Trustwave®

Secure Web Gateway

Version 11.0

Setup Guide

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: support@Trustwave.com

Trademarks

Revision History

Table 1: Revision history

Version	Date	Changes
1.0	February 2012	Version 10.2
2.0	October 2012	Version 11.0 update

About This Guide

This guide provides the instructions you need to install and setup your Trustwave SWG appliance.

Formatting Conventions

This guide uses the following formatting conventions to denote specific information.

Table 2: Formatting conventions

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in **Lucinda Console** indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, or to introduce a new term.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Warnings

Note: This symbol indicates information that applies to the task at hand.

Tip: This symbol denotes a suggestion for a better or more productive way to use the product.

Caution: This symbol highlights a warning against using the software in an unintended manner.

Question: This symbol indicates a question that the reader should consider.

Table of Contents

1 Before You Begin

Note: Physical SWG appliances come with the required image already loaded. Should you need to reload or replace the image, you can find instructions in the *SWG Installation Utility Guide*.

You should perform the following tasks in the order listed:

1. Install the Appliance (see Chapter 2).
2. Set Up the Appliance (see Chapter 3).
3. Perform Additional Configuration (see Chapter 4).

After you have setup the appliance, you can configure the Management Console according to your needs. Instructions are provided in the *Management Console Reference Guide*.

2 Installing the Appliance

This chapter contains the following instructions:

- Installing a Physical SWG Appliance
- Deploying a Virtual SWG From an OVF File

2.1 Installing a Physical SWG Appliance

Installation consists of connecting to the appliance. You can connect in any of the following ways:

- Using an Ethernet Cable
- Using a Serial Cable (SWG 3000 and SWG 5000 only)
- Using a keyboard and monitor

Instructions for connecting are provided on the following pages. Before connecting to the appliance, ensure that the following requirements are satisfied.

2.1.1 Requirements before Installing a Physical Appliance

- Working electrical outlet:
  - 1 x Outlet for the SWG 3000
  - 2 x Outlets for the SWG 5000
  - 4 x 16amp Outlets for the SWG 7000, preferably via PDU
- Network connection — cable and switch
- Hardware for connecting — ethernet cable, serial cable, or a keyboard and monitor
- Rack space for the appliance
  - 1U Rack space for SWG 3000 or SWG 5000
  - 7U Rack space for SWG 7000
- Switch port for the internet cable
- Appliance name
- Physical address
- DNS address
- DNS name
- Default gateway

2.1.2 Connecting an Appliance Using an Ethernet Cable

2.1.2.1 For SWG 3000 and SWG 5000 models:

1. Plug in the power cable and switch the appliance on.

2. Connect a PC directly to the appliance's GE0 port or via a switch (for 5000-SWG, see 5000-SWG Rear Panel) using a standard (8 thread) Ethernet cable. CAT5e cables (or better) are recommended.

3. The default IP of the GE0 interface is 10.0.0.1, and its default netmask is 255.255.255.0. Configure the TCP/IP settings of your PC so that it is on the same logical network subnet as the appliance's GE0 interface. For example, configure the IP on the PC as 10.0.0.101 and the PC's netmask as 255.255.255.0.

> **IMPORTANT:** Do not set the PC's IP to 10.0.0.1, as this will result in an IP conflict with the appliance.

4. Continue with Initial Setup of your SWG Appliance using Limited Shell.

2.1.2.2 For an SWG 7000 appliance:

The SWG 7000 model is a chassis containing blade servers, each of which operates as an appliance. This provides for overall higher end performance.

Perform the following procedure for each blade regardless of its intended network role.

1. Plug in the power cables.

2. Configure the network settings of any PC to match those of the appliance (IP address and subnet mask).

   - IP address in the same subnet e.g. 10.0.0.101

   - Subnet mask 255.255.255.0

3. Connect your PC to one of the ports on the Gigabit Ethernet switch in I/O switch module Bay 1 on the appliance using an ethernet cable.

