



USER GUIDE

Secure Web Gateway Cloud

June 2019

Legal Notice

Copyright © 2019 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave.

While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

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

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Revision History

Version	Date	Changes
1.0	December 7, 2018	Initial Release
1.1	January 10, 2019	Added formatting suggestions for user and group names
1.4	April 2019	Added Sandbox feature
1.5	June 2019	Added Firewall Redirect and Enterprise WiFi location types

Formatting Conventions

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

Table 1: Formatting Conventions

Formats and Symbols	Meaning
<u>Crimson Underline</u>	A crimson underline indicates a hyperlinked Web site or e-mail address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and checkbox names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in <code>Courier New</code> indicates computer code or information at a command line.
<i>Italics</i>	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 Cautions



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.

Table of Contents

Legal Notice	ii
Trademarks	ii
Revision History	iii
Formatting Conventions	iv
Notes, Tips, and Cautions	iv
Table of Contents	v
List of Tables	8
About This Document	9
1 Introduction	10
1.1 Preparing for SWG Cloud	10
1.2 SWG Cloud Provisioning Workflow	11
1.2.1 The Standard Workflow	11
1.2.2 The Advanced Workflow	11
1.3 Security Assertion Markup Language (SAML)	12
2 Quick Setup	13
3 Content Controls	14
4 Configuration	16
4.1 Settings	17
4.1.1 General	18
4.1.1.1 Time Zone and Language.....	18
4.1.1.2 MSC Related Options	18
4.1.1.3 Decryption Options.....	18
4.1.1.4 Safe Search.....	19
4.1.1.5 Default Optional Message	19
4.1.1.6 Username Domain	19
4.1.1.7 Trusted URLs.....	20
4.1.1.8 No Decrypt URL Categories	20
4.1.1.9 No Decrypt URLs	20
4.1.2 Identification.....	21
4.1.2.1 Location	21
4.1.2.2 SAML Configuration	21
4.1.2.3 User Agent.....	21

4.1.2.4	URL List.....	21
4.1.3	Advanced.....	22
4.1.3.1	Mobile Security Client.....	22
4.1.3.2	URL Lists	23
4.1.3.3	PAC	23
4.1.4	Quota	23
4.2	Rules.....	24
4.2.1	Actions	25
4.2.2	Time Frames.....	26
4.2.3	Comment	26
4.3	Locations.....	26
4.3.1	Add or Edit a Location	27
4.3.2	Add Stipulations or Restrictions to the Location	28
4.4	Users.....	28
4.5	Groups	30
4.6	Policies.....	31
4.6.1	URL Categories	32
4.6.2	Rules.....	34
4.6.3	Security Engines.....	35
4.7	Categories.....	35
4.7.1	Create a New Sub-Category.....	36
4.7.2	Add a or edit a URL in a Sub-Category	36
4.7.3	Add or Edit a Keyword in a Sub-Category.....	36
4.8	Quotas	37
4.9	Sandbox.....	38
4.9.1	Create or edit a Sandbox Profile:.....	39
4.9.2	View Sandbox Results	39
4.10	End User Messages.....	40
4.11	URL Lists.....	41
4.12	Time Frames.....	43
4.13	App Profiles.....	44
5	Policy and Rule Precedence.....	46
5.1	Line Item Exceptions	46
5.2	Named Policy.....	46
5.2.1	Out of Office Policy.....	47
5.2.2	Policy Node.....	47
5.3	Priority.....	47
5.4	Inheritance	48
5.4.1	Prohibit Override	48
5.5	Hierarchy.....	48
5.6	Identity.....	48
5.6.1	Testing Rules for Identity.....	49
5.6.2	Applying the Identity Basic Principle to Time Rules	49
5.7	Specificity.....	50
5.7.1	Testing Arguments for Specificity	50

5.8 Stopping Logic	51
6 Policy Test	53
6.1 Start with a Simple Test	53
6.2 Tests for Complex Rules and Policies	54
7 Cloud Downloads.....	55
7.1 Mobile Security Client	55
7.2 PAC File	57
Appendix A: List of Provided Web Site Categories.....	58
Appendix B: List of File Content Types.....	77
Appendix C: Application Control User Actions	87
Appendix D: User Agents.....	93
About Trustwave®	94

List of Tables

Table 1: Formatting Conventions	iv
Table 2: Configurations of SWG Cloud	16
Table 3: Common user interface controls	17
Table 4: Rule Types	24
Table 5: Actions by Rule Type	47
Table 6: Supported Versions of Platforms and Operating Systems	56
Table 7: Amazon Drive	87
Table 8: Apple iCloud Drive	88
Table 9: Box	88
Table 10: Dropbox.....	89
Table 11: Facebook.....	89
Table 12: Google Drive	90
Table 13: YouTube.....	91
Table 14: LinkedIn.....	91
Table 15: Microsoft OneDrive	92
Table 16: Twitter.....	92
Table 17: Predefined User Agent regular expressions and groupings	93

About This Document

Trustwave Secure Web Gateway Cloud (SWG Cloud) is a cloud-based web gateway that monitors client traffic, blocks malicious activity, and controls user access according to a policy you set. SWG Cloud is managed through Trustwave's TrustKeeper Platform.

Customers can quickly configure basic SWG Cloud connections and rules using the Quick Setup wizard in the SWG Cloud Platform application. The Quick Setup is covered in the *Trustwave SWG Cloud Getting Started Guide*.

This document provides a detailed description of the configuration settings for SWG Cloud available in the Platform.

1 Introduction

Trustwave Secure Web Gateway Cloud (SWG Cloud) provides advanced protection against malware and modern threats such as exploit kits and drive-by downloads in real time. It uses behavior-based malware detection engines for secure web browsing. SWG Cloud scans both inbound and outbound web traffic and provides:

- Real-time blocking of dynamic, new, obfuscated or encrypted malware
- Web filtering for acceptable use policies
- Granular control of web-based applications such as social media and cloud storage
- Ability to block uploads to known bad actor sites, malware command and control site, and prevent certain types of data from being removed from your organization.
- Protection against known malware via an included antivirus engine. It also decrypts and inspects SSL encrypted web traffic and inspects SSL certificates.
- Reporting on web browsing and security policy enforcement

1.1 Preparing for SWG Cloud

Before you can configure SWG Cloud, first consider what sort of traffic it should admit to your organization. Are certain categories of Web traffic off limits? Are some categories allowed to specific employees or groups or to the entire organization but only during certain time periods? Are yet other categories completely allowed? Consider carefully who should have access to what and when. See appendix A for SWG Cloud's list of Web categories.

Write these rules down. Be specific about who each rule applies to, what information (category of Web traffic or URL) is allowed or blocked and when the rule should be enforced. If possible, include the business purpose for the rule. This will help you refine the rule later.



Tip: Think in terms of who, what, where, when, and why. For example: "The entire company should not be able to access Shopping sites during business hours except for the office managers so that they can order office supplies."

If there are any conflicts in your rules, such as a case where two or more rules may apply, SWG Cloud will resolve these conflicts by applying common-sense principles. To avoid potential conflicts, craft your policies from the most general case (the default company policy) to the specific (individual users.) Carefully consider what order or precedence your LDAP groups should take. For an explanation on policies, rules, and their precedence; see chapter 4.

Finally consider how you want to customize SWG Cloud's default policy. This global policy is the basis for all policies in SWG Cloud. It blocks all websites that Trustwave places in its Security category, has a default end user message, and default Security Engines settings. You can change any part of this policy except for its Security Engines settings.

1.2 SWG Cloud Provisioning Workflow

After Trustwave has received your order for SWG Cloud service, Trustwave's delivery team assigns you access to SWG Cloud in the Management app. Then you can configure SWG Cloud in one of two ways:

- **Standard:** Ideal for most customers. This workflow modifies SWG Cloud's default policy and creates customizations for individual users, groups, and locations.
- **Advanced:** Intended for customers who want to build their own policies (called *named policies*) and modify the default policy.

1.2.1 The Standard Workflow

1. Quick Setup wizard – Configure your SWG Cloud account and define basic policies for your organization. See chapter 2 and the *Trustwave SWG Cloud Getting Started Guide*.
2. Content Controls – Select which categories and websites your organization should have access to. See chapter 3.
3. Configuration – Create rules for users, groups, and locations:
 - a. For users, see section 4.4.
 - b. For groups, see section 4.5.
 - c. For locations, see section 4.3.
4. Policy Test – Check that the policies you have created do what you expect, by testing them against possible identities such as users, groups, locations, and your website. See chapter 5.
5. Cloud Downloads – Download and install the Mobile Security Client or use the PAC file to enforce SWG Cloud policies in your organization. See chapter 6.

1.2.2 The Advanced Workflow

1. Quick Setup – Create basic policies for your organization. See chapter 2 and the *Trustwave SWG Cloud Getting Started Guide*.
2. Content Controls – Select which categories and websites your organization should have access to. See chapter 3.
3. Configuration – Use the Configuration pages to create named policies, rules, and configurations.



Tip: Trustwave recommends that that you create and use named policies for most situations. Only use rules for unique circumstances.

