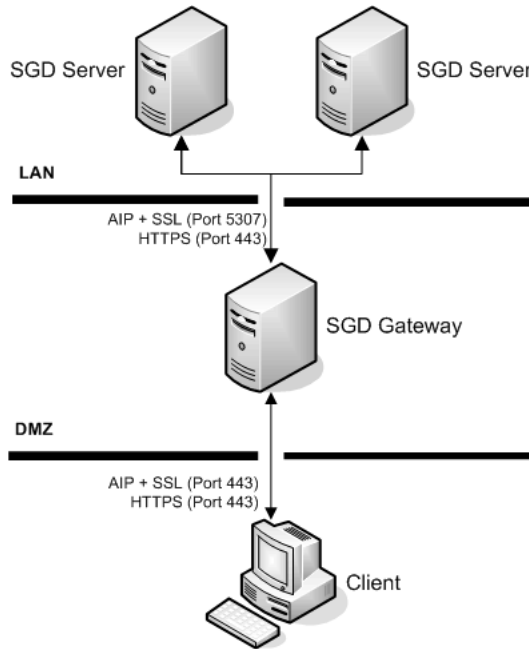
- [“Basic Deployment” on page 7](#)
- [“Load-Balanced Deployment” on page 9](#)

Basic Deployment

This section describes the configuration tasks for a basic deployment of the SGD Gateway.

A basic deployment uses a single SGD Gateway, as shown in [FIGURE 2-1](#).

FIGURE 2-1 Basic Deployment Using a Single SGD Gateway



Configuring a basic deployment involves configuring the connections shown in TABLE 2-1.

TABLE 2-1 Connections For a Basic Deployment of the SGD Gateway

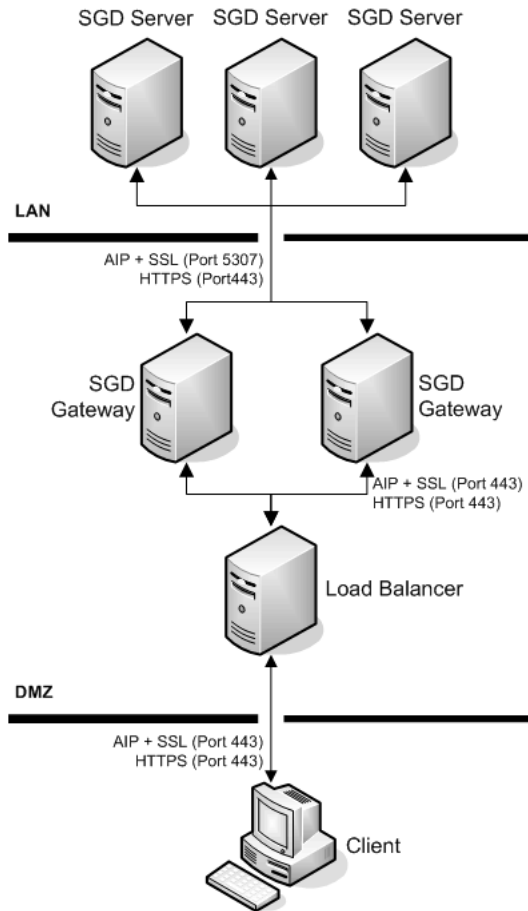
Connection	Configuration Steps
Client device to SGD Gateway	<ol style="list-style-type: none">1. Configure the ports and connections used by the SGD Gateway. You configured these settings when you installed the SGD Gateway. See “How to Configure the Ports and Connections for the SGD Gateway” on page 12 if you want to change the configuration of the SGD Gateway.2. On the SGD Gateway, install a Secure Sockets Layer (SSL) certificate for client connections. See “How to Install an SSL Certificate for Client Connections Into the Client Keystore” on page 13.
SGD Gateway to SGD servers	<ol style="list-style-type: none">1. Enable SGD security services for the array. The SGD servers must be running in secure mode. Firewall traversal is not supported. See “Setting Up Secure Client Connections (Manual Configuration)” in Chapter 1 of the <i>Sun Secure Global Desktop 4.5 Administration Guide</i> for details of how to do this.2. On the SGD Gateway, install security certificates for the SGD servers. Use the <code>gateway server</code> command to import CA certificates and SSL certificates for the SGD servers in the array into the SGD Gateway keystore. See “How to Install SGD Server Certificates” on page 14.3. Set up the SGD servers in the array to use the SGD Gateway. Install the SGD Gateway certificate on the SGD array, and use the <code>tarantella gateway add</code> command to register the SGD Gateway with the SGD array. See “How to Install SGD Gateway Certificates on the SGD Array” on page 16.4. Configure which SGD Client connections can use the SGD Gateway. See “How to Configure SGD Client Connections” on page 17.

Load-Balanced Deployment

This section describes the configuration tasks for a load-balanced deployment of SGD Gateway.

A load-balanced deployment uses multiple SGD Gateways and a load balancer as the network entry point, as shown in [FIGURE 2-2](#).

FIGURE 2-2 Network Deployment Using Multiple SGD Gateways and a Load Balancer



Configuring a load-balanced deployment involves configuring the connections shown in [TABLE 2-1](#).

TABLE 2-2 Connections For a Load-Balanced Deployment of the SGD Gateway

Connection	Configuration tasks
Client device to load balancer	<ol style="list-style-type: none"> <li data-bbox="511 335 1326 421">1. Enable incoming connections from client devices. Typically, this uses Transmission Control Protocol (TCP) port 443. See your load balancer documentation for details of how to do this. <li data-bbox="511 421 1326 508">2. (Optional) On the load balancer, install the SSL certificate used by the SGD Gateways for client connections. See your load balancer documentation for details of how to do this.
Load balancer to SGD Gateway	<ol style="list-style-type: none"> <li data-bbox="511 526 1326 578">1. Configure your load balancer to forward connections to the SGD Gateway. See your load balancer documentation for details of how to do this. <li data-bbox="511 578 1326 734">2. Configure the ports and connections used by the SGD Gateway. Set the network entry point to the address of the load balancer. You configured these settings when you installed the SGD Gateway. See “How to Configure the Ports and Connections for the SGD Gateway” on page 12 if you want to change the configuration of the SGD Gateway. <li data-bbox="511 734 1326 821">3. On each SGD Gateway, install an SSL certificate for client connections. See “How to Install an SSL Certificate for Client Connections Into the Client Keystore” on page 13.
SGD Gateway to SGD servers	<ol style="list-style-type: none"> <li data-bbox="511 838 1326 994">1. Enable SGD security services for the SGD array. The SGD servers must be running in secure mode. Firewall traversal is not supported. See “Setting Up Secure Client Connections (Manual Configuration)” in Chapter 1 of the <i>Sun Secure Global Desktop 4.5 Administration Guide</i> for details of how to do this. <li data-bbox="511 994 1326 1116">2. On the SGD Gateway, install security certificates for the SGD servers. Use the <code>gateway server</code> command to import CA certificates and SSL certificates for the SGD servers in the array into the SGD Gateway keystore. See “How to Install SGD Server Certificates” on page 14. <li data-bbox="511 1116 1326 1289">3. Set up the SGD servers in the array to use the SGD Gateways. Install SGD Gateway certificates on the SGD array, and use the <code>tarantella gateway add</code> command to register the SGD Gateways with the SGD array. See “How to Install SGD Gateway Certificates on the SGD Array” on page 16. <li data-bbox="511 1289 1326 1359">4. Configure which SGD Client connections can use the SGD Gateways. See “How to Configure SGD Client Connections” on page 17.

SGD Gateway Configuration Tasks

This section includes instructions for configuring the connections used by the SGD Gateway.

The following configuration tasks are described:

- [“Client Device to SGD Gateway Connections”](#) on page 12
- [“SGD Gateway to SGD Server Connections”](#) on page 14
- [“Client Device to Load Balancer Connections”](#) on page 17
- [“Load Balancer to SGD Gateway Connections”](#) on page 17

Client Device to SGD Gateway Connections

Configuring connections between the client device and an SGD Gateway involves the following configuration tasks:

1. (Optional) Configure the ports and connections used by the SGD Gateway.
You configure these settings when you install the SGD Gateway.
To change these settings, see [“How to Configure the Ports and Connections for the SGD Gateway”](#) on page 12.
2. (Optional) On the SGD Gateway, install an SSL certificate for client connections.
See [“How to Install an SSL Certificate for Client Connections Into the Client Keystore”](#) on page 13.

▼ How to Configure the Ports and Connections for the SGD Gateway

You only need to use this procedure if you want to change the settings you made during installation of the SGD Gateway.

1. **Log in as superuser (root) on the SGD Gateway host.**
2. **Run the `gateway config create` command.**

```
# /opt/SUNWsgdg/bin/gateway config create
```

Answer the on-screen questions, to configure the following:

- **SGD Gateway port settings.** The interface and port used by the SGD Gateway for incoming connections.
- **Network entry point.** The Internet Protocol (IP) address, or Domain Name System (DNS) name, and port that client devices use to connect to the SGD Gateway. This is not always the same as the address of the SGD Gateway. Depending on the configuration of your network, this can be the address of a load balancer or other external device.
- **Secure connections.** Whether to secure the connections between the SGD Gateway and the SGD servers in the array. To use secure connections, the SGD servers in the array must be running in secure mode.

3. Save the connection and port settings.

The SGD Gateway is configured using the settings you entered.

▼ How to Install an SSL Certificate for Client Connections Into the Client Keystore

The SSL certificate that the SGD Gateway uses for client connections is called the SGD Gateway SSL certificate. The SSL certificate is stored in the client keystore, `/opt/SUNWsgdg/proxy/etc/keystore.client`.

By default, the SGD Gateway uses a *self-signed* SGD Gateway SSL certificate for client connections, but you can replace the self-signed SSL certificate with a certificate signed by a certificate authority (CA).

The following procedure assumes you have an SSL certificate signed by a CA.

The private key you install must be in Privacy Enhanced Mail (PEM) format.

1. Log in as superuser (root) on the SGD Gateway host.
2. Copy the SSL certificate and the corresponding private key to the SGD Gateway host.
3. Import the SSL certificate and private key into the client keystore.