4. Power up the blades as follows:
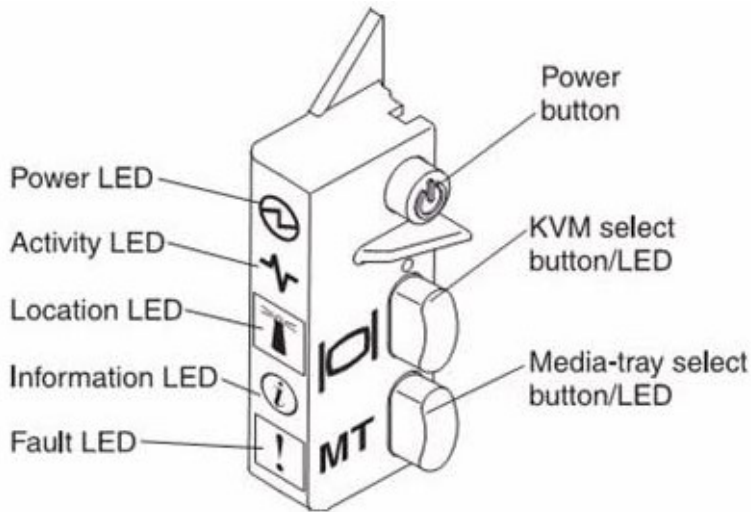
In the control panel for the blade:

a. Press the KVM Select button so that the VGA screen attached to the chassis displays output from the blade being powered up.

b. Press the Power button until the blade turns on. After the blade finishes booting, a login prompt is displayed.

5. Continue by doing either of the following:

- Repeat Step 1 for each blade, and when done, continue with initial Setup of your SWG Appliance blades using the Limited Shell, or

- Continue with Initial Setup of this SWG Appliance blade using the Limited Shell, and when done, repeat Step 1 for each blade.

Note: For more information on setting up the SWG 7000, contact your Trustwave representative.

2.1.3   Connecting an Appliance Using a Serial Cable

Note: Connection using a serial cable is applicable only to SWG 3000 and SWG 5000 appliances.

1. Connect the PC to the appliance's Serial Console, using the serial cable.
2. Using the Hyper Terminal application, enter the appropriate Port settings:

    - Bits per Second (Baud Rate): 19,200

    - Data Bits (Word): 8

    - Parity: None

    - Stop bits:1

2.2 Deploying a Virtual SWG from an OVF File

This section explains how to deploy a virtual SWG from an OVF file. Virtual SWG appliances are certified to work with VMWare ESXI version 4.1 servers.

Note: Before deploying the virtual appliance, ensure that you have access to a VMWare vSphere client and that the OVF files are accessible in your local machine.

1. In the vSphere client, choose File Æ Deploy OVF Template.
2. In the wizard, browse to the OVF file and then complete the deployment.

When done, it is recommended that you set the attributes for the virtual machine according to the values indicated in the following table.

Machine Attribute	Recommended Value
CPUs	At least 2
Memory	At least 4GB

3 Setting Up the Appliance

The setup procedure is the same for both physical and virtual SWG appliances. You perform setup using a setup script that is run in the Limited Shell.

> **Note:** Before setting up the installed appliance, you should prepare for setup by assembling the detailed information and values that you will need to supply as part of setup.