- a. Create custom app profiles (section 4.12), end user messages (section 4.9), quotas (section 4.8), time frames (section 4.11), and URL lists (section 4.10).
- b. Customize categories for your organization. See section 4.7.
- c. Alter the default policy which is applied to the entire company. See section 4.6.
- d. Create named policies. See section 4.6.
- e. Assigned names policies to users (section 4.4), groups (section 4.5), and locations (section 4.3).
- f. Customize settings. See section 4.1.

4. Policy Test – Check that the policies you have created do what you expect, by testing them against websites and IP addresses. See chapter 5.
5. Cloud Downloads – Enforce your SWG Cloud policies in your organization. See chapter 6.

1.3 Security Assertion Markup Language (SAML)

SAML is the preferred method to authenticate users for SWG Cloud. SAML is an XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider (IdP) and a Service Provider (SP).

SWG Cloud supports the SAML 2.0 single sign-on standard to integrate with directory services/user accounts, provide a secure way to authenticate users, and apply specific user and group policies.

User groups can be used to enforce policies if the chosen authentication method supports passing groups to the service. Where a user is a member of more than one group, you can determine which groups policies should apply first.

The authentication methods that pass group information are third party SAML services that support this feature and chained proxies performing authentication with `X-Authenticated-Groups` enabled. SWG Cloud also provides a Mobile Security Client (MSC) that provides access to LDAP groups.

During setup, you must give details of the SAML provider that you plan to use for integrated authentication (if any).

Preferred IdPs are Ping Identity, Shibboleth, and Microsoft Azure Active Directory. However, any SAML 2.0 compliant service can be used.



Note: For other services, Trustwave may require configuration details and testing.

Small companies (fewer than 100 users) that do not use a third-party SAML service can opt to use Trustwave SAML. Trustwave SAML is a Trustwave-managed service and does not integrate with any other directory services. Usernames and passwords are specific to the service.

2 Quick Setup

This page provides a step by step wizard that gathers the required settings for a customer's SWG Cloud instance. For details, see the *SWG Cloud Getting Started Guide*. All items set in Quick Setup can also be managed from the Configuration section.



Caution: When you run the Quick Setup wizard, if you do not click **Complete**, the Trustwave Platform saves your settings as a draft. If you continue the Quick Setup wizard later, the Platform retrieves these draft settings. In this case if you save the result of the continued Quick Setup, any configuration changes you made on other pages will be overwritten.

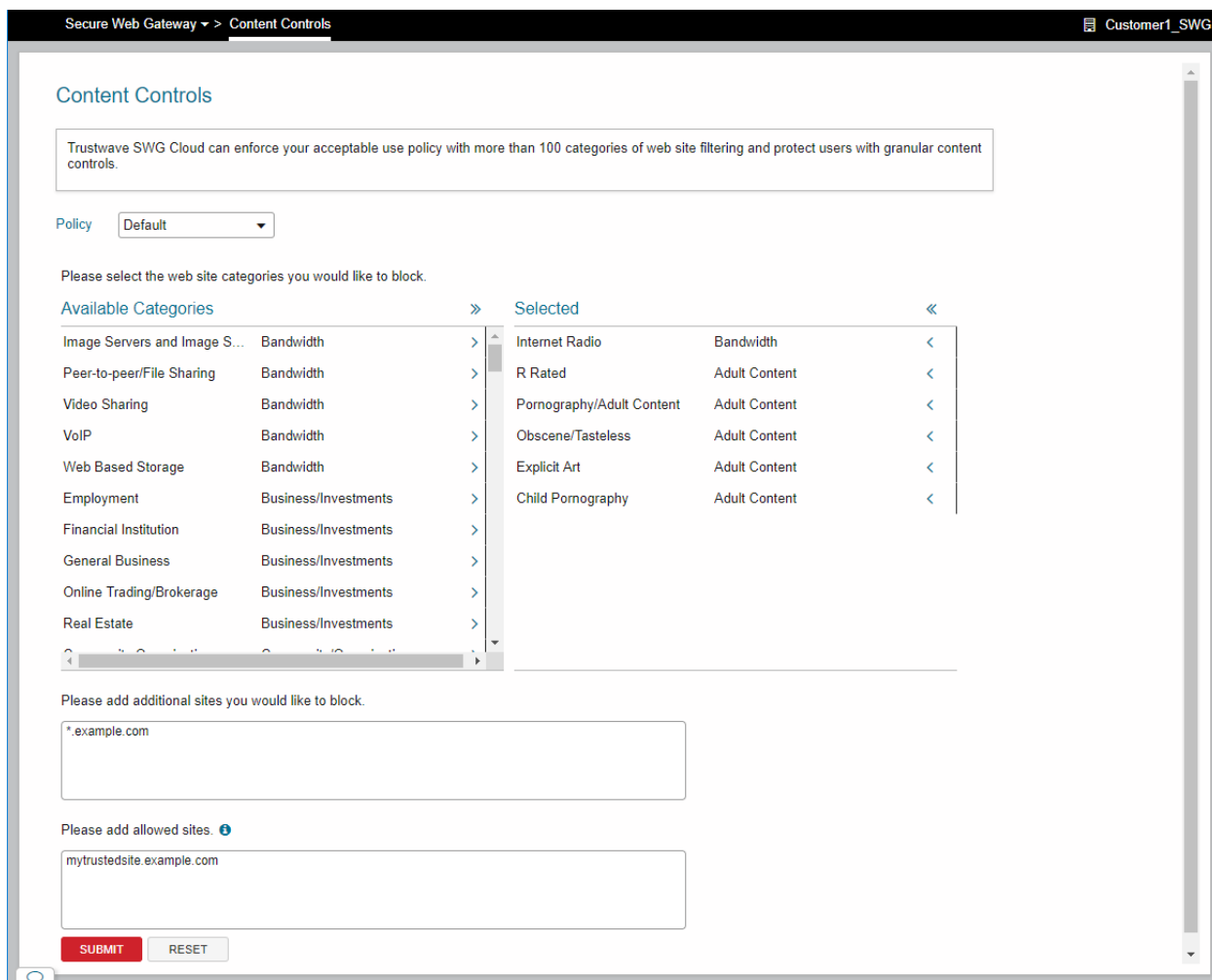
If a Quick Setup draft was saved, you can click **Discard** to delete the draft and load the current settings.

3 Content Controls

Trustwave SWG Cloud uses more than 100 categories of websites to filter the content of your company's Web traffic. You can select which of these content categories should be blocked from your organization by default and in additional policies (see below). When a category is blocked, then all websites and URLs associated with that category are inaccessible through SWG Cloud.

SWG Cloud also offers more granular control. You can block or permit access to specific websites and URLs by default and in additional policies. This individual access overrides any access that the URLs inherits from its category. For instance, if a casino uses SWG Cloud, they can block access to URLs in the Gambling category but allow access to their company website.

Access to categories and websites is defined in policies. You can view which categories and websites a policy blocks on the **Content Controls** tab. To view what categories and websites a policy allows, select the policy in the first dropdown list. The **Selected** list shows categories that are blocked by the policy. The fields below **Available Categories** list which websites are singled out for specific access.



To change the content control list of a SWG policy:



Note: If your login can be used to configure more than one Customer, select the correct customer at top right of the page before making changes on this page.

1. In the **Policy** drop down list, select the policy you want to configure.
2. To block access to a category, in the **Available Categories** list, click the arrow to the right of the category you want to block.



Note: Trustwave maintains and updates these categories frequently. See Appendix A for descriptions of these categories.

3. To block all categories, click the **Select All** double arrow at the top of the **Available Categories** list.
4. To permit access to a category of websites, in the **Selected** list, click the arrow to the right of the category you want to allow.
5. To allow access to categories, click the **Remove All** double arrow at the top the **Selected** list.



Tip: To work with Categories in more detail, see **Configuration | Categories**. Categories shown on this page are known as Sub-Categories in the Configuration section.

6. To block specific websites, enter the URL of each website in the first field beneath the **Available Categories** list. Enter one URL per line.
7. To allow specific websites, enter the URL of each website in the second field beneath the **Available Categories** list. Enter one URL per line.



Tip: You can import bulk lists of URLs to these fields in **Configuration | URL Lists**. See section 4.10 for more details.

8. To reset the lists, click **Reset**.
9. Click **Submit** to apply the changes. Your changes cannot be reset anymore.

4 Configuration

Instead of or in addition to the Quick Start wizard, you can create policies and configurations that are finely tuned to your organization. These policies can be as detailed as your organization requires to define access permissions or restrictions.

SWG Cloud evaluates the permission or restriction for each client request in a defined order. Essentially, exceptions or special cases are checked first, followed by more general cases like named policies. The default policy applies where no other permission or restriction is set.

Because SWG Cloud provides many options, the order of evaluation is complex. For full details, see Chapter 5.

SWG Cloud's configurations are organized into groups listed in the table below. In general, these configurations are not hierarchical. However, there are some dependencies you should be aware of before you customize any configurations.