Use the `gateway sslkey import` command, as follows:

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile temp.key \
--keyalg RSA \
--certfile example.com.pem
```

Here, the certificate file `example.com.pem` and the corresponding RSA-encoded private key, `temp.key`, are imported into the client keystore.

The existing self-signed SSL certificate in the client keystore is overwritten.

4. (Optional) Restart the SGD Gateway.



Caution – Only use this step if you are not performing initial configuration of the SGD Gateway. Restarting the SGD Gateway at this stage during initial configuration displays an error message, because initial configuration of the SGD Gateway has not been completed.

Restart the SGD Gateway if you are replacing the SSL certificate on an SGD Gateway that is already configured and running.

Note – Restarting the SGD Gateway disconnects all user sessions and application sessions that are running through the SGD Gateway.

On the SGD Gateway host, run the following command:

```
# /opt/SUNWsgdg/bin/gateway restart
```

SGD Gateway to SGD Server Connections

The connections between an SGD Gateway and the SGD servers in the array use certificates for mutual authorization. Configuring these connections involves the following configuration tasks:

1. Install SGD server certificates on the SGD Gateway.
See [“How to Install SGD Server Certificates”](#) on page 14.
2. Install the SGD Gateway certificate on the SGD array.
See [“How to Install SGD Gateway Certificates on the SGD Array”](#) on page 16.
3. Configure SGD Client connections for the SGD Gateway.
See [“How to Configure SGD Client Connections”](#) on page 17.

▼ How to Install SGD Server Certificates

To use this procedure, the SGD servers in the array must be running in secure mode.

Note – Do not use the `tarantella security enable` command to configure secure connections automatically for the SGD servers in this array. This command turns on firewall forwarding, which is not supported by the SGD Gateway. Instead, configure secure connections manually using the `tarantella security start` command.

See “Setting Up Secure Client Connections (Manual Configuration)” in Chapter 1 of the *Sun Secure Global Desktop 4.5 Administration Guide* for more information about how to enable security services on an SGD server.

Repeat the following procedure for each SGD server in the array.

1. Log in as superuser (root) on the SGD host.

2. Copy the CA certificate from the SGD server to the SGD Gateway keystore directory.

The CA certificate for an SGD server is at
`/opt/tarantella/var/info/certs/PeerCAcert.pem` on the SGD host.

Note – This is the same CA certificate that the SGD server uses for secure intra-array communication.

The SGD Gateway keystore directory is `/opt/SUNWsgdg/proxy/etc`.

3. Copy the SSL certificate from the SGD server to the SGD Gateway keystore directory.

The SSL certificate for an SGD server running in secure mode is at
`/opt/tarantella/var/tsp/cert.pem` on the SGD host.

The SGD Gateway keystore directory is `/opt/SUNWsgdg/proxy/etc`.

4. Log in as superuser (root) on the SGD Gateway host.

5. Import the certificates into the SGD Gateway keystore.

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd-server1 \  
--certfile /opt/SUNWsgdg/proxy/etc/PeerCAcert.pem --url https://sgd1.example.com \  
--ssl-certfile /opt/SUNWsgdg/proxy/etc/cert.pem
```

The `--server` option defines the alias names used when storing the certificates in the keystore. In this example, the CA certificate is stored using an alias of `sgd-server1`, the SSL certificate is stored using an alias of `sgd-server1-ssl`.

`https://sgd1.example.com` is the Uniform Resource Locator (URL) of the SGD web server.

6. Restart the SGD Gateway.

Note – Restarting the SGD Gateway disconnects all user sessions and application sessions that are running through the SGD Gateway.

On the SGD Gateway host, run the following command:

```
# /opt/SUNWsgdg/bin/gateway restart
```

▼ How to Install SGD Gateway Certificates on the SGD Array

Repeat the following procedure for each SGD Gateway.

1. Export the SGD Gateway certificate.

- a. Log in as superuser (root) on the SGD Gateway host.
- b. Export the SGD Gateway certificate from the SGD Gateway keystore.

Use the `gateway cert export` command, as follows:

```
# /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
```

The certificate is exported to the file `gateway1.pem`.

- c. Copy the certificate to the `/opt/tarantella/var/tsp` directory on the primary SGD server in the array.

2. Register the SGD Gateway with the SGD array.

- a. On the primary SGD server, log in as superuser (root).
- b. Import the SGD Gateway certificate.

```
$ tarantella gateway add --name sgd-gateway1 \  
--certfile /opt/tarantella/var/tsp/gateway1.pem
```

where `sgd-gateway1` is a name used by SGD to identify the SGD Gateway, and `gateway1.pem` is the SGD Gateway certificate file name.

To register multiple SGD Gateways at the same time, use the `--file` option of the `tarantella gateway add` command. See [“The tarantella gateway Command” on page 54](#) for more details.

Configuration changes made using `tarantella gateway add` are replicated to the other SGD servers in the array.

▼ How to Configure SGD Client Connections

- **Configure the SGD Client connections that use the SGD Gateway.**

On the primary SGD server, set the `--security-gateway` global attribute to define which SGD Clients can use the SGD Gateway, based on their IP address or DNS name.

To specify that all SGD Client connections are routed through TCP port 443 of a single SGD Gateway `gateway1.example.com`, use the following command:

```
$ tarantella config edit --security-gateway \  
"*:sgdg:gateway1.example.com:443"
```

To specify that all SGD Client connections are routed through TCP port 443 of an external load balancer `lb.example.com`, use the following command:

```
$ tarantella config edit --security-gateway \  
"*:sgdg:lb.example.com:443"
```

Note – Changes to the `--security-gateway` attribute affect all SGD servers in the array. The changes only apply to new user sessions.

See [“The `--security-gateway` Attribute” on page 58](#) for more details about how to use the `--security-gateway` attribute to define multiple SGD Client connection filters.

Client Device to Load Balancer Connections

Configuring connections between the client device and an external load balancer involves the following configuration tasks:

1. Configure the load balancer to accept connections from client devices.
See your load balancer documentation for details of how to do this.
2. (Optional) Install the SSL certificate for the SGD Gateway on to the load balancer.
See your load balancer documentation for details of how to do this.

Load Balancer to SGD Gateway Connections

Configuring connections between an external load balancer and the SGD Gateway involves the following configuration tasks:

1. Configure the ports and connections used by the SGD Gateway.
See “How to Configure the Ports and Connections for the SGD Gateway” on page 12.
2. (Optional) On the SGD Gateway, install an SSL certificate for incoming client connections.
See “How to Install an SSL Certificate for Client Connections Into the Client Keystore” on page 13.

Controlling the SGD Gateway

This section describes how to control the SGD Gateway. The following tasks are described:

- Starting the SGD Gateway
- Stopping the SGD Gateway
- Restarting the SGD Gateway

Starting the SGD Gateway

To start the SGD Gateway, use the following command:

```
# /opt/SUNWsgdg/bin/gateway start
```

Stopping the SGD Gateway



Caution – Stopping the SGD Gateway disconnects all user sessions and application sessions that are running through the SGD Gateway. This means that application data can be lost if the SGD Gateway is stopped unexpectedly.

To stop the SGD Gateway, use the following command:

```
# /opt/SUNWsgdg/bin/gateway stop
```

When you use the `gateway stop` command a warning message is displayed, prompting you to confirm that you want to stop the SGD Gateway. Use the `--force` option of the `gateway stop` command if you do not want to display this message.

Note – If the SGD Gateway is stopped, users from outside your network cannot connect to SGD using the SGD Gateway. Client devices that have been enabled using the `--security-gateway` attribute to access SGD directly without going through the SGD Gateway, can still access SGD. See [“The `--security-gateway` Attribute” on page 58](#).

Restarting the SGD Gateway



Caution – Restarting the SGD Gateway disconnects all user sessions and application sessions that are running through the SGD Gateway. This means that application data can be lost if the SGD Gateway is restarted unexpectedly.

To restart the SGD Gateway, use the following command:

```
# /opt/SUNWsgdg/bin/gateway restart
```

When you use the `gateway restart` command a warning message is displayed, prompting you to confirm that you want to stop the SGD Gateway. Use the `--force` option of the `gateway restart` command if you do not want to display this message.

Removing the SGD Gateway

To remove the SGD Gateway, you remove the software installed on the SGD Gateway host.

▼ How To Remove the SGD Gateway

1. Log in as superuser (root) on the SGD Gateway host.
2. Change the SGD Client routing configuration for the SGD array.
 - a. Log in as superuser (root) on the primary SGD server.

b. Edit the `--security-gateway` attribute for the SGD array.

For a basic deployment using a single SGD Gateway, run the following command:

```
# tarantella config edit --security-gateway ""
```

Note – For a load-balanced deployment using multiple SGD Gateways and an external load balancer, you do not need to edit the `--security gateway` attribute.

3. Uninstall the SGD Gateway.

Run the following command:

```
# /opt/SUNWsgdg/bin/gateway uninstall
```

A warning message is displayed, prompting you to confirm that you want to stop the SGD Gateway.



Caution – The `gateway uninstall` command is the only supported method of removing the SGD Gateway. Do not use the `pkgrm` or `rpm` commands directly to remove the SGD Gateway.

4. (Optional) Remove the SGD Gateway from the list of SGD Gateways registered for the SGD array.

a. Display the SGD Gateways registered for the SGD array.

```
# tarantella gateway list
Installed gateway: gateway1.example.com
Issuer: CN=gateway1.example.com, OU=Marketing, O=Example, L=Boston, ST=
Massachusetts, C=US
Serial Number: 1208509056
Subject: CN=gateway2.example.com, OU=Marketing, O=Example, L=Boston, ST=
Massachusetts, C=US
Valid from Fri Sep 26 09:57:36 GMT 2008 to Thu Dec 25 09:57:36 GMT 2008
```

b. Remove the SGD Gateway from the list of SGD Gateways registered for the SGD array.

```
# tarantella gateway remove --name gateway1.example.com
```

SGD Gateway Architecture Overview

This chapter describes the architecture and the main components of the SGD Gateway.

This chapter includes the following topics:

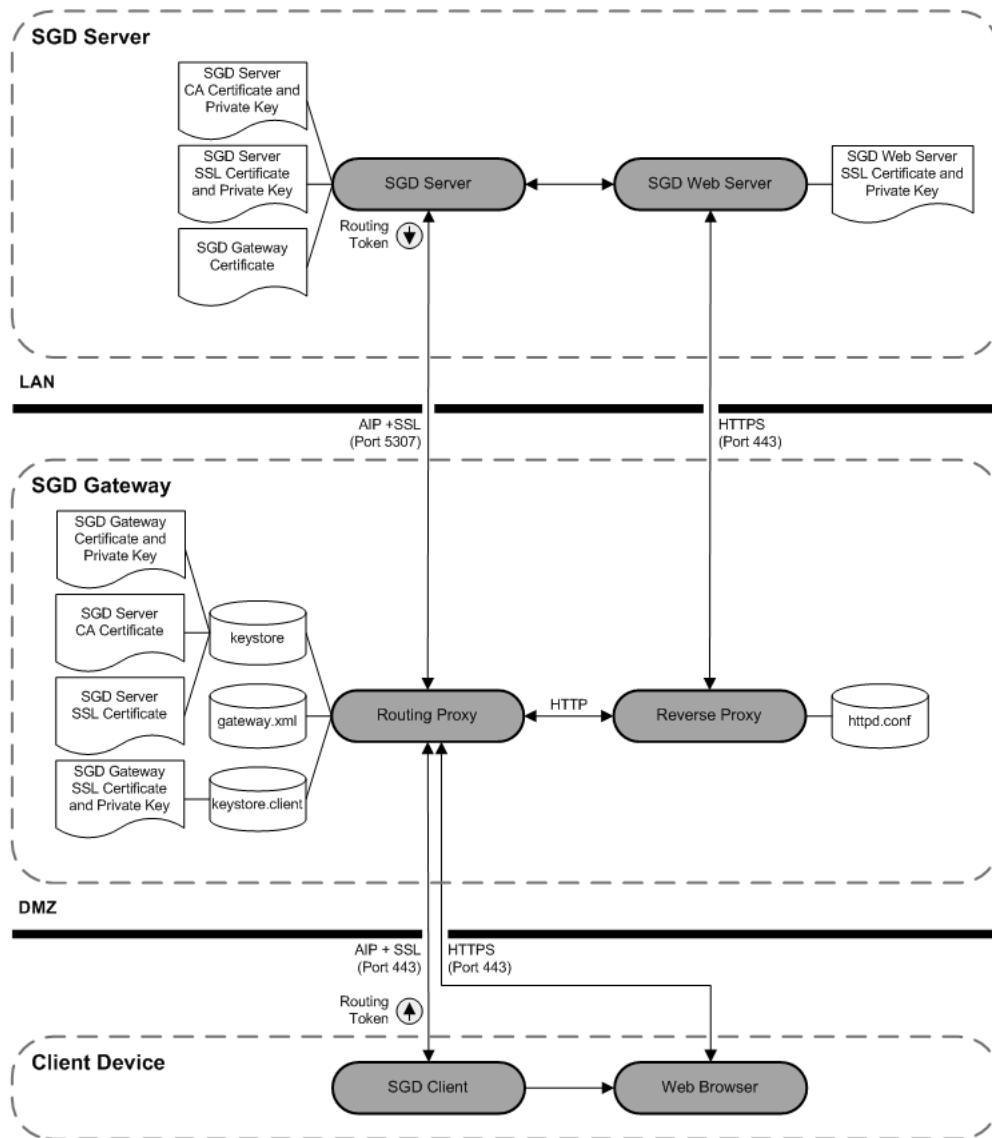
- [“SGD Gateway Architecture”](#) on page 21
- [“Components of the SGD Gateway”](#) on page 25
- [“Supported Cipher Suites”](#) on page 29

