Secure Web Gateway Version 12.0 - Quick Start Guide

This Quick Start guide is designed to help install Secure Web Gateway (SWG) for the first time. It describes the basic tasks to get the proxy up and running, how to identify users and how to modify policies. It also introduces some basic troubleshooting techniques you may need.

This guide assumes a simple SWG architecture. It is **not** meant as an all-encompassing guide for day-to-day use. For more information, refer to the *SWG Help*.

Installation and configuration of the SWG appliance as outlined in the *SWG Setup Guide* is a prerequisite for this document.

Table of Contents

1 Connecting to the GUI

Connect to the GUI with a browser – point to the IP address using: https://<ip address>.
Ignore any certificate warnings at this time.

The SWG Login screen opens. The default credentials are:
Username: admin, **Password**: TrustwaveSWG

When logging in for the first time you will need to change the password from the default. To log back to the Console directly, use the updated password.

2 Licensing SWG

You must have an SWG trial or full license to proceed. Licensing for SWG is modular, so you need to decide in advance which Anti-Virus component, URL Database etc. to use:

- **Anti-Virus:** Choose from Sophos, McAfee, or Kaspersky

- **Other Modules:** Caching, HTTPS

Note that:

- When logging into SWG for the first time you will be asked to enter your license key.

- It can take several minutes for SWG to validate the license.

- You will be asked to accept the End User License Agreement (EULA).

- Trustwave constantly strives to adapt its products to evolving threats. This effort includes the collection of real life data from customers. Customers can choose to activate the Customer Feedback Module run by Trustwave SpiderLabs, and allow the collection of transaction data from their site. To participate, select the **Enable sending customer feedback information** check box. (To disable this feature, go to **Administration | System Settings | Administrative Settings** and deselect the check box). For more, see https://www.trustwave.com/support/customer-feedback-module.asp

Once these steps are complete, you will have access to the SWG Management Console.

Note that clicking the **Help** button 🌐 (or pressing **F1** on the keyboard) will open context-sensitive help relating to the currently displayed GUI section. Help content is online – you will need Internet connectivity to view it.

3 Introducing the SWG Management Console

3.1 Welcome Screen

The Welcome screen opens only at the first login after installation, or if the user does not have permissions to access the Home page.

This screen provides quick links to several frequently-used activities. You can also display these links in the Home page, if required.

3.2 Home Page

The Home page, or Application Dashboard, is the entry point to the Management Console UI. Home page data is dependent on the permissions of the current user.

The Home page is always accessible by clicking the Home icon [home icon] on the Management Console toolbar. You can arrange the Home page to suit your needs. This page can:

- Provide quick links to recent and frequently used activities in the Management Console.

- Indicate pending system updates and changes, both automatic and those requiring user action.

- Display the System Logs or some selected logs and reports.

3.3 Working with the SWG Interface
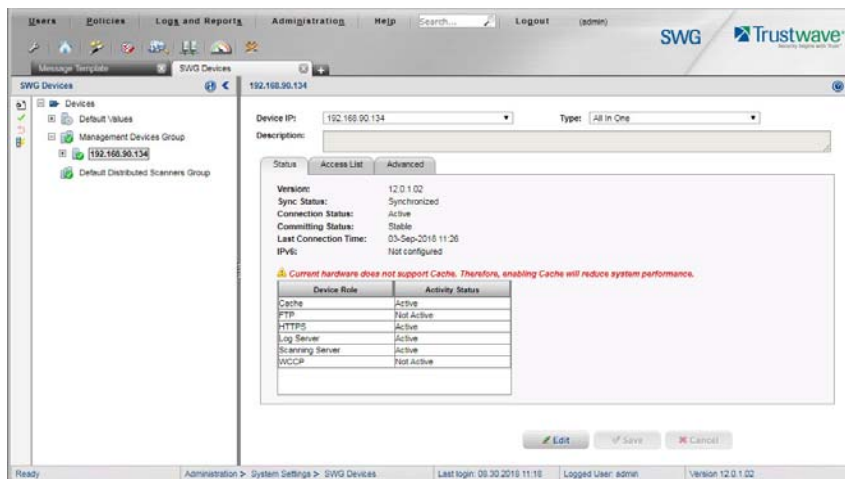
- **Right Pane** and **Left Pane:** Most sections of the SWG GUI display a Right Pane containing detailed information about the item selected in the Left Pane. Many definition/configuration windows in the right pane contain tabs, with each tab containing fields relevant to that tab.