This chapter contains the following sections:

- Preparing Values for the Appliance Setup

- Setting Up the Appliance

3.1 Preparing Values for the Appliance Setup

What to Prepare	Details
1 **Decide the role of the appliance**	You must define a single Policy Server (provides management and reporting services), and at least one Scanner (provides scanning and authentication services). You can choose to define both of these roles in the same appliance or in different appliances:
	- **All In One (Default)** – Defines the appliance as both a Policy server and a Scanner. This value is often used for SWG 3000 or 5000 models.
	- **SWG Scanner** – Defines the appliance or blade as a Scanner only.
	- **SWG Policy Server** – Defines the appliance or blade as a Policy Server only.
2 **Decide what network interface should be used for the appliance:**	

Network Interfaces	Description
GE0 (eth0): 1GB - Auto-negotiation enabled - Recommended!	Allows communication at a speed of up to 1GB with **Auto- Negotiation** enabled. Auto- negotiation enables simple, automatic connection of appliances by taking control of the cable when a connection is established to a network device that supports a variety of modes from a variety of manufacturers. The device is able to automatically configure the highest speed.
GE1 (eth1): 1GB - Auto-negotiation	Allows communication at a speed of up to 1GB with **Auto- Negotiation** enabled.
GE2 (eth2): 1GB - Auto-negotiation	(Available for SWG 5000, and the Policy Server in SWG 7000 only.) Allows communication at a speed of up to 1GB with Auto- Negotiation enabled.

11

What to Prepare	Details
GE3 (eth3) 1GB - Auto-negotiation	(Available for SWG 5000, and the Policy Server in SWG 7000 only.) Allows communication at a speed of up to 1GB with Auto- Negotiation enabled.

3   Determine the IP address and netmask for the selected interface as IP/ (netmask/prefix), if you will not be using the default settings.

4   Determine the Default Gateway IP address.

5   Determine the hostname if you will not be accepting the current settings.

6   Determine the IP address for the DNS Server if you will not be accepting the current DNS configuration settings. Note: DNS configuration setting is mandatory.

7   Determine the DNS domain names if you will not be accepting the current settings.

8   Decide on any password changes if required.

3.2 Setting Up the Appliance

Perform the setup using the values you prepared.

1.   Log in to the Limited Shell. The default user name and password for the shell (command line) is admin and finjan respectively:

- For a physical machine, you can connect from a remote machine using an SSH client, serial cable, or by connecting a keyboard and monitor to the appliance.

- For a virtual appliance, connect through the vSphere client.

2.   Enter the **setup** command. The current configuration status is displayed.

```
   ---Configuration status---
Role                   : None
Time Zone              : None
Current date and time  : 2010-10-27 10:47
Interface              : None
IP Address             : None
Default gateway        : None
Hostname               : None
DNS server             : None
DNS search             : None

(B - go back, Enter - accept default values, Q - exit from setup)

   --Set Role--


1. All in One (Default)
2. SWG Remote Device
3. SWG Policy Server
> _
```

3.   Using the data you prepared, page through the setup script entering the needed values. This displayed configuration is updated as you enter values.

4 Performing Additional Configuration

(Optional) You can optionally use the commands of the Limited Shell to manage the functionality of the appliance, and to monitor the appliance closely.

Each appliance has different configuration needs, so there is no set procedure. Instead, enter the relevant Limited Shell commands and values.

Limited Shell commands are divided into two categories; Configuration commands and Monitoring commands.

This chapter contains the following sections:

- Limited Shell Commands — Summary List

- Limited Shell Configuration Commands

- Limited Shell Monitoring Commands

4.1 Limited Shell Commands — Summary List

The following monitoring and configuration commands are available:

Note: The A/C/M column indicates if the command is an Administration (A), Configuration(C), or Monitoring (M) command.

Command	A/C/M	Description
access_list	C	Enables/disables access list
arp	M	Displays the arp table
change_password	C	Change password
check_connectivity	M	Checks connectivity to the remote devices (for Policy server or All-in-One appliances)
config_ ...	C	Network or service configuration. Double tab to view the config_network, config_time, config_hardware, config_upgrade, config_support, config_psweb, config_exclude, config_bridge, and config_access_log commands.
df	M	Displays disk usage