Table 2: Configurations of SWG Cloud

Configuration	Description	See section	Dependencies
Settings	Basic configuration, SSL options, client identification, quota settings, and other details	4.1	End user messages
Locations	Network locations and location-specific rules	4.3	Policies
Users	User-specific policies, rules, and settings	4.4	Policies
Groups	Group-specific policies and rules	4.5	Policies
Policies	Usage policies, including URL categories, rules, and security engine messages	4.6	Categories & time frames
Categories	Sub-categories and ability to add custom URLs and keywords to a category	4.7	None
Quotas	Usage quotas you can apply to Sub-Categories	4.8	None
Sandbox	Sandbox profiles used to define sandbox behavior for specific file types	4.9	None
End User Messages	Text messages and policy URL links for use in policies and rules	4.10	None
URL Lists	Lists of URLs for use in policies and rules	4.11	None

Time Frames	Time periods for use in policies and rules	4.12	None
App Profiles	Application control profiles used to limit user abilities in common web-based applications	4.13	None

To set these configurations, first create any categories, app profiles, end user messages, quotas, sandbox profile, time frames, or URL lists that you may need for your policies and rules. Next create any custom policies that you want to apply or users, groups, or locations.

To access any of these configurations, select the item you want on the **Configuration** page.



Caution: If you can configure multiple customers in TrustKeeper, choose the customer you want to configure before you begin by selecting that customer in the **Customers List**. The customer selector at the top right of the page does not affect the Configuration pages.



Important: On all **Configuration** pages, click **Submit** or **Save Configuration** to save your changes to the pending state. To apply or discard pending changes, click **Pending Changes** at the top right of the page.



The configuration interfaces use many common controls.

Table 3: Common user interface controls

Icon	Action
	Add item
	Edit selected item
	Delete selected item(s)
	Note: In most cases you cannot delete an item until you have committed it. If you do not want to add a pending new item, discard it from pending changes
	View details. This icon appears next to list items. Often, you can also see details of a list item by selecting it or by clicking the Details bar at the right of the window.
	Refresh list
	List checkboxes: select one or more items, and then perform an action

4.1 Settings

On this page, you can set many basic and advanced options. You can use the Quick Setup menu for a simpler way to control many of these options. Trustwave has chosen reasonable default values for the settings. Consider carefully before making changes.

Some settings marked  are **inherited** from the Trustwave default policy. You can choose to set a specific value for these items by selecting  **override**.



Notes:

- Most of the fields and controls in this section use the common user interfaces or standard fields. The instructions assume users are familiar with standard web navigation and data entry.
- Click **override** and SWG Cloud enables an empty field, then the default field is empty. You have not deleted any settings.
- Remember to click **Submit** or **Save Configuration** to save your changes to the pending state, and then apply or discard pending changes by clicking **Pending Changes** at the top right of the page.

4.1.1 General

This tab allows you to set options for Time Zone, Language, HTTPS decryption, trusted URLs, username domain, MSC, and Safe Search.

4.1.1.1 Time Zone and Language

Time zone is the default setting for evaluation of Time Frames. Users and locations can be assigned separate time zones.

Language affects the display in the Platform.

To change time zone:

1. Click **x** on the existing setting to remove it.
2. Start typing to see available options.
3. Select an option.

To change language:

1. Click **x** on the existing setting to remove it.
2. Start typing to see available options.
3. Select an option.

4.1.1.2 MSC Related Options

These settings allow you to control the default options for MSC. Users and groups can be assigned other options.

1. To enforce use of the MSC by preventing the user from disabling MSC on a computer, click **Prevent Disabling MSC**.
2. To enable automatic upgrade of the MSC client, click **Enable Automatic Client Upgrade**.

4.1.1.3 Decryption Options

Allowing SWG Cloud to decrypt HTTPS enhances the ability to check for malware and enforce content policies like DLP. Where personal privacy is a concern, you could choose not to decrypt. In addition to the options described here, see the No Decrypt URL Categories and No Decrypt URL lists below.

1. To prevent decryption of HTTPS, check the box **Don't Decrypt HTTPS**.
2. To prevent decryption of HTTPS only from MSC clients, check the box **Don't Decrypt HTTPS Mobile**.



Note: You can also prevent decryption based on location. See the **Location** section.

4.1.1.4 Safe Search

This option allows you to enforce Safe Search for Google by rewriting the requests.

- To enable enforcement of **Safe Search**, check the box.

4.1.1.5 Default Optional Message

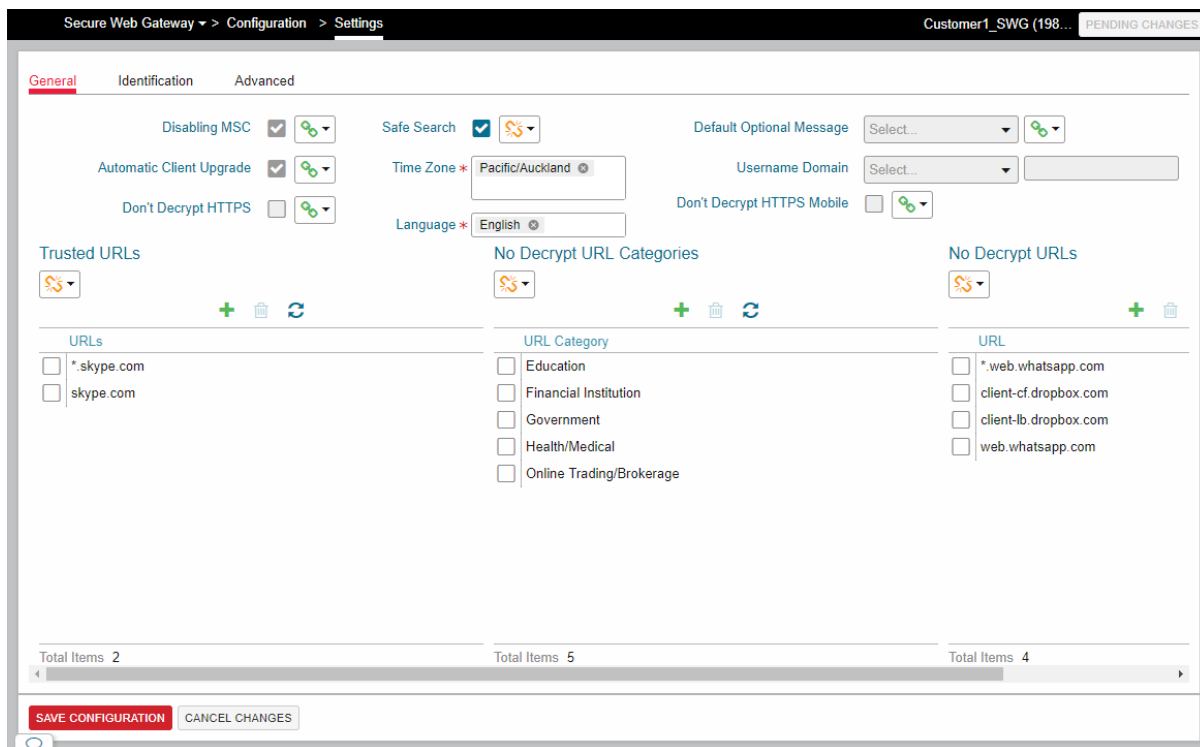
This option allows you to set a default welcome message for users. Before selecting a custom message, you must create it in **Configuration | End User Messages**.

- To select a message, choose it from the menu.

4.1.1.6 Username Domain

To enforce user-based controls, you may need to fix up domain information that could be provided in different formats by different providers. By default, this field is empty.

1. When you override the default option you can select from the following:
 - a. **No Change:** pass the username as received. For example, if you have users in more than one Windows domain that may have the same user part such as JSMITH, you may need to use this option.
 - b. **Fixed Domain:** enter a domain name in the field. All user names will be rewritten to use this domain.
 - c. **Remove Domain:** remove the domain part from the received user name. For example, if you have users in different domains but all users are uniquely named, you can use this option to normalize the entries.



4.1.1.7 Trusted URLs

Use this section to maintain a list of URLs that will be excluded from all checking and filtering. The Domain and path parts are supported. The wildcard * is supported at the start of the domain part. The URL must not contain a protocol part such as http://

1. Add or remove URLs from the list of Trusted URLs.
2. You cannot edit a URL in this list. You must delete and re-create it.

4.1.1.8 No Decrypt URL Categories

Use this section to maintain a list of URL categories that will be excluded from HTTPS decryption.

1. Add or remove Categories from the list.
2. Select available Categories using the menu.

4.1.1.9 No Decrypt URLs

Use this section to maintain a list of URLs that will be excluded from HTTPS decryption. The Domain and path parts are supported. The wildcard * is supported at the start of the domain part. The URL must not contain a protocol part such as http://

1. Add or remove URLs from the list of No Decrypt URLs.
2. You cannot edit a URL in this list. You must delete and re-create it.

4.1.2 Identification

This tab allows you to configure the information that allows SWG Cloud to recognize requests from your organization.

4.1.2.1 Location

Shows a list of the locations that have been configured. For more about locations, see **Quick Setup or Configuration | Locations**.