SGD Gateway Architecture

This section looks at the architecture of the SGD Gateway and includes a description of the connections made when you run SGD through the SGD Gateway.

[FIGURE A-1](#) shows the architecture of the SGD Gateway.

FIGURE A-1 SGD Gateway Architecture



The following steps describe the connections made when you access SGD through the SGD Gateway. The steps cover the initial connection to SGD using a browser, logging on to SGD, through to starting an application.

1. A browser on the client device makes an Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) connection to the SGD Gateway, on Transmission Control Protocol (TCP) port 443.

- For a basic deployment, users can access SGD by going to the Uniform Resource Locator (URL) of the SGD Gateway.
 - TCP port 443 is the default port for the SGD Gateway. The ports used by the SGD Gateway are defined using the routing proxy configuration file, `gateway.xml`. This file is created automatically during installation of the SGD Gateway, and is updated when the `gateway config` command is used to change the SGD Gateway configuration.
 - The SGD Gateway presents an SSL certificate. This certificate is the only entry in the `keystore.client` keystore on the SGD Gateway.
 - The location and passwords for the keystores used by the SGD Gateway are defined in the routing proxy configuration file, `gateway.xml`.
2. The routing proxy recognizes an HTTPS connection, decrypts the data stream, and forwards HTTP data to the Apache reverse proxy.
 - Hypertext Transfer Protocol (HTTP) data is sent internally on the first free port above TCP port 8080.
 - The configuration for the Apache reverse proxy is defined by the `httpd.conf` file. This file and related reverse proxy configuration files are created automatically during installation of the SGD Gateway. The files are updated when the `gateway config` command is used to change the SGD Gateway configuration.
 3. The reverse proxy uses HTTP load balancing to select an SGD web server in the array.
 - Connections between the reverse proxy and the SGD web server are secure, using HTTPS on TCP port 443.
 - The Apache reverse proxy sets a load balancing cookie in the browser. All subsequent HTTP requests by the browser use the same SGD web server.
 4. The SGD web server delivers HTML to the browser on the client device.
 - The HTML is sent as HTTPS data on the connection established to TCP port 443 on the SGD Gateway.
 - The SGD Gateway forwards the HTTPS data to the browser.
 5. The user logs in to SGD.
 - The SGD server authenticates the user, selects an SGD server to manage the user session, and starts a new user session.
 - The SGD Client is downloaded, installed, and started on the client device.
 - A routing token is included in HTML sent to the browser. The routing token contains the address of the SGD server selected to manage the user session. This information is used to route Adaptive Internet Protocol (AIP) data to the correct SGD server.

- The routing token is signed using the private key of the SGD server, and then encrypted using the SGD Gateway certificate on the SGD server.
 - The routing token is passed to the SGD Client.
 - Connections to the client device use HTTPS.
6. The SGD Client connects to the SGD Gateway on TCP port 443.
- The data connection between the SGD Client and the SGD Gateway uses AIP over Secure Sockets Layer (SSL).
 - The SSL certificate for the SGD Gateway is presented for the connection.
 - The routing proxy recognizes incoming AIP over SSL data.
 - The SSL data stream is decrypted, and the routing token is extracted from the AIP data stream.
 - The routing token is decrypted, using the SGD Gateway private key and then verified, using the CA certificate for the SGD server.
 - The SGD Gateway private key and the CA certificate for the SGD server are stored in the SGD Gateway keystore, *keystore*.
 - The time stamp on the routing token is checked, to ensure the routing token is valid.
 - The AIP data stream is re-encrypted using SSL.
7. AIP over SSL data is routed through the routing proxy to the SGD server indicated by the routing token.
- The AIP over SSL data connection uses TCP port 5307.
 - The routing token is not included with the AIP data stream.
8. The user starts an application on the SGD webtop.
- The application launch request is sent to the SGD Gateway using HTTPS.
 - The routing proxy recognises and decrypts HTTPS data, and forwards HTTP traffic to the Apache reverse proxy.
 - The reverse proxy detects the load balancing cookie and uses the SGD web server indicated by the cookie.
 - SGD application session load balancing selects the same SGD server to manage the application session.
 - A new routing token is created on the SGD server. The routing token is used to route AIP data to the SGD server selected to manage the application session.
 - The SGD server sends the routing token to the SGD Client. The routing token is included with the existing AIP data stream.
9. The SGD Client connects to the SGD Gateway on TCP port 443.
- The SSL certificate for the SGD Gateway is presented for the connection.
 - The routing proxy recognizes incoming AIP over SSL data.

- The routing token is decrypted, verified, and validated.
 - AIP over SSL data is routed through the routing proxy to the SGD server indicated by the routing token.
 - The routing token is not included with the AIP data stream.
10. The SGD server manages the application session.
- The application runs on an application server located on the local area network (LAN).

Components of the SGD Gateway

The SGD Gateway consists of the following components:

- **Routing proxy.** A Java™ technology-based application that routes AIP data connections to an SGD server.

The main components of the routing proxy are:

- Routing tokens – See [“About Routing Tokens” on page 25](#)
- Keystores – See [“Keystores Used By the SGD Gateway” on page 26](#)
- Routing proxy configuration file – See [“Routing Proxy Configuration File” on page 27](#)
- **Reverse proxy.** An Apache web server, configured to operate in reverse proxy mode. The reverse proxy also performs load balancing of HTTP connections.

The main components of the reverse proxy are:

- Configuration files for the Apache web server – See [“Apache Web Server Configuration Files” on page 27](#)
- Apache modules for reverse proxying and HTTP load balancing – See [“Apache Modules Used by the SGD Gateway” on page 28](#)

About Routing Tokens

The SGD Gateway uses a *routing token* to manage an AIP connection. A routing token is a signed, encrypted message which identifies the origin and destination SGD server for a route. The routing token includes a time stamp, which is used to limit the token lifetime.

Outgoing routing tokens are:

- Signed on the SGD server, using the private key for the SGD server.

- Encrypted on the SGD server, using the SGD Gateway certificate.
- Sent to the SGD Client on the client device.

Incoming routing tokens are:

- Decrypted on the SGD Gateway, using the SGD Gateway private key.
- Verified on the SGD Gateway, using the CA certificate for the origin SGD server.
- Discarded on the SGD Gateway. The connection presenting the routing token is routed to the destination SGD server.

Keystores Used By the SGD Gateway

The SGD Gateway uses private keys and certificates to digitally sign and verify routing tokens, to secure connections to the SGD servers in the array, to secure client connections to the SGD Gateway, and to authorize access to the reflection service.

The certificates and private keys used by the SGD Gateway are stored in keystores in the `/opt/SUNWsgdg/proxy/etc` directory.

This directory contains the following keystores:

- **SGD Gateway keystore.** The SGD Gateway keystore, `keystore`, contains the SGD Gateway certificate and private key, CA certificates for the SGD servers in the array, and SGD server SSL certificates for secure connections to the SGD servers in the array.

To add, remove, and list entries for the SGD Gateway keystore, use the `gateway` command.

- **Client keystore.** The client keystore, `keystore.client`, contains a single SGD Gateway SSL certificate and private key used for securing connections between the client device and the SGD Gateway. By default, this keystore contains a self-signed certificate. You can replace this certificate with a certificate signed by a Certificate Authority (CA).
- **Reflection service keystore.** The reflection service keystore, `keystore.reflection`, contains a certificate and private key used to authorize access to the reflection service on the SGD Gateway. By default, this keystore contains a self-signed certificate and private key.

The keystores are created automatically when you run the `gateway setup` command after installing the SGD Gateway.

Note – All keystores use the same password, which is defined in the `/opt/SUNWsgdg/etc/password` file. The password is a random password created automatically when the keystores are first created. The password file is only readable by superuser (root).

Routing Proxy Configuration File

The routing proxy configuration file is `/opt/SUNWsgdg/etc/gateway.xml`. This is an XML file that configures routes, depending on the data protocol type. The file also configures the keystore locations and passwords required for routing and SSL protocols.

The routing proxy configuration file is created automatically when you install the SGD Gateway and is updated when you use the `gateway config` commands to change the configuration of the SGD Gateway.



Caution – Do not edit the `gateway.xml` file manually. Incorrect configuration in this file might cause the SGD Gateway to stop working.

The default routing proxy configuration file uses the password in the `/opt/SUNWsgdg/etc/password` file to access the keystores used by the SGD Gateway. If you do not want to store this password on disk, make a note of the entry in the password file. Delete the password file, and delete the `password` entries for all `<keystore>` elements in the `gateway.xml` file. You are then prompted for the keystore password when you next start the SGD Gateway.

To change the password for a keystore used by the SGD Gateway, use the `-storepasswd` option of the `keytool` command. For example, to change the password for the `keystore.client` keystore run the following command:

```
# /opt/SUNWsgdg/java/default/bin/keytool -storepasswd \  
-keystore /opt/SUNWsgdg/proxy/etc/keystore.client
```

Note – The `/opt/SUNWsgdg/etc` directory also contains other `.xml` and `.template` files. These files are used internally by the `gateway config` command to update the `gateway.xml` file. Do not edit these files manually.

Apache Web Server Configuration Files

Configuration files for the Apache web server configured for use with the SGD Gateway are in the `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/conf` directory.

The configuration files in this directory are used to configure reverse proxy operation and load balancing for the Apache web server.