Command	A/C/M	Description
disable_ ...	C	Disables service. Double tab to view the disable_service_snmpd and disable_service_ssh commands.
enable_ ...	C	Enables service. Double tab to view the enable_service_snmpd and enable_service_ssh commands.
ethconf	C	Menu interface to ethtool
flush_dnscache	C	Flushes the DNS cache
ifconfig	M	Displays NIC configuration and statistics
ip2name	M	Resolves IP to hostname
iptraf	M	Interactive IP LAN monitor
last	M	Displays last login
name2ip	M	Resolves hostname to IP
netstat	M	Displays Network statistics
ping	M	Sends ICMP ECHO_REQUES to network hosts
poweroff	A	Powers off the system
reboot	A	Reboots the system
reset_config	C	Sends full configuration to appliance
restart_role	A	Restarts the role
save_exclude_logs	M	Saves Exclude logs
save_support_logs	M	Saves Support logs
setup	C	Runs configuration setup
show_ ...	M	Shows system or service status. Double tab to view the show_bridge, show_config, show_network, show_service, show_dbsize, show_proxy_buffers, show_proxy_connections, show_route, show_time, and show_version commands.
supersh	A	Provides access to privileged shell
tcpdump	M	Dumps traffic on a network. Results files will be under sftp chroot/tcpdump_captures. Files can be downloaded using any sftp client

Command	A/C/M	Description
`top`	M	Displays Linux tasks
`traceroute`	M	Prints the route packets taken to network host (traceroute
`uptime`	M	Displays uptime
`vmstat`	M	Reports information about system usage (usage: vmstat,
`w`	M	Shows who is logged on
`wget`	M	Retrieves files using HTTP, HTTPS and FTP

For more information on configuring the system, refer to Limited Shell Configuration Commands. For further in-depth analysis and diagnostics of the system, refer to Limited Shell Monitoring Commands.

4.2 Limited Shell Configuration Commands

Limited Shell configuration commands enable you to define the role the appliance takes, the security, access and time settings, and also carry out routine maintenance operations. The configuration commands are also used to define how the network works, and how the appliance communicates with the network.

access_list

This feature is configured from the Management Console. The administrator can define a range of IP addresses to access Management applications on predefined ports (such as the Management Console, SNMP, SSH) or User applications on predefined ports (such as HTTP, FTP, ICAP) or System ports (internal ports). Any IP address not defined in the IP range will then be blocked from accessing these applications on the ports defined by Trustwave.

The access_list command is used to enable or disable the Access List and is useful for situations when due to a mistaken configuration, or other circumstances, you cannot access the Management Console, and want to disable the Access List feature.

Enter the access_list command and choose enable or disable.

change_password

Allows system administrators to change the Limited Shell's password. For security reasons, it is recommended to choose a password which contains both characters (higher case and lower case) and digits. It is also recommended to change the password frequently.

Enter the change_password command and confirm current and new passwords.

config_ ...

Enables network, service and Policy Server configuration. Press the tab button twice to display the config_network, config_time, config_hardware, config_upgrade, config_support, config_psweb, config_exclude, config_bridge, and config_access_log commands.

config_network

Allows system administrators to configure network parameters, such as the IP address(es), routing information, DNS parameters. Enter the config_network command.

The current network configuration is displayed (i.e. the DNS Search Domain, nameserver and Hostname configuration). A Name Server is a network server that provides a naming, or directory service. A prompt is displayed asking you if you would like to change the configuration. Enter y to change the network configuration.

Select an option from the following commands:

- **View**: This command allows you to view the current network configuration: The IP address assigned to each interface, the current DNS configuration and the current hostname configuration.

- **Interface**: Allows system administrators to modify interface related parameters such as: Add, Remove or Change an IP address from a physical interface; Add, Remove or Change routing information; Enable or Disable a physical interface.

    - Choose an interface, for example, 1 (eth0). The editing options are displayed.

    - Choose an editing action, for example, 1 (Change IP address). To add a static route, choose 4 (Add route). The new route must be input as 'IP/via prefix IP'. For example, 1.1.1.1/32 via 10.0.3

- **Gateway**: Allows system administrators to set the default gateway of the appliance. The IP address of the default gateway must be a local IP address. It is mandatory to configure a default gateway to the appliance.