1. To add a location, click the **Add Location** icon above the **Locations** list. This action navigates away from **Settings** to the **Locations** window **Configuration | Locations**.
2. To specify that the location is used to identify the source of requests, check the box **Identification**.
3. To indicate that the location is a proxy server that re-transmits requests from clients and can provide authentication details via x-authenticated headers, check the box **Proxy Chaining**.

4.1.2.2 SAML Configuration

Shows the SAML identity information that has been configured (if any) and allows you to enter or edit the information.

1. To begin entering information, type a company name recognized by the IdP.
2. Enter the password required.
3. Paste the metadata provided by the IDP
4. Use the buttons to copy **SP Metadata** (internal) and **Mobile SP Metadata** (external) for entry to the IdP site.

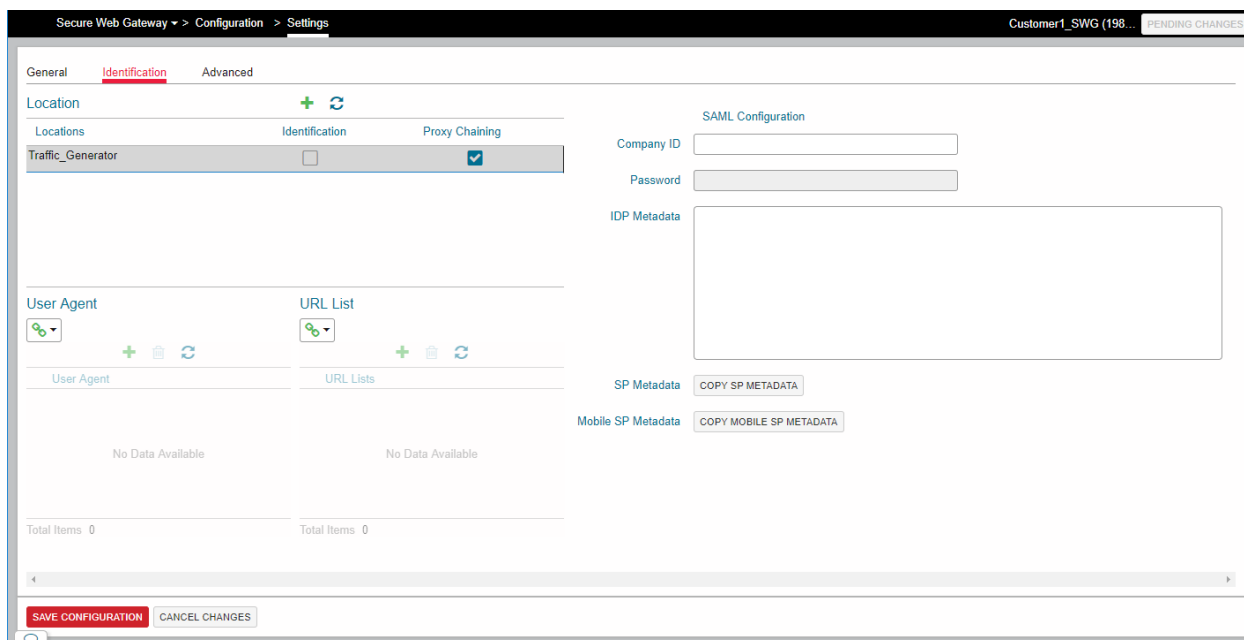
4.1.2.3 User Agent

The User Agent list allows user agents that are not SAML compliant to bypass the SAML authentication, so those agents can work. For each agent, enter a string that can be matched for identification. Copy the string from the application.

4.1.2.4 URL List

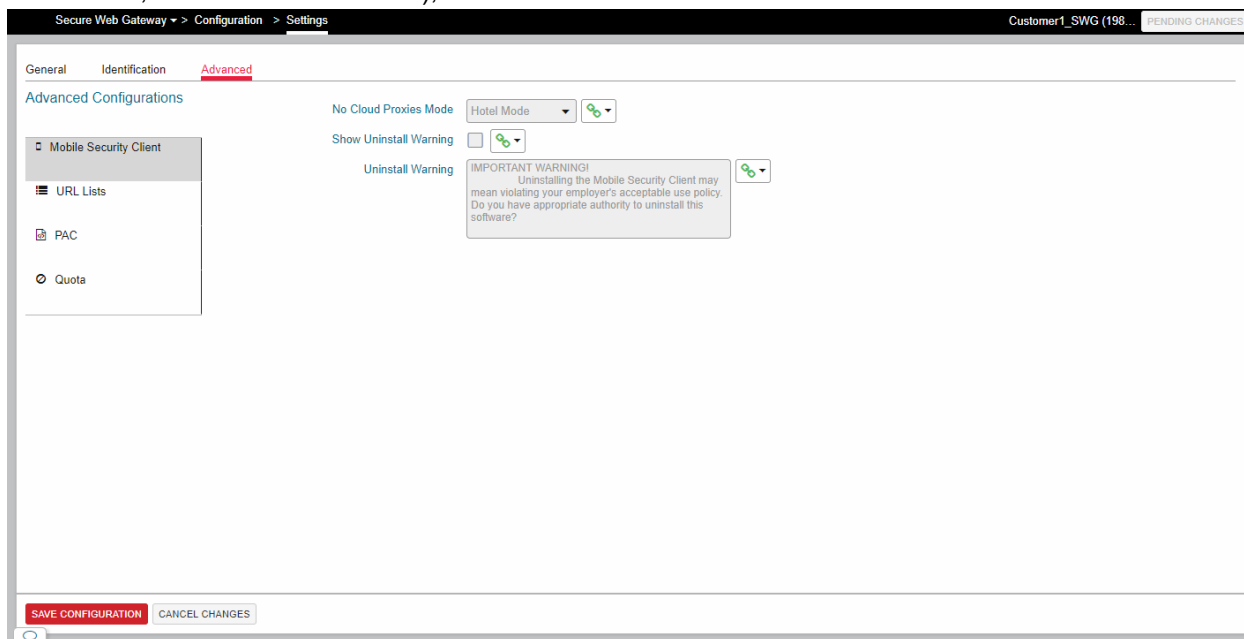
The URL List allows you allow to identify URLs that are not SAML compliant which may bypass the SAML authentication, so those your users can reach those URLs.

1. Select lists using the menu. To create URL Lists, see **Configuration | URL Lists**.



4.1.3 Advanced

This tab allows you to configure advanced options for MSC, URL lists (SSL certificates, Digital Certificates, Don't Scan Containers), and PAC file customizations.



4.1.3.1 Mobile Security Client

- To control MSC behavior when the client cannot contact the cloud service, select an option:
 - Fail Close:** deny network access
 - Fail Open:** allow Internet access unfiltered

- **Hotel Mode:** allow local network access for a short period. This mode allows the user to complete registration with a Wi-Fi network that requires registration on a local web page (commonly found in hotels)
2. Select whether to show a warning when uninstalling (if uninstall is permitted).
 3. Enter text of the warning to show.

4.1.3.2 URL Lists

The lists in this section are used to control SWG behavior in detail.

- To allow access to some sites even if the SSL certificate is not valid, add URLs to the **Ignore SSL Certificates** list.
- To allow access to software that has an invalid Digital Certificate, add URLs to the **Ignore Digital Certificates** list.
- To bypass scanning of containers (such as archives), add URLs to the **Don't Scan Containers** list.

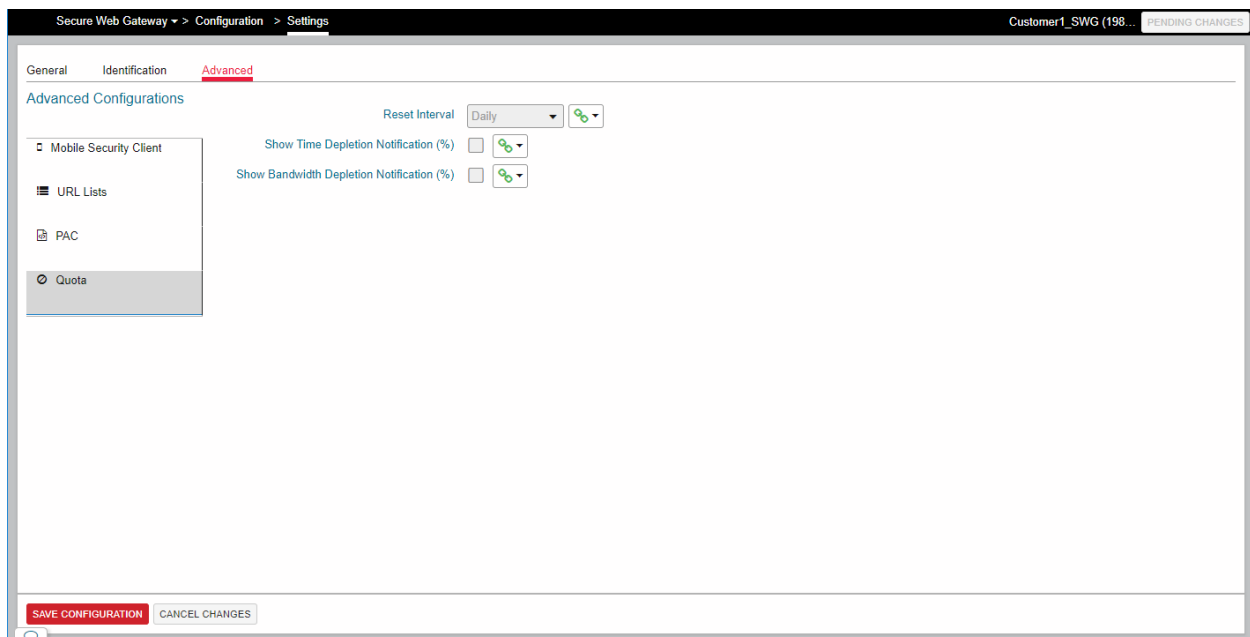
4.1.3.3 PAC

Enter text in the fields in this section to customize the SWG Cloud PAC. A default PAC is generated automatically. The full PAC is available for download on the **Cloud Downloads** page.