Configuring Reverse Proxying and Load Balancing

Files for configuring reverse proxy operation and load balancing are in the `extra/gateway` subdirectory. These files are enabled by the following `Include` directive in the main `httpd.conf` file:

```
# SGD Reverse Proxy/Load Balance settings
Include conf/extra/gateway/httpd-gateway.conf
```

The `httpd-gateway.conf` file configures reverse proxying and load balancing for the Apache web server. The members of the load balancing group are defined using an `Include` directive in the `httpd-gateway.conf` file, as follows:

```
<Proxy Balancer://mysgdserver/>
Include conf/extra/gateway/servers/*.conf
</Proxy>
```

The `extra/gateway/servers` directory contains configuration files for each of the SGD web servers in the load balancing group. The configuration files are named `server-name.conf`, where `server-name` is the server name used in the gateway `server add` command. See “[gateway server add](#)” on page 42 for more details about this command.

The SGD Gateway uses *sticky session* HTTP load balancing. This means that the Apache reverse proxy sets a cookie in the client browser, to ensure that the browser always returns to the SGD web server that was selected by load balancing. The cookie expires at the end of the user session.

Sticky session cookies are enabled by the `Header add Set-Cookie` directive in the `httpd-gateway.conf` file, as follows:

```
Header add Set-Cookie "BALANCEID=balanceworker. %{BALANCER_WORKER_ROUTE}e; path=
/" env=BALANCER_ROUTE_CHANGED
```

where `BALANCEID` is the name of the cookie, and `BALANCER_WORKER_ROUTE` and `BALANCER_ROUTE_CHANGED` are environment variables exported by the Apache `mod_proxy_balancer` module. See the Apache `mod_proxy_balancer` documentation for more information about these environment variables.

Apache Modules Used by the SGD Gateway

The Apache web server supplied with the SGD Gateway uses the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.

The modules are enabled by `LoadModule` directives in the `httpd.conf` Apache configuration file, at `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/conf/httpd.conf`.

Supported Cipher Suites

The SGD Gateway supports the following cipher suites for secure connections:

- `SSL_RSA_WITH_RC4_128_MD5`
- `SSL_RSA_WITH_RC4_128_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
- `TLS_DHE_RSA_WITH_AES_256_CBC_SHA`
- `TLS_DHE_DSS_WITH_AES_128_CBC_SHA`
- `TLS_DHE_DSS_WITH_AES_256_CBC_SHA`
- `SSL_RSA_WITH_3DES_EDE_CBC_SHA`
- `SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
- `SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA`
- `SSL_RSA_WITH_DES_CBC_SHA`
- `SSL_DHE_RSA_WITH_DES_CBC_SHA`
- `SSL_DHE_DSS_WITH_DES_CBC_SHA`
- `SSL_RSA_EXPORT_WITH_RC4_40_MD5`
- `SSL_RSA_EXPORT_WITH_DES40_CBC_SHA`
- `SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA`
- `SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA`

Command-Line Reference

This chapter describes how you can manage, control, and change the configuration for the SGD Gateway from the command line.

Commands are provided for tasks such as setting up keystores and certificates, configuring the ports used by the SGD Gateway, and configuring load balancing for the SGD servers in the array.

This chapter includes the following topics:

- [“The gateway Command” on page 31](#)
- [“The tarantella gateway Command” on page 54](#)
- [“The --security-gateway Attribute” on page 58](#)

The gateway Command

Use the gateway command to configure and control the SGD Gateway.

Note – The full path of the gateway command is `/opt/SUNWsgdg/bin/gateway`.

Syntax

```
gateway start | stop | restart | config | server | status | setup | version | sslcert  
| sslkey | cert | key | setup | uninstall
```

Description

The available gateway commands are shown in the following table.

Command	Description	More Information
<code>gateway start</code>	Starts the SGD Gateway	“gateway start” on page 33
<code>gateway stop</code>	Stops the SGD Gateway	“gateway stop” on page 33
<code>gateway restart</code>	Stops and then restarts the SGD Gateway	“gateway restart” on page 34
<code>gateway config</code>	Configures the SGD Gateway, and updates the Apache reverse proxy configuration files	“gateway config” on page 34
<code>gateway server</code>	Installs SGD server security certificates and configures load balancing for the SGD array	“gateway server” on page 41
<code>gateway status</code>	Displays the current status for the SGD Gateway	“gateway status” on page 45
<code>gateway version</code>	Displays the version number of the SGD Gateway	“gateway version” on page 45
<code>gateway sslcert</code>	Exports and prints the Secure Sockets Layer (SSL) certificate in the client keystore	“gateway sslcert” on page 46
<code>gateway sslkey</code>	Manages the private key and certificate in the client keystore	“gateway sslkey” on page 48
<code>gateway cert export</code>	Exports the SGD Gateway certificate from the SGD Gateway keystore	“gateway cert export” on page 51
<code>gateway key import</code>	Imports a private key and certificate into the SGD Gateway keystore	“gateway key import” on page 52
<code>gateway setup</code>	Runs the SGD Gateway setup program	“gateway setup” on page 53
<code>gateway uninstall</code>	Uninstalls the SGD Gateway software	“gateway uninstall” on page 54

Note – All gateway commands include a `--help` option. You can use this option to display help for the command.

Examples

The following example starts the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway start
```

The following example means that the SGD server `server.example.com` is not authorized to use the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway server remove --server server.example.com
```

gateway start

Starts the SGD Gateway.

Syntax

```
gateway start
```

Description

Starts the SGD Gateway.

Examples

The following example starts the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway start
SGD Gateway started successfully
```

gateway stop

Stops the SGD Gateway.

Syntax

```
gateway stop [--force]
```

Description

Stops the SGD Gateway, after prompting the user for confirmation.

The `--force` option stops the SGD Gateway, without asking for confirmation.

Examples

The following example stops the SGD Gateway, prompting the user for confirmation.

```
# /opt/SUNWsgdg/bin/gateway stop
```

gateway restart

Stops and then restarts the SGD Gateway.

Syntax

```
gateway restart [--force]
```

Description

Stops and then restarts the SGD Gateway. Before stopping the SGD Gateway, the user is prompted for confirmation.

The `--force` option stops the SGD Gateway, without asking for confirmation.

Examples

The following example stops and restarts the SGD Gateway, prompting the user for confirmation.

```
# /opt/SUNWsgdg/bin/gateway restart
```

gateway config

Configures the SGD Gateway. The `gateway config` command configures secure connections, ports, and reverse proxy server settings for the SGD Gateway.

Syntax

```
gateway config create | show
```

Description

The following table shows the available subcommands for this command.

Subcommand	Description	More Information
create	Creates a new configuration for the SGD Gateway	"gateway config create" on page 35
list	Lists the current configuration for the SGD Gateway	"gateway config list" on page 36
edit	Edits the current configuration for the SGD Gateway	"gateway config edit" on page 38
enable	Enables an SGD Gateway service	"gateway config enable" on page 39
disable	Disables an SGD Gateway service	"gateway config disable" on page 40

Examples

The following example lists the current configuration for the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway config list
```

gateway config create

Creates a new configuration for the SGD Gateway, overwriting the current configuration.

Syntax

```
gateway config create { [ --interface interface:port ]  
                        [ --entry-point ip-address:port ]  
                        [ --out plaintext | ssl ]  
                      } | --file file
```

Description

The following table shows the available options for this command.

Option	Description
<code>--interface</code>	Interface and port that the SGD Gateway listens on for incoming proxy connections. The default is Transmission Control Protocol (TCP) port 443, on all interfaces.
<code>--entry-point</code>	Entry point for the network. This is the Internet Protocol (IP) address, and port that clients use to connect to the SGD Gateway. You can specify a Domain Name System (DNS) address instead of an IP address.
<code>--out</code>	Format of outgoing traffic from the SGD Gateway to the SGD servers in the array. If you are using secure connections, choose <code>ssl</code> .
<code>--file</code>	Specifies a file containing configuration settings.

Note – If no options are specified for the `gateway config create` command, a series of online prompts are displayed, enabling you to type in the required settings.

If you use the `--file` option for `gateway config create`, the specified file must be of the same format as the `/opt/SUNWsgdg/etc/gatewayconfig.xml` file. This file is created during initial configuration of the SGD Gateway, as described in [“How to Configure the Ports and Connections for the SGD Gateway”](#) on page 12.

Examples

The following example configures an SGD Gateway to listen on TCP port 443 for connections from the network entry point, at 192.168.0.1. Secure connections are used between the SGD Gateway and the SGD servers in the array.

```
# /opt/SUNWsgdg/bin/gateway config create --interface *:443 \  
--entry-point 192.168.0.1:443 --out ssl
```

`gateway config list`

Lists the current SGD Gateway configuration.

Syntax

```
gateway config list [ --binding ]  
                   [ --routes-http-maxcon ]  
                   [ --routes-aip-maxcon ]  
                   [ --routes-reverseproxy-redirect ]  
                   [ --services-reflection-binding ]  
                   [ --services-reflection-auth-binding ]
```

Description

The command-line options enable you to list specific configuration settings. If no options are specified, the full configuration details for the SGD Gateway are displayed.

The current SGD Gateway configuration is stored in the `/opt/SUNWsgdg/etc/gatewayconfig.xml` file.

The following table shows the available options for this command.

Option	Description
<code>--binding</code>	Interface and port that the SGD Gateway listens on for incoming proxy connections
<code>--routes-http-maxcon</code>	Maximum number of Hypertext Transfer Protocol (HTTP) connections
<code>--routes-aip-maxcon</code>	Maximum number of Adaptive Internet Protocol (AIP) connections
<code>--routes-reverseproxy-redirect</code>	HTTP redirection port
<code>--services-reflection-binding</code>	Interface and port used for unauthenticated access to the SGD Gateway reflection service
<code>--services-reflection-auth-binding</code>	Interface and port used for authenticated access to the SGD Gateway reflection service

Examples

The following example shows binding configuration and the maximum number of AIP connections for the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway config list --binding --routes-aip-maxcon  
binding: *:443  
routes-aip-maxcon: 2920
```

The following example shows full details for the current SGD Gateway configuration.