- **Data Refresh:** Clicking the **Refresh** button [refresh icon] at the top of the left pane manually refreshes the GUI to display current information.

- **Quick-access icons:** Many tree panes have action icons to the left of the tree entries. You can select an entry in the tree, and then click the appropriate action icon. Pop-up tooltips provide a description of each icon. You can also right-click a tree item to open a context-sensitive menu.

- **Tabs:** Using tabs can save time when switching back and forth between commonly used areas of the GUI.
  Clicking the ![+] tab opens another window instance. By default, the Home page is displayed. You can navigate to another location in the new window.

- **Item Detail:** Some list screens have an icon ![] that displays the details of the item when clicked.

- **Editing:** Most windows used for editing provide **Edit**, **Save**, and **Cancel** buttons. Note that if you want to edit an existing definition, you must click the **Edit** button first; until you do, the definition fields are displayed in protected mode and cannot be modified.

- **Mandatory fields** appear in yellow when empty (or in some cases, if they contain invalid data). In multi-tab screens, if mandatory data is missing, the ![⚠] symbol appears at the top of the tab.

- **Commit Changes:** After defining or configuring a component and performing a **Save**, you must click **Commit Changes** ![] in the toolbar to synchronize the Policy Server and the scanners. If there are no changes to make, this icon is disabled.

- Windows that can contain long lists of information generally have a Previous/Next button to allow you to scroll. Some of them allow you to perform a search on a value.

- **Toolbar:** Click the toolbar icons to save time accessing commonly used functions. You can customize which icons are displayed by clicking the **Edit Toolbar Buttons** icon ![].

- **Status Bar:** The Status bar at the bottom of the Console shows the path to the currently displayed view. The Status Bar also provides information on system status, and login and version details.

- **Context-Sensitive Help:** Click the **Help** button ![] (or press **F1**) for help relating to the currently displayed GUI section. Note that Help content is online – you will need Internet connectivity to view it.

For more information, see the *SWG Help*.

4 Confirming Operations

4.1 Confirming Proxy Operation

To confirm that the Proxy is handling Web requests correctly:

1. Point a browser at the SWG. The default listening ports for SWG are 8080 and 8443 for HTTP and HTTPS respectively.

    Note: If using the same browser to access the SWG GUI and to test the proxy, you should exclude the IP of the SWG from proxying altogether.

2. Browse to some sites. The following test sites should trigger SWG default policies:

    - http://test.8e6.net: Blocked as Adult if using the Trustwave URL DB (actual content is safe for work)

    - https://www.trustwave.com/EVG/eicar.com.txt: Contains several forms of the harmless Eicar test virus. The HTTPS link can be used to confirm that HTTPS content scanning works correctly.

Is normal browsing working correctly? Are the above sites blocked by SWG?

3. Go to **Logs and Reports | Web Logs** to confirm normal operation or troubleshoot abnormal proxy behavior.

4.1.1 No Web Logs Visible

If you can access the Web via the proxy, but you see no Web Log entries, confirm that an appropriate logging Policy is enabled:

a. Go to Policies | User Policies | Logging.

b. Right-click Log everything except Image files and select Set as Default.

During initial setup and troubleshooting it is useful to log everything. Later, it may be advisable to revert to a Logging Policy that logs less information. This is both for performance reasons and to keep the Web Logs more usable by having fewer entries.

If you still do not see any Web Logs:

a. Double-check that you are actually browsing via the SWG.

b. Double-check your proxy settings in the browser.

c. Confirm that the SWG is operating as a normal explicit proxy:
    Go to **Administration | System Settings | SWG Devices**. Then, in the Devices tree in the Left Pane, expand the IP address and Scanning Server nodes and go to **General | Transparent Proxy Mode**. Confirm that the **Enable Transparent Proxy Mode** check box is not enabled.