4.1.3.4 Quota

This section allows you to choose the reset interval (daily or monthly), for quotas.

To notify users they have used a percentage of their quotas, check either or both boxes and then enter a number between 1 and 99 for each to set the percentage.



4.1.3.5 Other

This section includes two settings:

- **Block Password-protected Files:** Allows you to choose whether to allow files that are passworded and so cannot be scanned. Default: True (password-protected files are blocked)
- **Allow complex archives:** Allows you to choose whether to allow archive files which have more than five levels, or which contain more than 2000 items. Scanning these files will have an impact on performance. Default: False (complex archives are blocked).

4.2 Rules

SWG Cloud Rules allow you to manage permission conditions and actions easily. For example, you can allow all requests to a URL (like www.trustwave.com/support) or block all requests for a file by extension (like `.com`). You can apply rules at some times of day or on some days of the week. Rules can be created and applied as part of many configuration items including users, groups, locations, and policies. This section lists the options available in Rules. Not all options can be used in all rule types.

The **Add Rule** or **Edit Rule** window uses standard fields and menus. Remember to click **Submit**, and then save and apply the changes in the parent window.

Most rules include actions and time frames. The table below lists additional options for some rule types.

Table 4: Rule Types

Type	Purpose	Options
Application control Profile	Take action if the request matches a pre-defined application control action	Select a profile from the menu. Optionally select an additional user message (created in Settings End User Messages).

Type	Purpose	Options
Content Size	Take action if the content is over a certain size	Enter the file size in KB.
Custom Application Control	Take action if the request is for a specific application action.	Enter the application name, and the item/action name. For a list of applications and items, see Appendix C.
Custom URL	Take action if the request is for a specific URL	Enter the URL.
DLP	Take action if the content matches a DLP profile. Optionally restrict the rule by the destination URL	Select a profile name. Optionally enter a URL destination. Destinations can have a wildcard * at the left, and can include a path part, but cannot include a protocol part. TODO link to explanation of the profiles.
File Extension	Take action based on the file extension of the returned content.	Enter a file extension.
File Extension Group	Take action based on presence of the file extension (of the returned content) in a pre-populated group.	Select a group.
File Type	Take action based on the file type of the content returned. File type is determined by the internal structure of the file	Select a file type.
Quota	Take action based on the quota status for a particular quota	Select a quota.
Sandbox	Take action based on a specified sandbox profile	Select a Sandbox Profile.
URL Category	Take action based on presence of the URL requested in a Trustwave-maintained URL category	Select a URL category.
URL List	Take action based on presence of the URL requested in a URL List	Select a URL list.
User Agent	Take action based on the User-Agent string of the request	Enter the User-Agent string.

4.2.1 Actions

Most rules allow you to select from the following actions:

- **Whitelist:** The request is explicitly allowed. This action is available only for URL lists.
- **Allow:** The request is permitted. SWG Cloud does no further evaluation.

- **Block:** The request is denied. This action is final. No further rules or other blocking configuration will be checked. Block rules normally result in display of a user message, and you can select an **optional message** (created in **Settings | End User Messages**).
- **Coach:** The request is interrupted with a message that the user must accept to proceed. The message is generally a warning or suggestion (“Are you sure?”).



Note:

- For Enterprise WiFi location filtering, some requests may be approved without fully passing through the rules engine. Such requests will not trigger a Coach message even if they would otherwise trigger one.

-
- **Pass:** The request is not denied by this rule. Evaluation of the request continues with other rules and blocking configuration. This action is rarely used.
- **X-Ray:** The request is passed but is also logged with information about how it would have been handled if blocked. This action allows you to test and monitor rules before they are implemented to block or control browsing. This action is rarely used.

Sandbox rules allow you to select from the following actions, where the file type and URL Category match the associated Sandbox Profile:

- **Hold and Scan:** Content matching the Sandbox Profile is queued for scanning by the Sandbox Service. Delivery of this content is deferred until the content has been scanned.
- **Pass and Scan:** The request is not denied by this rule. Evaluation of the request continues. Content matching the Sandbox Profile is queued for scanning by the Sandbox Service. Future requests for the content will use the cached result from the Sandbox Service.
- **Pass:** The request is not denied by this rule. Evaluation of the request continues with other rules and blocking configuration.

4.2.2 Time Frames

Choose the times when the rule applies. Create time frames in **Settings | Time Frames**. Time frames are evaluated relative to the time zone set for the company, the location, the user, or the user group.

4.2.3 Comment

As best practice, add a description of the purpose of the rule and other important information like reference or ticket ID.

4.3 Locations

SWG Cloud uses locations to assign rules, policies, and other configuration unique to the location’s circumstance. At a minimum, a location requires a single IP address. However, you can add other information such as a name, range of IP addresses, and time zone. For each location you can assign or create:

- Safe Search

- A policy from pre-existing policies. (See section 4.6.)
- Rules specific to that location
- New redirect rules for Google.com.

The screenshot displays the 'Locations' configuration page. On the left, a table lists the location 'Traffic_Generator' with an IP range of '192.0.2.1'. On the right, the 'Edit Location' drawer is open, showing various configuration options. The 'Address' field is set to '192.0.2.1'. The 'Location Type' is set to 'Normal', with 'Firewall Redirect' as an option. There are two 'Time Zone' dropdown menus, both currently set to 'Select...'. The 'Assigned Policy' and 'Safe Search' fields are also set to 'Select...'. Below the 'Edit Location' drawer, there is a 'Redirect Rules for google.com' section with radio buttons for 'Override', 'Do Not Redirect Requests', and 'Redirect Requests To'. The 'Rules' section below that shows a table with columns for 'Rule Summary', 'Action', 'Time Frame', and 'EUM', which is currently empty with the message 'No Data Available'. At the bottom of the drawer, there are 'SAVE' and 'CANCEL' buttons.

4.3.1 Add or Edit a Location

1. For a new location:
 - a. Click the **Add Item** icon above the **Location** list. The **Add Location** drawer opens.
 - b. In the **Range Name** field, enter the name of the location.



Note: Range names are optional. If you do not enter one, then the **Address** becomes the **Range name** and the **Address** cannot be changed later.

2. For an existing location, highlight the location. The **Edit Location** drawer opens.
3. In the **Address** field, enter the IP address for the location. If this location has a range of addresses, enter the first address in the range.
4. Add any of this optional information:
 - a. If this location has a range of addresses, enter the last address in the range in the **Address Range End** field.
 - b. To assign a time to this location, begin typing in the **Time Zone** field. Select from the list of possible choices that appears.
5. Add any stipulations or restrictions to the location. (See below.)
6. Click **Save**.

4.3.2 Add Stipulations or Restrictions to the Location

While you are creating a new location or editing an existing location, you can add these rules, policies and configurations to the location:

- To use this location for Firewall Redirect (DNAT traffic forwarding) or Enterprise WiFi (DNS based filtering), select the appropriate **Location Type**.



Notes:

- For more details of required network setup to support these options, contact Trustwave.
- Enterprise Wifi is an optional add-on service.
- To exclude this location from decryption of HTTPS requests, mark the **Don't Decrypt HTTPS** checkbox. Excluding HTTPS decryption may be useful for guest WiFi locations (Enterprise WiFi) where the client will not have the SWG Cloud root certificate used for SSL decryption installed.
- To assign a specific policy to this location, choose the policy from the **Assigned Policy** drop down list.
- To enforce Safe Search, choose the option from the **Safe Search** drop down list.
- To override the redirect rules for Google searches, mark the **Override** check box and then select whether to redirect requests. If requests should be redirected, select to where in the **Redirect Requests to** drop down list.
- To add a rule to the location, click the **Add** icon over the **Rules** list. In the **Add Rule** dialog, select the rule type and any other required information.

4.4 Users

You can configure SWG Cloud to place limits on or expand access for specific users. SWG Cloud determines which users it affects from information provided in each request. Specifically, SWG Cloud draws this information from:

- the MSC client
- SAML when a PAC file is used
- chained proxies that provide the `X-Authenticated-User` header.



Tip: Defining individual users is optional. Use this feature to override policy and rules that apply by default or to groups. For a full explanation of the order of evaluation, see Chapter 5.