```
# /opt/SUNWsgdg/bin/gateway config list
binding: *:443
routes-http-maxcon: 100
routes-aip-maxcon: 2920
routes-reverseproxy-redirect: null
services-reflection-binding: localhost:81
services-reflection-auth-binding: *:82
```

gateway config edit

Edits the current SGD Gateway configuration.

Syntax

```
gateway config edit [ --binding int:port ]
                    [ --routes-http-maxcon num ]
                    [ --routes-aip-maxcon num ]
                    [ --routes-reverseproxy-redirect port ]
                    [ --services-reflection-binding int:port ]
                    [ --services-reflection-auth-binding int:port ]
```

Description

The command-line options enable you to edit specific configuration settings. You must specify at least one command-line option.

The current SGD Gateway configuration is stored in the `/opt/SUNWsgdg/etc/gatewayconfig.xml` file.

You must restart the SGD Gateway to enable any configuration changes you make.

The following table shows the available options for this command.

Option	Description
<code>--binding</code>	Interface and port that the SGD Gateway listens on for incoming proxy connections. The default is TCP port 443, on all interfaces.
<code>--routes-http-maxcon</code>	Maximum number of HTTP connections. The default value is configured at install time and depends on the memory resources available on the SGD Gateway. See “Tuning the SGD Gateway” on page 61 .
<code>--routes-aip-maxcon</code>	Maximum number of AIP connections. The default value is configured at install time and depends on the memory resources available on the SGD Gateway. See “Tuning the SGD Gateway” on page 61 .
<code>--routes-reverseproxy-redirect</code>	HTTP redirection port. The default is TCP port 8080.
<code>--services-reflection-binding</code>	Interface and port used for unauthenticated access to the SGD Gateway reflection service. The default is TCP port 81 on the localhost loopback interface.
<code>--services-reflection-auth-binding</code>	Interface and port used for authenticated access to the SGD Gateway reflection service. The default is TCP port 82 on all interfaces.

Examples

The following example changes the maximum number of HTTP and AIP connections for the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

gateway config enable

Enables one or more SGD Gateway services.

Syntax

```
gateway config enable [ --services-reflection ]
                    [ --services-reflection-auth ]
                    [ --routes-http-redirect ]
```

Description

Use the command line options to enable specific SGD Gateway services. You must specify at least one command-line option.

Note – After using this command to enable a service, you must restart the SGD Gateway to start the service.

The following table shows the available options for this command.

Option	Description
<code>--services-reflection</code>	Enables unauthenticated access to the SGD Gateway reflection service. By default, this service is disabled. See “The Reflection Service” on page 67 for more details about the SGD Gateway reflection service.
<code>--services-reflection-auth</code>	Enables authenticated access to the SGD Gateway reflection service. By default, this service is disabled. See “The Reflection Service” on page 67 for more details about the SGD Gateway reflection service.
<code>--routes-http-redirect</code>	Enables the HTTP redirection service. By default, this service is disabled.

Examples

The following example enables authenticated access to the SGD Gateway reflection service.

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
```

```
gateway config disable
```

Disables one or more SGD Gateway services.

Syntax

```
gateway config disable [ --services-reflection ]  
                      [ --services-reflection-auth ]  
                      [ --routes-http-redirect ]
```

Description

Use the command line options to disable specific SGD Gateway services. You must specify at least one command-line option.

Note – After using this command to disable a service, you must restart the SGD Gateway to stop the service.

The following table shows the available options for this command.

Option	Description
<code>--services-reflection</code>	Disables unauthenticated access to the SGD Gateway reflection service. By default, this service is disabled. See “The Reflection Service” on page 67 for more details about the SGD Gateway reflection service.
<code>--services-reflection-auth</code>	Disables authenticated access to the SGD Gateway reflection service. By default, this service is disabled. See “The Reflection Service” on page 67 for more details about the SGD Gateway reflection service.
<code>--routes-http-redirect</code>	Disables the HTTP redirection service. By default, this service is disabled.

Examples

The following example disables authenticated access to the SGD Gateway reflection service.

```
# /opt/SUNWsgdg/bin/gateway config disable --services-reflection-auth
```

gateway server

Authorizes SGD servers to use the SGD Gateway.

Syntax

```
gateway server add | remove | list
```

Description

The following table shows the available subcommands for this command.

Subcommand	Description	More Information
add	Authorizes an SGD server to use the SGD Gateway	“gateway server add” on page 42
remove	Removes authorization for an SGD server to use the SGD Gateway	“gateway server remove” on page 43
list	Lists the SGD servers authorized to use the SGD Gateway	“gateway server list” on page 44

Examples

The following example removes authorization to use the SGD Gateway for the SGD server `sgd.example.com`.

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

```
gateway server add
```

Authorizes an SGD server to use the SGD Gateway.

Syntax

```
gateway server add --server server-name  
                  --certfile cert-file  
                  --url server-url  
                  [ --ssl-certfile ssl-cert ]
```

Description

The following table shows the available options for this command.

Option	Description
<code>--server</code>	DNS name of the SGD server

Option	Description
<code>--cert-file</code>	Certificate Authority (CA) certificate for the SGD server
<code>--url</code>	Uniform Resource Locator (URL) for the SGD web server
<code>--ssl-certfile</code>	SSL certificate for the SGD server

The `gateway server add` command does the following:

- Imports the CA certificate for the SGD server into the SGD Gateway keystore, at `/opt/SUNWsgdg/proxy/etc/keystore`. The CA certificate is stored to the keystore using an alias with the same name as the SGD server specified by the `--server` option.
- Imports the SSL certificate for the SGD server into the SGD Gateway keystore, at `/opt/SUNWsgdg/proxy/etc/keystore`. The SSL certificate is stored to the keystore using an alias constructed by appending “-ssl” to the SGD server name specified by the `--server` option.
- Adds the SGD server to the load balancing group used by the Apache reverse proxy server

Note – After using `gateway server add`, you must restart the SGD Gateway for any changes to take effect.

Examples

The following example adds the CA certificate `PeerCAcert.pem` to the SGD Gateway keystore, using the alias `sgd.example.com`. The SSL certificate `cert.pem` is also added to the keystore, using the alias `sgd.example.com-ssl`.

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd.example.com \
--certfile PeerCAcert.pem \
--url https://sgd.example.com \
--ssl-certfile cert.pem
```

In this example, the URL for the SGD web server, `https://sgd.example.com`, is added to the reverse proxy load balancing group and a configuration file is created at `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/conf/extra/gateway/servers/conf/sgd.example.com.conf`.

`gateway server remove`

Removes authorization for an SGD server to use the SGD Gateway.

Syntax

```
gateway server remove --server server-name
```

Description

The CA certificate and SSL certificate for the SGD server are removed from the SGD Gateway keystore.

Note – After using `gateway server remove`, you must restart the SGD Gateway for any changes to take effect.

Examples

The following example removes authorization for the SGD server `sgd.example.com` to use the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

gateway server list

Shows details for the SGD servers authorized to use the SGD Gateway.

Syntax

```
gateway server list
```

Description

This command shows certificate details and URLs for the SGD servers that are authorized to use the SGD Gateway.

Examples

The following example lists details of the authorized SGD servers for the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway server list
```

gateway status

Displays the current status of the SGD Gateway.

Syntax

```
gateway status
```

Description

This command indicates if the SGD Gateway is started, stopped, or if there is a problem.

Examples

The following example displays status information for the SGD Gateway. In this example, the SGD Gateway is stopped.

```
# /opt/SUNWsgdg/bin/gateway status  
SGD Gateway status: STOPPED
```

gateway version

Displays the version number of the SGD Gateway software.

Syntax

```
gateway version
```

Description

Displays the version number of the SGD Gateway.

Examples

The following example displays the SGD Gateway version installed on the host where the command is run.

```
# /opt/SUNWsgdg/bin/gateway version
Sun Secure Global Desktop Gateway 4.50.301
```

gateway sslcert

Print or exports the SGD Gateway SSL certificate stored in the client keystore.

Syntax

```
gateway sslcert export | print
```

Description

The following table shows the available subcommands for this command.

Subcommand	Description	More Information
export	Exports the SGD Gateway SSL certificate from the client keystore	“gateway sslcert export” on page 47
print	Prints the SGD Gateway SSL certificate stored in the client keystore	“gateway sslcert print” on page 47

Examples

The following example prints the SGD Gateway SSL certificate stored in the client keystore.

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

gateway sslcert export

Exports the SGD Gateway SSL certificate from the client keystore.

Syntax

```
gateway sslcert export --certfile cert-file
```

Description

Exports the SGD Gateway SSL certificate from the client keystore, at `/opt/SUNWsgdg/proxy/etc/keystore.client`. The certificate is written to the file specified by the `--certfile` option.

To access the client keystore, this command uses the password in `/opt/SUNWsgdg/etc/password`. If this file is not present, the command prompts for a password.

Examples

The following example exports the SGD Gateway SSL certificate from the client keystore to the file, `gateway-ssl.pem`.

```
# /opt/SUNWsgdg/bin/gateway sslcert export --certfile gateway-ssl.pem
```

gateway sslcert print

Prints the SGD Gateway SSL certificate.

Syntax

```
gateway sslcert print
```

Description

Prints the SGD Gateway SSL certificate stored in the client keystore, at `/opt/SUNWsgdg/proxy/etc/keystore.client`.

The command writes details of the certificate to the terminal window.

To access the client keystore, this command uses the password in `/opt/SUNWsgdg/etc/password`. If this file is not present, the command prompts for a password.

Examples

The following example prints the SGD Gateway SSL certificate stored in the client keystore.

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

gateway sslkey

Manages SSL key and certificate entries in the client keystore.

Syntax

```
gateway sslkey import | export
```

Description

The following table shows the available subcommands for this command.

Subcommand	Description	More Information
import	Imports a private key and certificate into the client keystore	“gateway sslkey import” on page 49
export	Exports a private key from the client keystore	“gateway sslkey export” on page 50

Examples

The following example exports the SGD Gateway SSL certificate stored in the client keystore.

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

gateway sslkey import

Imports an SSL key and certificate into the client keystore.

Syntax

```
gateway sslkey import --keyfile key-file
                        [ --keyalg RSA|DSA ]
                        { --certfile cert-file |
                          --certfile cert-file.. [ --cacertfile ca-cert-file ] }
                        [ --alwaysoverwrite ]
```

Description

Imports an SSL private key, and the corresponding SSL certificate, into the client keystore, at `/opt/SUNWsgdg/proxy/etc/keystore.client`. By default, this keystore contains a single self-signed certificate.

If the client keystore already has an entry, this command overwrites it. By default, a confirmation prompt is shown before overwriting the keystore entry.

To access the client keystore, this command uses the password in `/opt/SUNWsgdg/etc/password`. If this file is not present, the command prompts for a password.

The following table shows the available options for this command.

Option	Description
<code>--keyfile</code>	File containing the SSL private key. The key must be in Privacy Enhanced Mail (PEM) format.
<code>--keyalg</code>	Encoding algorithm used by the private key. Options are RSA and Digital Signature Algorithm (DSA). By default, RSA is selected.
<code>--certfile</code>	SSL certificate file.
<code>--cacertfile</code>	CA certificate or root certificate file.
<code>--alwaysoverwrite</code>	Do not prompt before overwriting the entry in the client keystore.

To import a certificate chain, use the `--cacertfile` option to specify the Intermediate CA certificate. All certificates in the chain must be in PEM format.

If a certificate chain uses multiple CA certificates, combine all the CA certificates in the chain into a single file. The CA certificate used to sign the server certificate *must appear first*, for example:

```
-----BEGIN CERTIFICATE-----  
...Intermediate CA's certificate...  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
...CA root certificate...  
-----END CERTIFICATE-----
```

Examples

The following example imports an RSA-encoded SSL private key `gateway1-ssl.key`, and the corresponding SSL certificate `gateway1-ssl.pem`, into the client keystore.

```
# /opt/SUNWsgdg/bin/gateway sslkey import \  
--keyfile gateway1-ssl.key \  
--certfile gateway1-ssl.pem
```

The following example imports an RSA-encoded SSL private key and an SSL certificate chain into the client keystore. The Intermediate CA certificate is `gateway1-ca.pem`.

```
# /opt/SUNWsgdg/bin/gateway sslkey import \  
--keyfile gateway1-ssl.key \  
--certfile gateway1-ssl.pem \  
--cafile gateway1-ca.pem
```

gateway sslkey export

Exports the SGD Gateway SSL private key from the client keystore.