    To change the current gateway configuration, enter the IP address.

- **DNS**: Allows configuring the DNS servers, which the appliance uses in order to resolve the hostnames to IP addresses. It is also possible to configure a search domain under the DNS settings which allows the appliance to complete the domain name (according to the configured value) in case the host name is not completed. For example, if the search is on http://mize and the search domain is TRUSTWAVE .com, the appliance will try to resolve to http://mize.M86Security.com.

IMPORTANT: It is mandatory to configure the DNS Server that has the ability to resolve external IP addresses

The current DNS configuration is displayed. Select an action, for example, 1 (change search).

- **Hostname**: Allows configuring the appliance hostname.

- **Hosts**: Allows configuring the host files.

config_time

Allows system administrators to set the system date and time, the time zone and also the NTP Server. To change a setting, type y. Select an option from the menu, else Q to exit.

config_hardware

This command allows the system administrator to configure an installed Caching Kit and/or Bypass NIC.

Note: Caching Kit is relevant to both physical and virtual devices. Bypass NIC is relevant only to physical devices.

When the command is entered, the screen displays the installation and configuration status of these two pieces of hardware.

To configure an installed piece of hardware, select the hardware option (**Caching Kit** or **Bypass NIC**) from the menu, and then enter **Y** to configure it. Select **Q** to exit.

config_upgrade

After upgrading the Policy Server to a new version, running this command will upgrade the scanners.

config_support

Allows you to install support packages.

config_psweb

Allows you to change the Policy Server management port for enhanced security. To change the Listening port for the Policy Server, add the new Port settings.

config_exclude

Defines bypass rules in intercepting proxy mode.

config_bridge

Configures intercepting proxy to work in bridge mode. In Bridge mode, only traffic that should be scanned will be processed. All other traffic will flow uninterrupted.

config_access_log

Enables or disables the access log.

disable_ ...

Disables the service. The disable command includes the disable_service_snmpd and disable_service_ssh commands.

disable_service_snmpd

Disables the snmpd network service. Enter the disable_service_snmpd command.

disable_service_ssh

Disables the ssh network service. Enter the disable_service_ssh command.

enable_ ...

Enables the network service. The enable command includes the enable_service_snmpd and enable_service_ssh commands.

enable_service_snmpd

Enables the snmpd network service. Enter the enable_service_snmpd command.

enable_service_ssh

Enables the ssh network service. Enter the enable_service_ssh command.

ethconf

Enables configuring the Network Interface parameters.

Enter the ethconf command and choose the required interface. Choose the required speed or select Auto-negotiation to enable the appliance to negotiate its own speed.

Enter the ethconf command and choose the interface, for example, enter 1 (eth1).

The settings for the selected interface are displayed.

Choose configuration for the adapter and confirm to make the settings permanent

> **Note:** According to the IEEE 802.3 standard, when working with 1000Base-T at a speed of 1000Mbps, auto-negotiation must be enabled. A fixed speed of 1000Mbps is not supported. For more information, refer to the 1000BASE-X Auto-Negotiation standard as defined in Clause 37 of the IEEE 802.3 standard.

flush_dnscache

Flushes the dns cache.

reset_config

Rebuilds the appliance configuration in extreme situations where the appliance, for whatever reason, was disconnected for a period of time. This action restarts the appliances and may take several minutes.

4.3 Limited Shell Monitoring Commands

arp

Address Resolution Protocol command — the standard method for finding a host's hardware address when only its network layer address is known. Enter the arp command to display the appliance's arp table.

check_connectivity

For Policy server or All-in-One appliance, checks connectivity to the remote devices.

df

Disk free command — a standard Unix command used to display the amount of available disk space for file systems.