When a user is identified in this information, SWG Cloud checks its user identities for related rules and policies. User identities (also called users) contain a user ID and optional information:

- a default policy for the user
- a time zone for time-based rules
- Safe Search and MSC options that override default options in the policy

- custom rules for the user

You can add, edit, and delete user identities in the **Configurations** section of SWG Cloud.

To create or edit a user:

1. For a new user:
 - a. Click the **Add** icon above the **User Identities** list. The **Add User** drawer opens.
 - b. In the **User ID** field, enter the ID of the user.



Tip: The exact format of the User ID depends on the identity provider, such as a SAML IdP, the SWG Cloud Mobile Security Client, or proxy X-headers. (Proxy chaining allows you to deliver x-forwarded-for headers that provide the device IP which Trustwave uses only for reporting only and not for policy assignment.) Some common formats are `user@domain.tld` or `domain\user`. You can use the SWG Cloud Settings to normalize the user domain information. If the group comes from Trustwave MSC, the format is `user@FQDN`.

2. For an existing user, click it. The **Edit User** drawer opens.
3. Add any of this optional information:
 - a. Select a default policy for the user.
 - b. To assign a time to this location, begin typing in the **Time Zone** field. Select from the list of possible choices that appears. This will be used in time-based rules.
 - c. Select whether to override the default options for:
 - Safe Search
 - MSC disabling
 - Automatic client upgrade

d. Add custom rules for the user. See section 4.2.

4. Click **Save**.

4.5 Groups

You can configure SWG Cloud to place limits on or expand access for specific groups. SWG Cloud determines which (if any) groups it affects from information provided in each request. Specifically, SWG Cloud draws this information from:

- with SAML when the MSC client or a PAC file is used
- with chained proxies that provide the `X-Authenticated-Groups` header.



Note: SWG Cloud assigns group membership based on information received in web requests. SWG cloud does not retrieve group information directly from servers such as AD or LDAP.

When a group is identified in this information, SWG Cloud checks its group identities for related rules and policies. Group identities (also called groups) contain a group name, priority, and optional information. SWG Cloud uses the priority to determine which rules and policy to apply to a user if that user belongs to multiple groups. The optional information is:

- a default policy for the group
- the time zone for time-based rules
- Safe Search and MSC options (overriding default options for the policy)
- custom rules for the group

You can add, edit, and delete user identities in the **Configurations** section of SWG Cloud.

The screenshot shows the 'Groups' configuration page in the SWG Cloud interface. The page is titled 'Secure Web Gateway > Configuration > Groups' and shows 'Customer1_SWG (198...)' with 'PENDING CHANGES'.

Group Identities Table:

Group Name	Priority	Assigned Policy	Rules
IT	1	Power Users	
Product Engineering	2		
Sales	3	Default	

Edit Group Form (Sales):

- Group Name: Sales
- Priority: 3
- Assigned Policy: Default
- Time Zone: Select...
- Safe Search: Select...
- Disabling MSC: Select...
- Automatic Client Upgrade: Select...

Rules Table:

Rule Summary	Action	Time Frame	EUM
<input type="checkbox"/> Custom URL - salesforce.com	Whitelist		

Total Items: 1

Buttons: SAVE, CANCEL

To create or edit a group:

1. For a new group:
 - a. Click the **Add** icon above the **Group Identities** list. The **Add Group** drawer opens.
 - b. In the **Group Name** field, enter the name of the group.



Tip: The exact format of the Group ID depends on the identity provider, such as a SAML IdP, the SWG Cloud Mobile Security Client, or proxy X-headers. (Proxy chaining allows you to deliver x-forwarded-for headers that provide the device IP which Trustwave uses only for reporting only and not for policy assignment.) Some common formats are `group@domain.tld` or `domain\user`. You can use the SWG Cloud Settings to normalize the group domain information. If the group comes from Trustwave MSC, the format is `group@domain`.

2. For an existing group, click it. The **Edit Group** drawer opens.
3. In the **Priority** field, enter a number that indicates how important this group is in your organization. The lower the number, the more important the group.



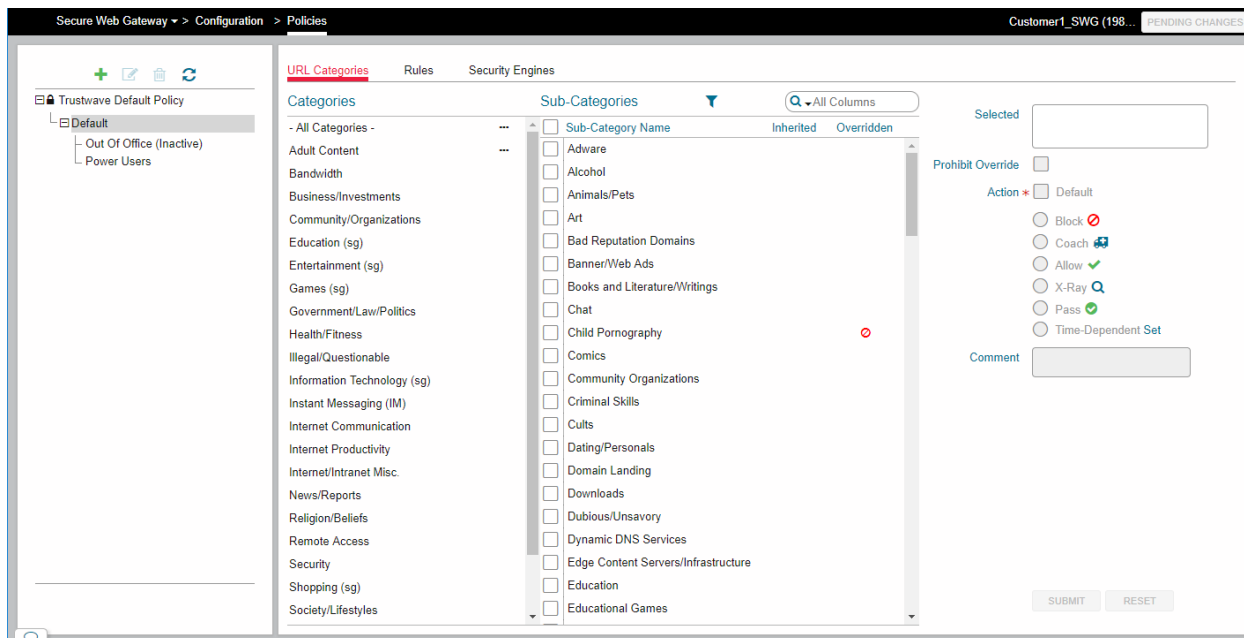
Tip: When a user belongs to multiple groups, SWG Cloud evaluates all of the policies assigned to all of the groups that the user belongs. These policies are ordered according to the priorities of their groups. SWG then applies the policies and rules.

4. Add any of this optional information:
 - a. Select a default policy for the group.
 - b. To assign a time to this location, begin typing in the **Time Zone** field. Select from the list of possible choices that appears. This will be used in time-based rules.
 - c. Select whether to override the default options for:
 - Safe Search
 - MSC disabling
 - Automatic client upgrade
 - d. Add custom rules for the group. See section 4.2.
5. Click **Save**.

4.6 Policies

SWG Cloud allows you to customize its default policy and to create named policies. Policies (default and named) control end user's web usage and messaging. A policy can include URL category actions, rules, and Security Engine messages. Initially, SWG Cloud only has its default policy. You must create all named policies.

A named policy is one that you create and that inherits setting from either the default policy or another named policy. Named policies refine their parent policy. You can apply named policies to users, groups and locations.



The left pane of the **Policies** page shows the list of policies as a tree. Child policies in the tree inherit the settings of the parent policies. When you add a policy, you choose the parent policy for the new policy.

The root item of the tree is the **Trustwave Default Policy**. You can view the content of this policy, but you cannot edit it.

Each customer has a **Default** policy that inherits from the Trustwave default policy.

You can create new policies that inherit from the customer **Default** policy.

- To view details of a policy and make changes if permitted, select it in the left pane.
- To add a policy, click the **Add Item** icon above the policy list. Enter a name. Select the parent policy. Enter notes to explain the intent of the policy.
- To edit the name or notes, or to change the parent policy of a policy, select it in the tree and click the **Edit Item** icon.
- To delete a policy, select it and click the **Delete Item** icon. You cannot delete a policy if the policy is assigned to an Identity such as a user or groups.



Note: If you make any changes to inherited policies or override actions, those changes will only take effect after you commit them. See chapter 5 for information about policy and rule precedence.



4.6.1 URL Categories

The URL Categories tab shows a list of Categories. In the **Categories** list, **---** indicates a Category that includes at least one sub-category that applies Rule actions.

Select a category to show a list of the sub-categories it contains.