Syntax

```
gateway sslkey export --keyfile key-file [ --keypass passwd ]
```

Description

Exports the SGD Gateway SSL private key from the client keystore, at `/opt/SUNWsgdg/proxy/etc/keystore.client`. The private key is written to the file specified by the `--keyfile` option.

A password for the private key can be specified using the `--keypass` option. By default, the password from `/opt/SUNWsgdg/etc/password` is used.

Examples

The following example exports the SGD Gateway SSL private key from the client keystore to the file, `gateway-ssl.key`.

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

gateway cert export

Exports the SGD Gateway certificate from the SGD Gateway keystore.

Syntax

```
gateway cert export --certfile file-name
```

Description

Exports the SGD Gateway certificate from the SGD Gateway keystore, at `/opt/SUNWsgdg/proxy/etc/keystore`. The certificate is written to the file specified by the `--certfile` option.

To access the SGD Gateway keystore, this command uses the password in `/opt/SUNWsgdg/etc/password`. If this file is not present, the command prompts for a password.

Examples

The following example exports the SGD Gateway certificate from the SGD Gateway keystore to the file, `gateway1.pem`.

```
# /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
```

gateway key import

Imports an SGD Gateway key and SGD Gateway certificate into the SGD Gateway keystore.

Syntax

```
gateway key import --keyfile key-file
                    [ --keyalg RSA|DSA ]
                    { --certfile cert-file |
                      --certfile cert-file.. [ --cacertfile ca-cert-file ] }
                    [ --alwaysoverwrite ]
```

Description

Imports a private key, and the corresponding public key certificate, into the SGD Gateway keystore, at `/opt/SUNWsgdg/proxy/etc/keystore`.

If the keystore already has an SGD Gateway key entry, it is overwritten. By default, a confirmation prompt is shown.

To access the SGD Gateway keystore, this command uses the password in `/opt/SUNWsgdg/etc/password`. If this file is not present, the command prompts for a password.

The following table shows the available options for this command.

Option	Description
<code>--keyfile</code>	File containing the private key. The key must be in PEM format.
<code>--keyalg</code>	Encoding algorithm used by the private key. Options are RSA and DSA. By default, RSA is selected.
<code>--certfile</code>	SSL certificate file.
<code>--cacertfile</code>	CA or root certificate file.
<code>--alwaysoverwrite</code>	Do not prompt before overwriting an entry in the keystore.

To import a certificate chain, use the `--cacertfile` option to specify an Intermediate CA certificate. All certificates in the chain must be in PEM format.

If a certificate chain uses multiple CA certificates, combine all the CA certificates in the chain into a single file. The CA certificate used to sign the server certificate *must appear first*, for example:

```
-----BEGIN CERTIFICATE-----  
...Intermediate CA's certificate...  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
...CA root certificate...  
-----END CERTIFICATE-----
```

Examples

The following example imports an RSA-encoded private key `gateway1.key`, and the corresponding public key certificate `gateway1.pem`, into the SGD Gateway keystore.

```
# /opt/SUNWsgdg/bin/gateway key import \  
--keyfile gateway1.key \  
--certfile gateway1.pem
```

The following example imports a private key and a certificate chain into the SGD Gateway keystore. The Intermediate CA certificate is `gateway1-ca.pem`.

```
# /opt/SUNWsgdg/bin/gateway key import \  
--keyfile gateway1.key \  
--certfile gateway1.pem \  
--cafile gateway1-ca.pem
```

gateway setup

Runs the setup program for the SGD Gateway.

Syntax

```
gateway setup
```

Description

Answer the on-screen questions to configure ports, interfaces, and security settings used by the SGD Gateway.

Examples

The following example runs the SGD Gateway setup program.

```
# /opt/SUNWsgdg/bin/gateway setup
```

```
gateway uninstall
```

Uninstalls the SGD Gateway software.

Syntax

```
gateway uninstall
```

Description

Stops the SGD Gateway and removes the SGD Gateway software, including all configuration information.

Before stopping the SGD Gateway, the command prompts the user for confirmation.

Examples

The following example uninstalls the SGD Gateway software from the host where the command is run.

```
# /opt/SUNWsgdg/bin/gateway uninstall
```

The tarantella gateway Command

Use the `tarantella gateway` command to configure authorized gateways for an SGD array.

Syntax

```
tarantella gateway add | list | remove
```

Description

Using the `tarantella gateway` command, you can add, remove, and list the gateways for an SGD array.

The `tarantella gateway` command can be used on any SGD server in the array. Any changes you make are automatically replicated on other array members.

When an SGD server joins an array, the set of gateways defined on the primary SGD server is copied to the new array member, overwriting any authorized gateways already present. Registered gateways are not deleted from an SGD server when it is detached from an array.

The available subcommands for the `tarantella gateway` command are shown in the following table.

Subcommand	Description	More Information
<code>add</code>	Adds an SGD Gateway for an SGD array	“tarantella gateway add” on page 56
<code>list</code>	Lists the SGD Gateways for an SGD array	“tarantella gateway list” on page 57
<code>remove</code>	Removes an SGD Gateway for an SGD array	“tarantella gateway remove” on page 57

Note – All `tarantella gateway` subcommands include a `--help` option. You can use this option to display help for the subcommand.

Examples

The following example adds `gateway1.example.com` to the list of registered gateways for the SGD array.

```
$ tarantella gateway add --name gateway1.example.com \  
--certfile /opt/gateway1_cert_file.pem
```

tarantella gateway add

Registers an SGD Gateway with an SGD array.

Syntax

```
tarantella gateway add {  
    --name server-name  
    --certfile cert-file  
} | --file file
```

Description

The following table shows the available options for this command.

Option	Description
<code>--name</code>	Name of the SGD Gateway to register.
<code>--certfile</code>	SGD Gateway certificate used by the SGD server. The certificate can be in Definite Encoding Rules (DER) or PEM format.
<code>--file</code>	A batch file containing configuration settings for multiple SGD Gateways.

Examples

The following example adds `gateway1.example.com` to the list of registered gateways for the SGD array.

```
$ tarantella gateway add --name gateway1.example.com \  
--certfile /opt/gateway1_cert_file.pem
```

The following example uses the `--file` option of `tarantella gateway add` to register multiple gateways at the same time.

```
$ tarantella gateway add --file gateways.list
```

The `--file` option specifies a batch file, `gateways.list`, that contains a line of settings for each gateway, as follows:

```
--name gateway1.example.com --certfile /opt/gateway1_cert_file.pem  
--name gateway2.example.com --certfile /opt/gateway2_cert_file.pem
```

tarantella gateway list

Lists the SGD Gateways registered for an SGD array.

Syntax

```
tarantella gateway list
```

Description

Shows details for the SGD Gateways that have been registered for an SGD array using `tarantella gateway add`.

Examples

The following example lists the registered gateways for the SGD array.

```
$ tarantella gateway list
```

tarantella gateway remove

Removes an SGD Gateway from the list of registered gateways for an SGD array.

Syntax

```
tarantella gateway remove --name server-name | --file file
```

Description

The following table shows the available options for this command.

Option	Description
<code>--name</code>	Name of the SGD Gateway to remove registration details for
<code>--file</code>	A batch file containing configuration settings for multiple SGD Gateways

Examples

The following example removes the SGD Gateway `gateway1.example.com` from the list of registered gateways for the SGD array.

```
$ tarantella gateway remove --name gateway1.example.com
```

The `--security-gateway` Attribute

You use the `--security-gateway` attribute to enable SGD Gateway usage for the SGD array. The attribute defines the SGD Clients that can access the SGD Gateway, based on their IP address or DNS name.

Changes to the `--security-gateway` attribute apply to all SGD servers in the array.

The syntax for the attribute is as follows:

```
--security-gateway filter-spec...
```

Replace *filter-spec* with a filter specification of the type:

```
client-ip-address | * : gateway protocol : gateway-address : gateway-port
```

where *client-ip-address* is the IP address of the SGD Client. An asterisk, `*`, represents all IP addresses. For connections through the SGD Gateway, this is the address that the SGD servers in the array use to connect to the SGD Gateway.

Note – If you are using an external load balancer with the SGD Gateway, type the address of the load balancer for the *client-ip-address*.

The *gateway protocol* is `sgdg` for connections through the SGD Gateway, or `direct` for SGD Clients that connect directly to an SGD array, without going through the SGD Gateway.

The *gateway-address* is the external address of the SGD Gateway, or an external load balancer, if used. This is the address that client devices use to contact the SGD Gateway.

The *gateway-port* is the port that client devices use to connect to the SGD Gateway, or an external load balancer, if used.

Separate multiple *filter-spec* entries with a `“,”` character.

The following example enables all SGD Clients to connect using TCP port 443 of the SGD Gateway `gateway1.example.com`.

```
$ tarantella config edit --security-gateway "*:sgdg:gateway1.example.com:443"
```

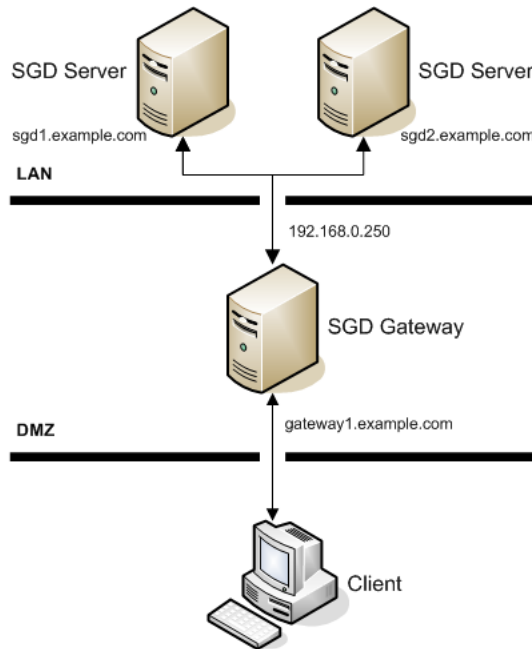
The following example enables all SGD Clients to connect using an external load balancer, `lb.example.com`.

```
$ tarantella config edit --security-gateway \  
"*:sgdg:lb.example.com:443"
```

You can use multiple filter specifications, as shown in the following example.

Consider a basic deployment, as shown in [FIGURE B-1](#). The deployment uses a single SGD Gateway, `gateway1.example.com`, with an SGD array that contains two SGD servers, `sgd1.example.com` and `sgd2.example.com`. The address of the SGD Gateway on the internal network is `192.168.0.250`.

FIGURE B-1 Using Multiple Filter Specifications



The following filter specification might be used for this example:

```
"192.168.0.250:sgdg:gateway1.example.com:443, \  
*:direct:sgd1.example.com:80"
```

With this configuration, the following applies:

- Connections to the SGD servers in the array are allowed from the SGD Gateway IP address, 192.168.0.250. SGD Clients outside the organization connect using TCP port 443 of the SGD Gateway, `gateway1.example.com`.
- All other SGD Clients, such as those on the local area network (LAN), connect directly to TCP port 80 on the SGD server `sgd1.example.com`. These connections do not use the SGD Gateway.
- The order of the filters is important. If the order of the filters is reversed, all SGD Clients connect directly to the SGD server `sgd1.example.com`.