Enter the df command to display the disk usage.

ifconfig

This Unix command is used to display TCP/IP network interfaces. Enter the ifconfig command to display configuration and statistics.

ip2name

Looks up the hostname associated with an IP address entered by the administrator. Enter the ip2name command followed by the IP address to display the associated hostname.

iptraf

This command is a Linux network statistics utility. It gathers a variety of parameters such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/ UDP traffic breakdowns, and LAN station packet and byte counts. Enter the iptraf command to display the IP traf options:

- IP traffic monitor

  - General Interface Statistics

- Detailed Interface Statistics

- Statistical breakdowns

- LAN station monitor

For example, select IP traffic monitor to display the IP traffic monitor details.

last
Displays a list of the previous administrators who logged on to the Limited Shell - including those still logged on.

name2ip
Displays the IP address associated with a given hostname. Enter the name2ip command followed by a hostname to display the associated IP address.

netstat
This command is a useful tool for checking your network configuration and activity. It displays the status of network connections on either TCP, UDP, RAW or UNIX sockets to the system.

ping
Use the ping command to check the network connectivity - for example after using netconf.

poweroff
Enables you to remotely shut down the appliance.

> **IMPORTANT**: Physical access to the appliance is needed to bring the system back online for all models except the 7000-SWG.

reboot
Enables you to remotely reboot the appliance.

restart_role
Restarts all role services.

save_exclude_logs

Saves Exclude logs in the Exclude directory.

save_support_logs

Saves Support logs in the Support directory.

setup

Assists you in setting up the appliance for the first time. It guides you to perform all the necessary steps to establish a working appliance. You can choose to rerun the Setup command to repeat the initial configuration commands at any time.

show_ ...

Shows system or service status. The show command includes show_bridge, show_config, show_network, show_service, show_dbsize, show_proxy_buffers, show_proxy_connections, show_route, show_time, and show_version.

show_bridge

Shows the Bridge role configuration.

show_config

Shows the current configuration.

show_network

Shows the current network configuration. This includes: defined interfaces, DNS configuration, DNS cache and current hostname.

show_service

Allows system administrators to view the service configuration status.

The following options are available:

- show_service_all: Displays the service configuration status for all the available services.

- show_service_snmpd: Displays the service configuration status for snmpd.

- show_service_ssh: Displays the service configuration status for ssh.

show_dbsize

Shows the file size of the data- bases connected with your appliance.

show_proxy_buffers

Shows the status of proxy buffers.

show_proxy_connections

Shows the status of proxy connections.

show_route

Allows system administrators to view the Kernel IP routing table.

show_time

Allows system administrators to view the time, date, time zone and ntp settings.

show_version

Allows system administrators to view the time, date, time zone and ntp settings.

supersh

Enables root access to the appliance. This command is reserved for Trustwave Support only.

tcpdump

Allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It writes all the information into a tcpdump file. This file can then be downloaded for further analysis. Up to 4 files of 100 MB each are kept. When the fourth file gets full, the first file is deleted (i.e.cyclic progression). SFTP, such as WinSCP, is required in order to download the files.

top

Displays all the running processes, and updates the display every few seconds, so that you can interactively see what the appliance is doing.

traceroute

Displays the route over the network between two systems, listing all the intermediate routers a connection must pass through to get to its destination. It can help you determine why connections to a given server might be poor, and can often help you figure out where exactly the problem is.

Performing Additional Configuration

uptime

Produces a single line of output that shows the current time, how long the system has been running (in minutes) since it was booted up, how many user sessions are currently open and the load averages.

vmstat

Reports statistics about kernel threads, virtual memory, disks, traps and CPU activity. Reports generated by the vmstat command can be used to balance system load activity.

w

Shows who is currently logged on and the current command they are running.

wget

Allows you to download web files using HTTP, HTTPS and FTP protocols.

23

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses thought the world. Trustwave analyzes, protects and validates an organization's data management infrastructure from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electric exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia, and Australia.