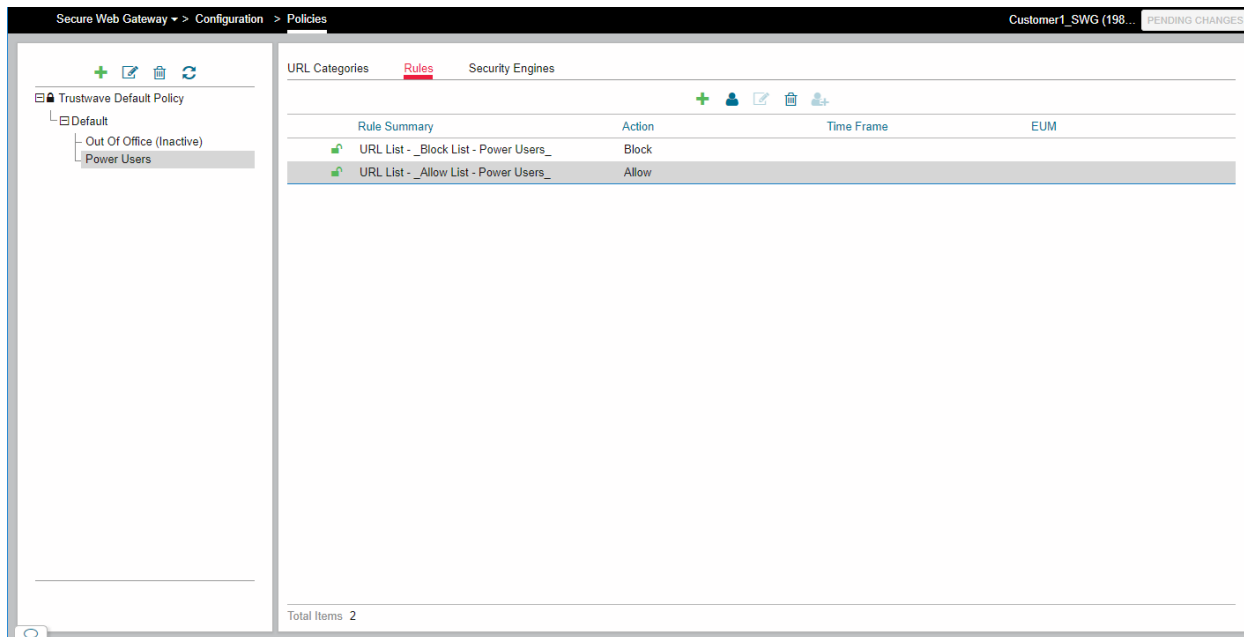


Tip: To edit the Category and Sub-Category lists, see **Configuration | Categories**.

- For each sub-category, two columns show the icon for the Rule action that will be taken, if any:
 - **Inherited:** the action inherited from a parent profile. Where this action is overridden in the current profile, the icon is disabled (greyed out).
 - **Overridden:** the action specified in the current profile. If this column is blank, the inherited action (if any) applies.
- 1. To filter the list of sub-categories by action, click the **Filter**  icon above the list and select the actions you want to include. The **Filter** icon changes color . To clear the filter, click the icon again.
- 2. To filter the list of sub-categories by name, or by the text of the action, use the **Search** box above the list.
- 3. To edit the actions for one or more sub-categories, select them using the checkboxes. The **Selected** field in the right pane lists the selected categories. Choose actions using the controls in the right pane.
 - a. Check **Prohibit Override** to force child policies to inherit from this policy.
 - b. Check **Action (Default)** to accept the inherited action, if any.
 - c. To set a local action, clear **Action** and use the radio buttons to select an action.
 - d. If you select **Time Dependent**, on the **Time Dependent Actions** window click **Add Item**, then select an existing **Time Frame** and an action. You can add more than one Time Dependent Action.
 - e. Optionally add a comment to describe the purpose of this action.




4.6.2 Rules

The **Rules** tab lists rules that apply to the policy. If you use the Quick Setup, then each policy includes rules to apply a URL Block List and a URL Allow List. If you do not use Quick Setup, this tab is empty by default.








The list shows the action, and any time frame or custom end user message that applies.

At the left of the list, the first column shows the status of inheritance from the parent:

- **Blank** for a local rule that can be overridden
- **Parent icon**  for an inherited rule
- **Parent with +**  for a rule that is inherited but has an overriding change
- **Lock**  for an inherited rule that cannot be overridden

The second column shows the permissions for inheritance by children:

- **Closed lock**  for a rule that cannot be overridden
 - **Open lock**  for a rule that can be overridden
1. To show rules from parent policies, click the **Show Parent Rules**  icon above the list. The icon changes color to indicate parent rules are shown. To hide rules from parent policies, click the **Hide Parent Rules**  icon.
 2. To add a rule, click the **Add Item** icon above the list. For details see the section on rules.
 3. To edit a rule, click the **Edit Item** icon above the list. For details see the section on rules.
 4. To delete a rule, select it and click the **Delete** icon.
 5. To override a parent rule, select it and click the **Override**  icon, and then make changes.

4.6.3 Security Engines

On the Security Engines tab, you can view the list of security engines that are applied, and the actions taken when each engine triggers. Security Engines cannot be edited.

- Select an action to view details of the default message and to add a custom message.

4.7 Categories



In addition to the default categories that SWG Cloud provides, you can create and manage sub-categories that you customize to your organization. These sub-categories may block or allow access to specified URLs and use keywords to block or allow searches and other URLs. You can also customize existing sub-categories with URLs and keywords to match your organization's needs.

Trustwave's Web Filter Database provides the default category content. All custom sub-categories must be created under these categories.

The screenshot displays the 'Categories' configuration page. The left sidebar contains a list of categories, including 'Adult Content', 'Bandwidth', 'Business/Investments', 'Community/Organizations', 'Education (sg)', 'Entertainment (sg)', 'Games (sg)', 'Government/Law/Politics', 'Health/Fitness', 'Illegal/Questionable', 'Information Technology (sg)', 'Instant Messaging (IM)', 'Internet Communication', 'Internet Productivity', 'Internet/Intranet Misc.', 'News/Reports', 'Religion/Beliefs', 'Remote Access', 'Security', 'Shopping (sg)', 'Society/Lifestyles', 'Streaming Media', and 'Travel/Events'. The main area shows a list of sub-categories, with 'Art' selected. Below this, there are sections for 'URLs' and 'Keywords'. The 'URLs' section has a table with one row: 'www.notamuseum.museum' under the 'URL' column, with 'Include' and 'Exclude' buttons. The 'Keywords' section is empty, showing 'No Data Available'. At the bottom, there are 'SUBMIT' and 'CANCEL' buttons.

The **Configuration | Categories** page is organized hierarchically. Its left pane contains a list of SWG Cloud's categories. Select a category to see its sub-categories in the right list. When you select a sub-category (inherited or new), you can modify its content.

There are two unique icons on the page:

Icon	Meaning
	a category that includes non-inherited sub-categories
	a sub-category that is inherited from the parent category

4.7.1 Create a New Sub-Category

1. Select the category you want to augment.
2. Click the **Add** icon above the **Sub-Categories** list. The **Add Sub-Category** dialog opens.
3. Select the category you want to augment.
4. In the **Sub-Category** field, enter the name of the new sub-category.
5. Click **Submit**.
6. In the **Sub-Categories** list, select the new sub-category.

4.7.2 Add a or edit a URL in a Sub-Category

1. Select the category you want to augment.
2. Select the sub-category you want to edit.
3. Click the **Add** icon above the URLs list. Alternatively, highlight an existing time slot and click the **Edit** button.
4. Choose whether to include or exclude the URL from the sub-category.
5. Enter or edit the URL. Do not include its protocol.
6. Click **Submit**.

4.7.3 Add or Edit a Keyword in a Sub-Category

1. Select the category you want to augment.
2. Select the sub-category you want to edit.
3. Click the **Add** icon above the **Keywords** list. Alternatively, highlight an existing time slot and click the Edit button.
4. Choose whether the keyword should be a search term or in a URL.



Tip: SWG Cloud can match keywords against both search phrase and URLs. When a URL is chosen, you can also choose to match against the URL parameters (query string).

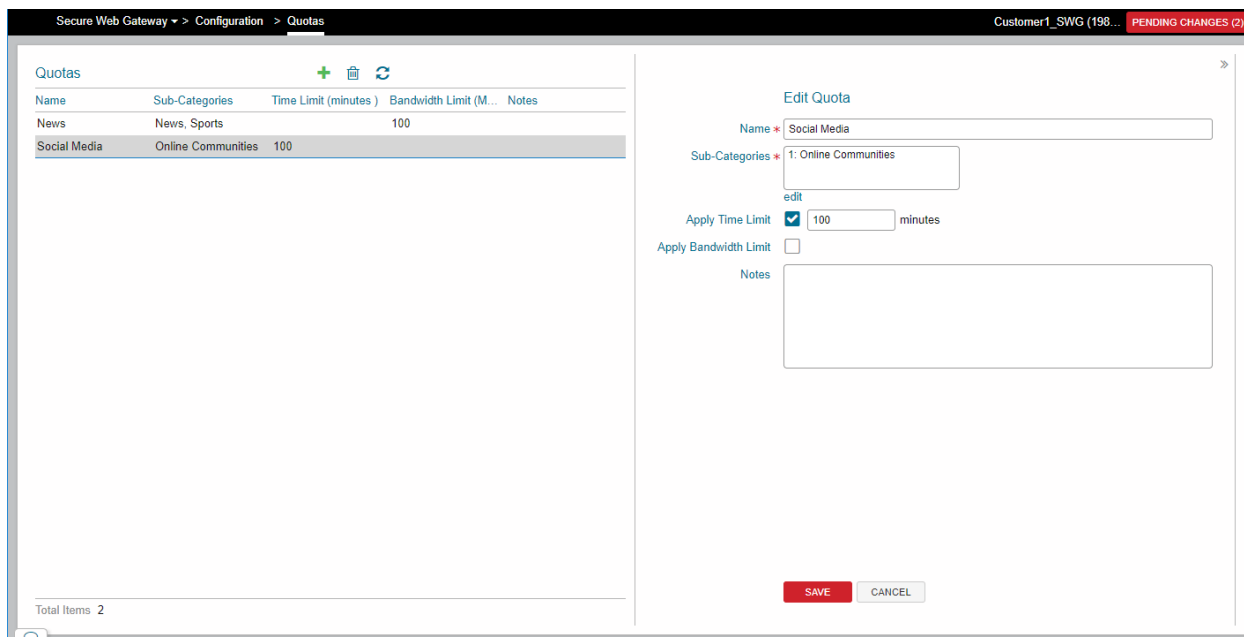
5. Enter or edit the keyword.
6. Click **Submit**.