Advanced Configuration

This chapter includes information about configuring and using the advanced features of the SGD Gateway.

This chapter includes the following topics:

- [“Tuning the SGD Gateway” on page 61](#)
- [“Configuring HTTP Redirection” on page 64](#)
- [“Changing the Binding Port for the SGD Gateway” on page 65](#)
- [“Enabling the Balancer Manager Application” on page 65](#)
- [“Using Unencrypted Connections to the SGD Array” on page 66](#)
- [“Using Unencrypted Incoming Connections to the SGD Gateway” on page 67](#)
- [“The Reflection Service” on page 67](#)

Tuning the SGD Gateway

When you install the SGD Gateway, default values for the maximum number of simultaneous Adaptive Internet Protocol (AIP) and Hypertext Transfer Protocol (HTTP) connections are configured automatically, based on the available memory on the SGD Gateway host. The memory size allocated to the SGD Gateway’s Java Virtual Machine (JVM™) is also optimized for this number of connections.

After installing the SGD Gateway, depending on the expected number of SGD users and the number of applications they will run, you can adjust the default settings. When you do this, you might also need to adjust the JVM memory size. This process is called *tuning* the SGD Gateway.



Caution – If the JVM memory size is too low for the expected number of connections, the SGD Gateway might stop working and refuse all subsequent connections. In this case, you need to tune the SGD Gateway so that sufficient JVM memory is available.

A `java.lang.OutOfMemoryError` error message on the SGD Gateway indicates that tuning might be required.

To tune the SGD Gateway, you do the following:

- Change the maximum number of AIP connections. See [“Changing the Maximum Number of AIP Connections”](#) on page 62.
- Change the maximum number of HTTP connections. See [“Changing the Maximum Number of HTTP Connections”](#) on page 63.
- Change the JVM memory size. See [“Changing the JVM Memory Size”](#) on page 63.

Changing the Maximum Number of AIP Connections

The maximum number of AIP connections is configured at install time. The default setting depends on the memory resources available on the SGD Gateway host.

You can change this setting to a value more appropriate for your deployment. See [“Calculating the Number of AIP Connections”](#) on page 62 for details of how to calculate the maximum number of AIP connections used by an SGD Gateway.

To change the maximum number of AIP connections, use the `--routes-aip-maxcon` option of the `gateway config edit` command. For example, to change the maximum number of AIP connections to 3000, run the following command:

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

You must restart the SGD Gateway to enable any changes you make.

Calculating the Number of AIP Connections

The number of AIP connections used by an SGD Gateway depends on the number of concurrent SGD users, and the number of applications they run, as follows:

Number of AIP connections = $(\textit{number of applications} + 3) \times \textit{number of SGD users}$

For example, an SGD Gateway with 1000 SGD users, each running four applications requires the following maximum number of simultaneous AIP connections:

$$(4 + 3) \times 1000 = 7000 \text{ AIP connections}$$

Changing the Maximum Number of HTTP Connections

The maximum number of HTTP connections is configured at install time. The default value is 100.

To change the maximum number of HTTP connections, use the `--routes-http-maxcon` option of the `gateway config edit` command. For example, to change the maximum number of HTTP connections to 200, run the following command:

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
```

You must restart the SGD Gateway to enable any changes you make.

Changing the JVM Memory Size

When you change the maximum number of AIP and HTTP connections, you might need to change the memory size allocated to the SGD Gateway's JVM. To do this, edit the following settings in the `/opt/SUNWsgdg/proxy/etc/tuning_parameters` file:

- `-Xms` – Initial memory size for the JVM
- `-Xmx` – Maximum memory size for the JVM

See “Calculating the JVM Memory Size” on page 64 for details of how to calculate these values.

Note – Ensure that your system is configured with sufficient memory resources for the JVM settings you make.

You must restart the SGD Gateway to enable any changes you make.

Calculating the JVM Memory Size

The amount of JVM memory used by the SGD Gateway depends on the number of simultaneous AIP connections and HTTP connections.

As each SGD Gateway connection requires approximately 300 kilobytes of JVM memory, the required JVM memory is given by:

(number of AIP connections + number of HTTP connections) x 300 kilobytes

For example, an SGD Gateway with 500 SGD users, each running two applications. The maximum number of simultaneous AIP connections is:

$(2 + 3) \times 500 = 2500$ AIP connections

The SGD Gateway must also handle sufficient simultaneous HTTP connections to the SGD Web Server. For this example, the maximum number of HTTP connections is:

250 HTTP connections

So, the required JVM memory is:

$(2500 + 250) \times 300$ kilobytes = 806 Megabytes, approximately.

Note – In the `/opt/SUNWsgdg/proxy/etc/tuning_parameters` file, set `-Xms` and `-Xmx` to the calculated JVM memory value. `-Xms` and `-Xmx` are normally set to be the same value for performance reasons.

Configuring HTTP Redirection

By default, the SGD Gateway refuses HTTP connections on Transmission Control Protocol (TCP) port 80.

To enable connections on TCP port 80, use the `gateway config enable` command to enable the HTTP redirection service, as follows:

```
# /opt/SUNWsgdg/bin/gateway config enable --routes-http-redirect
```

You must restart the SGD Gateway to enable any changes you make.

Changing the Binding Port for the SGD Gateway

The interface and port that the SGD Gateway uses for incoming connections is called the *binding port*. By default, the SGD Gateway uses TCP port 443 on all interfaces as the binding port.

To change the binding port, use the `--binding` option of the `gateway config edit` command. For example, to change the binding port to TCP port 4443, run the following command:

```
# /opt/SUNWsgdg/bin/gateway config edit --binding *:4443
```

Alternatively, you can change the binding port by running the `/opt/SUNWsgdg/bin/gateway config create` command on the SGD Gateway host. This command prompts you to specify an interface and port to use for incoming proxy connections.

Note – The `gateway config create` command creates a new configuration and overwrites any configuration settings you have made.

You must restart the SGD Gateway to enable any changes you make.

Enabling the Balancer Manager Application

The Apache reverse proxy includes a web application called Balancer Manager. Balancer Manager enables you to manage the SGD web servers in the load balancing group used by the reverse proxy.

Using Balancer Manager, you can do the following:

- View status information for SGD web servers in the load balancing group
- View and change load balancing routes for SGD web servers
- Remove SGD web servers from the load balancing group

To enable Balancer Manager, remove the comments in the reverse proxy configuration file, `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/conf/extra/gateway/httpd-gateway.conf` that disable the application.

```
# Allows the configuration of load balancing parameters
#
# <Location /balancer-manager>
#     SetHandler balancer-manager
#     Order Deny,Allow
#     Deny from all
#     Allow from all
# </Location>
```

You must restart the reverse proxy to enable any changes you make.

To access Balancer Manager, start a browser and go to `https://gateway.example.com/balancer-manager`, where `gateway.example.com` is the SGD Gateway host.

For more details about configuring the Balancer Manager, see the Apache `mod_proxy_balancer` documentation.

Using Unencrypted Connections to the SGD Array

By default, connections between the SGD Gateway and the SGD servers in the array are secured using Secure Sockets Layer (SSL). This means that AIP over SSL data uses TCP port 5307, and HTTPS data uses TCP port 443.

To use unencrypted connections between the SGD Gateway and the SGD servers in the array, run the following command:

```
# gateway config create
```

When prompted whether to use secure connections to the SGD server, type `n`.

Note – Ensure that the SGD servers in the array are configured to use standard, unencrypted connections. To do this, run `tarantella security stop` on each SGD server in the array to turn off SGD security services.

For unencrypted connections, AIP data uses TCP port 3144, and HTTP data uses TCP port 80.

Using Unencrypted Incoming Connections to the SGD Gateway

By default, the SGD Gateway is configured to work with incoming HTTP and AIP data connections that are secured using SSL. Depending on your network configuration, you might instead want to use unencrypted incoming connections to the SGD Gateway.

To enable unencrypted incoming connections, change the symbolic link for the `gateway.xml` file, so that it links to the `gateway-plaintext.xml` file, instead of the default setting of `gateway-ssl.xml`. To do this, run the following command:

```
# ln -fs /opt/SUNWsgdg/etc/gateway-plaintext.xml /opt/SUNWsgdg/etc/gateway.xml
```

Note – Depending on your network configuration, you might also need to change the binding port for the SGD Gateway when you enable unencrypted incoming connections. How to do this is described in [“Changing the Binding Port for the SGD Gateway”](#) on page 65.

You must restart the SGD Gateway to enable any changes you make.

The Reflection Service

The *reflection service* is a collection of RESTful web services used by the routing proxy component of the SGD Gateway. Using the reflection service, an SGD Gateway Administrator can configure routes, services, logging levels, and connections, and show status information for the routing proxy.

This section includes the following reflection service topics:

- [“Enabling the Reflection Service”](#) on page 68
- [“Using the Reflection Service”](#) on page 71

Enabling the Reflection Service

By default, the reflection service is not enabled for the SGD Gateway.

You enable the reflection service for one or more of the following access methods:

- **Unauthorized access** – Users do not need to authenticate.

By default, unauthorized access is only available from the SGD Gateway host.

See “[How to Enable Unauthorized Access to the Reflection Service](#)” on page 68 for details of how to enable unauthorized access.

- **Authorized access** – Users must authenticate before accessing the reflection service.

See “[How to Enable Authorized Access to the Reflection Service](#)” on page 69 for details of how to enable authorized access.

▼ How to Enable Unauthorized Access to the Reflection Service

1. On the SGD Gateway host, log in as superuser (root).
2. Enable unauthorized access to the reflection service.

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection
```

3. (Optional) Change the interface used by the reflection service.



Caution – By default, unauthenticated access to the reflection service is only available from the SGD Gateway host. Enabling unauthenticated access on other interfaces can present a security risk.

The default interface used for unauthorized access to the reflection service is the `localhost` loopback interface. The following example shows how to enable unauthorized access on all interfaces:

```
# /opt/SUNWsgdg/gateway config edit \  
--services-reflection-binding *:81
```

4. (Optional) Change the port used by the reflection service.

The default port used for unauthorized access to the reflection service is TCP port 81. You can change this to another port that is not in use, as follows:

```
# /opt/SUNWsgdg/gateway config edit \  
--services-reflection-binding localhost:portnum
```

where *portnum* is the port number used by the reflection service.

5. Restart the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway restart
```

6. Access the reflection service.

On the SGD Gateway host, you can start a browser and go to `http://localhost:81`.

The home page for the reflection service is shown.

▼ How to Enable Authorized Access to the Reflection Service

1. On the SGD Gateway host, log in as superuser (root).

2. Export the certificate and private key for the reflection service.

The certificate and private key for the reflection service are stored in the reflection service keystore, at `/opt/SUNWsgdg/proxy/etc/keystore.reflection`. This keystore is created automatically during installation of the SGD Gateway.

By default, the reflection service keystore contains a single, self-signed certificate and key pair.

a. Export the certificate for the reflection service.