4.2 Confirming Updates Work Correctly

If SWG does not receive updates it will not work correctly or at its best. It needs URL updates to apply any rules based on URL Filtering. Anti-Virus updates are also needed.

Only proceed to the next section when the updates are working correctly.

To ensure that the system is up to date, go to Administration | Updates and Upgrades | Management.

Note the tabs in the Updates and Upgrades Management screen:

- **Available Updates:** Available but not yet installed

- **Installed Updates:** Updates successfully downloaded and installed

- **Update Key:** Some customers use SWG in an isolated network that is not connected to the Internet. With a special license, you can download updates using an Offline Updates application.

To check for updates immediately, click **Retrieve Updates** in the **Updates and Upgrades Management** screen. If you have just configured Internet connectivity, and there are updates available, these should appear in the **Available Updates** tab.

> **Note:** There are options to enable an **Automatic Install** for the different types of updates; Security updates, Critical OS updates, and OS version updates. Click **Help** for more information.

4.2.1 Troubleshooting

If the Available Updates or Installed Updates tabs do not have any line entries, then updates are not being downloaded. There may be a problem with Internet access, or you may need to configure access via a proxy. To do this, go to **Administration | Updates and Upgrades | Configuration**.

To troubleshoot further, go to: **Logs and Reports | System Logs**. The System Logs should record the success or failure for update retrieval and installation.

5 Configuring Identification and Authentication

Identification policies define whether and how Scanning Servers identify end-users who are browsing via the Secure Web Gateway system. SWG has a number of pre-supplied Identification policies that use different mechanisms to perform Identification. If you choose an Authentication-type Identification policy, you must also define a Realm.

5.1 Configuring Identification Policy

View the various default Logging Policies available under **Policies | Device Policies | Identification**. The two of primary interest will likely be:

• **Get User Credentials:** Uses NTLM to challenge the browser for user details

• **Authentication:** Takes the additional step of checking the credentials against an Authentication Site (such as AD)

It is easiest to start off with **Get User Credentials** as it does not require you to set up any connection to your user directory at this time.

For more information on how to define and customize Identification Policy, see the *SWG Help*.

5.2 Implementing Authentication

Authentication is a type of Identification policy. When a scanning server is assigned an Authentication-type Identification policy, it matches user identifiers with available user credentials.

If you will be assigning a Scanning Server an Authentication-type Identification policy, you must configure Authentication parameters for that Scanning Server (for example, if and for how long to retain Authentication data). The actual set of parameters depends in part on whether the Scanning server is configured to work in Transparent Proxy mode or in Explicit Proxy mode.

For more information on how to configure Identification and Authentication, see the *SWG Help*.

6 Defining Security Policies

SWG provides a number of pre-defined policies for different purposes. A main purpose is setting security - determining how content is handled. Policies consist of three basic components: the **Policy** itself, **Rules**, which determine how to handle the content (for example, block or allow), and **Conditions**, which determine whether a particular rule is activated (for example, if a particular type of content is detected).