```
# /opt/SUNWsgdg/java/default/bin/keytool -exportcert \  
-alias server-name -rfc \  
-keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \  
-storepass "$(cat /opt/SUNWsgdg/etc/password)" \  
-file client.pem
```

where *server-name* is the alias used for the reflection service certificate in the reflection keystore and *client.pem* is the file name of the exported certificate.

b. Export the private key for the reflection service.

Use the KeyManager application included with the SGD Gateway.

```
# /opt/SUNWsgdg/java/default/bin/java \  
-jar /opt/SUNWsgdg/proxy/KeyManager.jar export \  
--keyfile client.key \  
--keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \  
--keyalias alias-name \  
--keypass "$(cat /opt/SUNWsgdg/etc/password)" \  
--storepass "$(cat /opt/SUNWsgdg/etc/password)"
```

where *alias-name* is the alias used for the reflection service key in the reflection keystore and *client.key* is the file name of the exported key.

3. Install the certificate and private key on the client device.

The certificate and private key are used by the client device to authorize to the reflection service.

4. Enable authorized access to the reflection service.

On the SGD Gateway host, run the following command:

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
```

5. (Optional) Change the interface and port used by the reflection service.

The default binding used for authorized access to the reflection service is TCP port 82 on all interfaces. You can change this to another interface and a port that is not in use, as follows:

```
# /opt/SUNWsgdg/gateway config edit \  
--services-reflection-binding int:portnum
```

where *int* is the interface, and *portnum* is the port number used by the reflection service.

6. Restart the SGD Gateway.

```
# /opt/SUNWsgdg/bin/gateway restart
```

7. Connect to the reflection service from the client device, using the certificate and private key.

```
$ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82
```

In this example, the `curl` command is used to access the home page of the reflection service at `https://gateway.example.com:82`, where `gateway.example.com` is the name of the SGD Gateway. The certificate and private key for the reflection service are `client.pem` and `client.key`.

Using the Reflection Service

Use a client application to access the RESTful web services provided by the reflection service. Examples of suitable client applications include the following:

- **Browser.** Using a browser is the simplest method of accessing the reflection service. However, a browser only supports HTTP GET requests and therefore limits access to only those RESTful web services that retrieve information. In practice, using a browser is helpful for tasks such as displaying status information and listing routes and services for the routing proxy.
- **curl.** This is a command-line tool for UNIX and Linux platforms that supports HTTP GET, PUT, POST, and DELETE requests. This means that the full range of RESTful web services for the reflection service can be used. Output from this tool can be redirected to a file, or to another program for further processing.

Alternatively, if you have your own client application that supports RESTful web services, you can use it to access the reflection service.

Note – You do not need to restart the SGD Gateway when you use the reflection service to change the configuration of the routing proxy.

Data can be returned from the reflection service in the following output formats:

- **ASCII.** This is the default output format. Data is returned in tab-delimited ASCII format. This output format is useful if the data is to undergo further processing, such as parsing.
- **HTML.** Data is returned in Hypertext Markup Language (HTML) format, suitable for displaying in a browser. To return HTML output, append `/html` to the end of the web service Uniform Resource Identifier (URI).

About the RESTful Web Services

The following table lists the RESTful web services for the SGD Gateway reflection service.

Relative URI	HTTP Request Method	Description
/	GET	Shows high-level information for the routing proxy, such as the uptime.
/service	GET	Lists the available services. A service represents an entry point from which the routing proxy creates incoming connections.
/service/ <i>Service-Id</i>	GET	Lists information for a service, identified by <i>Service-Id</i> .
/service/ <i>Service-Id</i>	PUT	Starts a service, identified by <i>Service-Id</i> .
/service/ <i>Service-Id</i>	DELETE	Stops a service, identified by <i>Service-Id</i> .
/client	GET	Lists the available clients. A client represents an exit point on which the routing proxy constructs outgoing connections.
/client/ <i>Client-Id</i>	GET	Lists information for a client, identified by <i>Client-Id</i> .
/route	GET	Lists the available routes. A route represents a path through the routing proxy, from incoming connections through services to outgoing connections through clients.
/route/ <i>Route-Id</i>	GET	Lists information for a route, identified by <i>Route-Id</i> .
/route/ <i>Route-Id</i>	PUT	Starts a route, identified by <i>Route-Id</i> .
/route/ <i>Route-Id</i>	DELETE	Stops a route, identified by <i>Route-Id</i> .
/route/ <i>Route-Id</i> /connection	GET	Lists the connections for a specific route, identified by <i>Route-Id</i> .
/route/ <i>Route-Id</i> /connection/ <i>Connection-Id</i>	DELETE	Terminates a connection, identified by <i>Connection-Id</i> .
/connection	GET	Lists all currently running connections, for all routes.
/logging/level	GET	Shows the global logging level.
/logging/level/ <i>Log-Level</i>	PUT	Sets the routing proxy's global logging level.
/logging/ <i>Package</i> /level	GET	Shows the logging level for a specific component of the routing proxy.
/logging/ <i>Package</i> /level/ <i>Log-Level</i>	PUT	Sets the logging level for a specific component of the routing proxy.

To access a RESTful web service, append the relative URI for the web service to the Uniform Resource Locator (URL) of the reflection service.

For example, to list the available routes for an SGD Gateway, *gateway.example.com*, append `/route` to the URL of the reflection service, as follows:

```
$ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82/route
```

where *client.pem* and *client.key* are the certificate and private key for the reflection service. In this example, the client is authorized before accessing the reflection service.

Examples of Using the Reflection Service

All of the following examples use the `curl` command as a client application to access the reflection service.

The examples use authenticated access to the reflection service on an SGD Gateway called *gateway.example.com*. The client is authorized using a certificate, *client.pem*, and a private key, *client.key*.

To list the available services for the SGD Gateway:

```
$ curl --cert client.pem --key client.key -k \  
-X GET https://gateway.example.com:82/service
```

To stop a route, specify the Route Id that the reflection service uses for the route:

```
$ curl --cert client.pem --key client.key -k \  
-X GET https://gateway.example.com:82/route  
Route Id  Route Uptime    Service Id  ...  
0         21h18m20s743m  ssgd-route-service ...  
1         21h18m20s736m  shttp-ssl-service ...  
$ curl --cert client.pem --key client.key -k \  
-X DELETE https://gateway.example.com:82/route/1
```

To set the global logging level to FINER:

```
$ curl --cert client.pem --key client.key -k \  
-X PUT https://gateway.example.com:82/logging/level/FINER
```


Troubleshooting the SGD Gateway

This chapter includes troubleshooting topics, to help you to diagnose and fix problems with the SGD Gateway.

This chapter includes the following topics:

- “Logging and Diagnostics” on page 75
- “SGD Gateway Error Messages” on page 78

Logging and Diagnostics

This section describes the logging and diagnostics features of the SGD Gateway.

This section includes the following topics:

- “About SGD Gateway Logging” on page 75
- “Displaying SGD Gateway Process Information” on page 77
- “Checking the Configuration From the Command Line” on page 77
- “SGD Gateway Error Messages” on page 78

About SGD Gateway Logging

SGD Gateway logging uses the Java logging application programming interface (API). For more details about how logging is implemented in Java, see <http://java.sun.com/javase/6/docs/technotes/guides/logging/overview.html>.

Changing the Logging Level

A logging properties configuration file, `logging.properties`, is supplied with the SGD Gateway. This file is in the `/opt/SUNWsgdg/proxy/etc` directory.

You can edit the `logging.properties` file to change the default logging level, and to configure logging levels for specific SGD Gateway services. Each SGD Gateway service is represented by an `async.channel` entry in the `logging.properties` file.

For example, if you want to increase logging levels for incoming and outgoing Transmission Control Protocol (TCP) connections, set the TCP service logging level to `FINEST`. Uncomment the following line in the `logging.properties` file:

```
# async.channel.tcp.level=FINEST
```

You must restart the SGD Gateway to enable any changes to logging levels you make by editing the `logging.properties` file.

Note – You can also use the SGD Gateway reflection service to change logging levels. See [“The Reflection Service” on page 67](#) for information about configuring and using the reflection service.

Log File Locations

If you have problems with the SGD Gateway, consult the following log files:

- **Routing proxy log files.** The location and names of these log files are set in the `logging.properties` file. By default, the SGD Gateway creates routing proxy log files in the `/opt/SUNWsgdg/proxy/var/log` directory on the SGD Gateway host.
- **Reverse proxy log files.** Details of load balancing and proxy server activity for HTTP and HTTPS connections are logged to the Apache log files in the `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/logs` directory on the SGD Gateway host.
- **SGD server log files.** Each SGD server in the array writes error messages to log files in the `/opt/tarantella/var/log` directory on the SGD server host. See *“Monitoring and Logging”* in Chapter 6 of the *Sun Secure Global Desktop 4.5 Administration Guide* for more details about configuring logging for SGD servers.

Displaying SGD Gateway Process Information

When you start the SGD Gateway, the process ID of the routing proxy is stored to the `/opt/SUNWsgdg/proxy/var/run/proxy.pid` file on the SGD Gateway host.

The process ID of the reverse proxy is stored to the `/opt/SUNWsgdg/httpd/httpd-2.2.10_openssl-0.9.8i_jk.1.2.25/logs/httpd.pid` file. This file location can be changed using the `PidFile` directive in the `httpd.conf` Apache configuration file.

To display the running SGD Gateway processes, use the following command on the SGD Gateway host:

```
# ps -ef | grep SUNWsgdg
```

Checking the Configuration From the Command Line

You can use the following commands to check your SGD Gateway configuration.

- `gateway status` – Shows status information for the SGD Gateway.

Run the following command on the SGD Gateway host:

```
# /opt/SUNWsgdg/bin/gateway status
```

See also “[gateway status](#)” on page 45 for more information about this command.

- `tarantella gateway list` – Displays a list of the SGD Gateways that are authorized for use by the SGD array.

Run the following command on any SGD server in the array:

```
$ tarantella gateway list
```

See “[The tarantella gateway Command](#)” on page 54 for more details about using the `tarantella gateway` command.

- `tarantella config list` – Displays global settings for the SGD array.

Run the following command on any SGD server to show the `--security-gateway` attribute setting. This attribute determines which SGD Clients are allowed to use the SGD Gateway.

```
$ tarantella config list --security-gateway
```

See “[The --security-gateway Attribute](#)” on page 58 for more details about this attribute.

SGD Gateway Error Messages

SGD Gateway error messages are reported to the routing proxy log files, located in the `/opt/SUNWsgdg/proxy/var/log` directory on the SGD Gateway host.

Some typical SGD Gateway error messages, along with an explanation of the probable cause, are listed in the following table.

Error Message	Probable Cause
Failed to validate token: Token time not yet valid	The clocks on the SGD Gateway and the SGD servers in the array are not synchronized
Failed to decode token: No trusted signature found	The CA certificate for the SGD server has not been installed on the SGD Gateway
Failed to validate token: No recipient available to decrypt token	The SGD Gateway certificate has not been installed on the SGD array
SSL error: Check the proxy SSL keystore has valid trusted certificates	The SSL certificate for the SGD server has not been installed on the SGD Gateway