To view security policies, go to **Policies | User Policies | Security**.
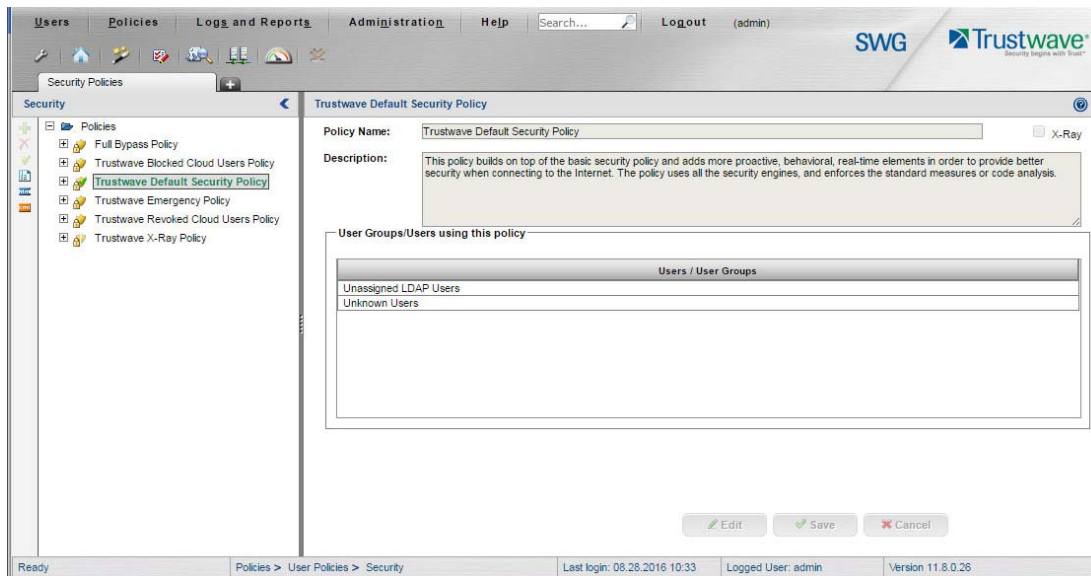
Note that all the policies have a padlock on the icon, indicating that each Policy is read-only. You cannot edit a pre-supplied Security Policy. However, you can duplicate a pre-supplied Security Policy and then edit the duplicate; you can also create a Security Policy from scratch.

Note the following Rule Properties:

- **Rule Conditions:** The components that must match in order for the rule to trigger.

- **Rule Actions:** The action taken if the rule triggers; Block, Coach (warn user), or Bypass.

- **Enable Rule:** Turns the Rule on or off.

- **Block Message:** Controls the text of the message seen by the end user.

If a default policy does not meet your needs, you can walk through the rules (of a duplicated policy) enabling and disabling rules and rule components as needed. Here are some key Rules to focus on:

- **Block Blacklisted, Spyware or Adware Sites:** View the rule conditions. Note that this rule blocks access to multiple URL lists, including one called Customer Defined Black List.

Go to: **Policies | Condition Elements | URL Lists**

Edit the URL list and add URLs that need to be blacklisted outright.

You may have an existing list of URLs that need to be blacklisted. If so, you can import these URLs into this SWG URL list. Right-click **Customer Defined Black List** and choose **Import to List**. Browse to your own URL List file.

- **Allow Trusted Sites:** You can maintain a URL list of trusted sites and have this rule bypass scanning for those sites. BE CAREFUL! Only add sites here that you trust completely. This rule will bypass all malware-related Rules, regardless of whether they come above or below this rule. (See Rule Order below.)

- Block Customer-Defined and Trustwave Recommended Site Categories: This rule requires some consideration.

This rule blocks all your chosen URL categories. You should walk through each URL Category in the URL Database and enable/disable as required. Note that a URL category such as Adult Content or Bandwidth has sub-categories which need to be reviewed. For more information on what each category name means, you can check the Trustwave Database Categories (applies to Trustwave URL DB Only).

- **Block Suspicious File Types:** This rule blocks a selection of file types deemed suspicious by SWG. You may need to modify this list if the selected files are unsuitable for blocking in your organization.

- **Block Suspicious Archives:** This rule blocks password protected archives. If this is not appropriate, modify the rule conditions accordingly.

For more information on how to define and customize Security Policies, see the *SWG Help*.

6.1 Rule Order

It is very important to understand how rules are evaluated, and how the order of rules works.

SWG regards each Web transaction as having a Request and a Response side. Rules are evaluated from the top down on the request side, and again from the top down, on the response side.

Conditions that are evaluated on the Request include URL Lists, URL filtering, File Extensions and so on. Conditions that are evaluated on the Response include all Anti-Virus and behavior analysis.

This has serious implications for Bypass rules. If a Bypass rule triggers on the Request, then it will bypass the entire Response evaluation. This is the reason that even a Bypass rule placed last in your Policy can bypass a Rule that is placed at the top, if that rule is evaluated in the Response side.

7 Enabling HTTPS Scanning

HTTP Policies define which HTTPS sites are fully bypassed, which are inspected, which request user approval to continue, and which are blocked. The blocking mechanism is based on Black Lists, URL categorization, and checking to see if Certificates have errors or comply with validation criteria.

You cannot edit a pre-supplied HTTPS Policy. However, you can duplicate a pre-supplied HTTPS policy or HTTPS Emergency policy and then edit the duplicate; you can also create an HTTPS Policy from scratch.

By default, SWG performs HTTPS scanning on all HTTPS traffic it receives on port 8443. If enabling HTTPS scanning for your users, note the following:

Certificate Roll Out
If you perform HTTPS scanning on Web traffic, the end-user will receive the certificate provided by SWG. If this is not made known to their browsers in advance, end-users will receive a certificate error. To avoid this problem, it is recommended that the certificate is pushed to desktops using Group Policy or something similar.

HTTPS Device Settings
Each Scanning Server has some advanced HTTPS Settings. The **Allow Certificate Wildcards** default setting should be changed; otherwise many legitimate sites will be blocked.

1. Go to Administration | System settings | SWG Devices.
2. In the Devices tree in the Left Pane, expand the IP address of the Scanning Server and go to **Scanning Server | HTTPS | Advanced** tab.
3. Ensure that the **Allow Certificate Wildcards** check box is enabled.

HTTPS and Web Logs
If the SWG receives a request on its HTTPS port (8443) it will be listed in the Weblogs in the Protocol column as 'HTTPS' .

If HTTPS traffic is sent by the browser to the HTTP port (8080), the protocol is listed in the Web Logs as 'HTTP Tunnel'.

8 Creating Custom HTTPS Policies

HTTPS policies focus on securing Internet Content on HTTPS sites. They provide the option to define which HTTPS sites are fully allowed, which are inspected, which request user approval to continue and which are blocked. The blocking mechanism is based on White Lists, URL categorization and checking to see if Certificates have errors or comply with validation criteria.

You cannot edit a pre-supplied HTTPS Policy. However, you can duplicate a pre-supplied Policy and then edit the duplicate; you can also create an HTTPS Policy from scratch.

To view the policies, go to: **Policies | User Policies | HTTPS**

Each policy contains one or more Rules, and each Rule has one or more Conditions. The main Condition Setting associated with HTTPS Rules is the **HTTPS Certificate Validation Profile**. You must edit this profile if you want to relax the default HTTPS policy (due to over-blocking, for example).

Go to: **Policies | Condition Elements | HTTPS Certificate Validation**

As with the Default HTTPS Policy, the default Validation Profile is read-only, and if you wish to edit you must duplicate it. If you do this, you must configure your HTTPS Rule to use the new Profile.

Another common HTTPS customization is to exclude certain sites from HTTPS scanning. To do this, add a bypass rule to your HTTPS Policy.

Add a URL List rule condition, and select your HTTPS Whitelist.

NOTE: There are two important HTTPS Policy issues to be aware of:

1) If you configure a Bypass rule in your HTTPS Policy, it will bypass all Security Policies that might come after. As such, you can't, for example, exclude a URL from HTTPS inspection with a bypass, and then block it with a URL Filtering Security Rule. Thus a site that is deemed an adult or porn site will not get blocked by the Security Rules, if that site has triggered an HTTPS bypass rule.

2) All HTTPS traffic reaching the SWG HTTPS port is inspected by default. Effectively there is a hidden rule at the end of the HTTPS policy which says 'inspect all traffic'. If specific sites or categories need to be excluded from HTTPS inspection, you will need an explicit Bypass rule to do so.

For more information on how to define and customize HTTPS Policies, see the *SWG Help*.

Legal Notice

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

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: tac@trustwave.com

Trademarks

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than 2.7 million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is a privately held company, headquartered in Chicago, with customers in 96 countries.

For more information, visit https://www.trustwave.com.