4.8 Quotas

SWG Cloud can limit the amount of time and bandwidth spent accessing specified sub-categories. These quotas are added to rules. You can also place quotas on URL sub-categories.

Once configured and enabled, quotas are reset daily by default. You can manage the interval from **Configuration | Settings, Quota** tab. See section 4.1.4.

No quotas exist by default.



To create or edit a quota:

- For a quota from:
 - Click the **Add** icon above the **Quotas** list. The **Add Quotas** drawer opens.
 - In the **Name** field, enter the name of the time frame.
- For an existing quota, highlight the quota. The **Edit Quota** drawer opens.
- Click the **edit** link to call a list of sub-categories.
 - Mark the checkboxes of the sub-categories you want.
 - Click **Apply Selected**. Your selections appear in the **Sub-Categories** field.
- To create a time limit, mark the **Apply Time Limit** check box and enter the number of minutes allowed.
- To limit the bandwidth spent on these sub-categories, mark the **Apply Bandwidth Limit** check box and enter the number of megabytes (MB) allowed.
- Explain the purpose of this quota in the Notes field.

7. Click **Save**.

4.9 Sandbox

SWG Cloud can analyze files for malware content using the Malware Analysis Sandbox service. You can create profiles that determine the content you want to scan with this service. Profiles can be based on the URL Category and File Type. Sandbox profiles are used in rules. Within each rule you can determine the action to take on matching files (Pass and Scan, or Hold and Scan).



Note: Sandbox is an additional service that must be purchased in addition to SWG Cloud.

The screenshot displays the 'Sandbox Profiles' configuration page. On the left, a table lists the existing profiles:

Name	Sub-Categories	File Types	Notes
R rated	Obscene/Tasteless...	HTML Web Page, ...	

Below the table, it indicates 'Total Items 1'. On the right, the 'Edit Sandbox Profile' form is shown for the 'R rated' profile. The form includes the following fields:

- Name:** R rated
- Sub-Categories:** 2: Obscene/Tasteless, R Rated
- File Types:** Zip Archive + 6 more
- Notes:** (Empty text area)

At the bottom of the form are 'SAVE' and 'CANCEL' buttons. The top navigation bar shows 'Secure Web Gateway > Configuration > Sandbox Profiles' and 'Customer1_SWG (198... PENDING CHANGES (1))'.

The sandbox feature comes with default two profiles that are enabled upon provisioning. These profiles are:

- **Default Sandbox Profile - Hold And Scan** on these file types:
 - Windows Executable File
 - DOS Executable File
 - Microsoft Office Document
 - OpenOffice Document
 - MSI installation package
 - Standalone JavaScript
 - Rich Text Format

- **Default Sandbox Profile - Pass And Scan** on these file types:
 - TIFF image
 - Java Class
 - MS Windows Html Help Data
 - Link File
 - Cap File
 - MIME Container File
 - URL File
 - Adobe Flash Application
 - Standalone VBScript
 - RAR Archive
 - TAR Archive
 - Zip Archive

When a sandbox rule runs and generates a result for a file, SWG Cloud caches the result. If there are any subsequent requests for that file, SWG Cloud uses the cached result. If a file was analyzed as safe, it will be returned with no delay from a “hold and scan” rule.

4.9.1 Create or edit a Sandbox Profile:

1. For a new profile:
 - a. Click the **Add** icon above the **Sandbox Profiles** list. The **Add Sandbox Profile** drawer opens.
 - b. In the **Name** field, enter the name of the profile.
2. For an existing profile, click the profile. The **Edit Sandbox Profile** drawer opens.
3. Click the **edit** link to call a list of sub-categories.
 - a. Mark the checkboxes of the sub-categories you want.
 - b. Click **Apply Selected**. Your selections appear in the **Sub-Categories** field.
4. In the **File Types** drop down list, mark the types of files you want to quarantine.
5. Click **Save**.

4.9.2 View Sandbox Results

Detailed results of Sandbox analysis are available from the Web Activity request logs. (This information is not available for Policy Test results.)

To view the logs:

1. Open **Data Explorer | Web Activity | Explorer**
2. Search the log entries for the web requests related to Sandbox rules.



Tip: To find Sandbox related activity at a glance, in the Web Requests detail view click the column chooser and add the Sandbox columns to the list.

Snapshot	Requests	Transaction ID	Time	User	IP	User Group	URL	Category	Action	Status	Device	Sandbox Key	Sandbox Act...	Sandbox Pa...
2019-05-01 13:17:28	14,594	5cc25c6a9256010a007c	2019-04-26 04:18:35	prodtester2	24.9.36.4	prodgroup2	https://urs.microsoft.co...	information tech...	Bypass	200	10.127.98.101			
		5cc25c6a9256010a007c	2019-04-26 04:18:34	prodtester2	24.9.36.4	prodgroup2	https://urs.microsoft.co...	information tech...	Bypass	200	10.127.98.101			
		5cc25c3ca59010a0007d	2019-04-26 04:18:33	prodtester2	24.9.36.4	prodgroup2	https://urs.microsoft.co...	information tech...	Bypass		10.127.98.101			
		5cc25c3ca59010a0007d	2019-04-26 04:17:55	prodtester2	24.9.36.4	prodgroup2	https://teams.microsoft.c...	information tech...	Bypass		10.127.98.101			
		5cc25c3e9996010c0079	2019-04-26 04:17:50	prodtester2	24.9.36.4	prodgroup2	https://mobile.pipe.aria...	information tech...	Bypass		10.127.98.101			
		5cc25c3ca3f010c0078	2019-04-26 04:17:48	prodtester2	24.9.36.4	prodgroup2	http://mobile.pipe.aria...	information tech...	Bypass		10.127.98.101			
		5cc25c3b5154010c0077	2019-04-26 04:17:47	prodtester2	24.9.36.4	prodgroup1	http://api.bing.com:443	search engines	None		10.127.98.101			
		5cc25c3ac367010a0089	2019-04-26 04:17:46	prodtester2	24.9.36.4	prodgroup2	http://go.microsoft.com...	information tech...	Bypass		10.127.98.101			
		5cc25c27501401070078	2019-04-26 04:17:27	prodtester2	24.9.36.4	prodgroup1	http://api.bing.com:443	search engines	None		10.127.98.101			
		5cc25c2774170100007a	2019-04-26 04:17:27	prodtester2	24.9.36.4	prodgroup1	http://52.18.58.97/lu...	other	None	200	10.127.98.101	97c542b0-3104...		
		5cc25c1d54560100007a	2019-04-26 04:17:17	prodtester2	24.9.36.4	prodgroup1	http://api.bing.com:443	search engines	None		10.127.98.101			
		5cc25c1dbcc7010a0083	2019-04-26 04:17:17	prodtester2	24.9.36.4	prodgroup1	http://52.18.58.97/plu...	other	None		10.127.98.101			
		5cc25c1baae010a00084	2019-04-26 04:17:15	prodtester2	24.9.36.4	prodgroup2	http://teams.microsoft.c...	information tech...	Bypass		10.127.98.101			
		5cc25c040f01080078	2019-04-26 04:17:01	prodtester2	24.9.36.4	prodgroup1	http://api.bing.com:443	search engines	None		10.127.98.101			
		5cc25c0408ca01000078	2019-04-26 04:17:01	prodtester2	24.9.36.4	prodgroup1	http://api.bing.com:443	search engines	None		10.127.98.101			
		5cc25c0d9554010c0075	2019-04-26 04:17:01	prodtester2	24.9.36.4	prodgroup1	https://api.bing.com/qa...	search engines	None		10.127.98.101			
		5cc25c0daa90010a0085	2019-04-26 04:17:01	prodtester2	24.9.36.4	prodgroup1	http://52.18.58.97/tpu...	other	None		10.127.98.101			
		5cc25c05d541010a0088	2019-04-26 04:16:53	prodtester2	24.9.36.4	prodgroup1	http://roaming.officeap...	web based email	None		10.127.98.101			
		5cc25b77a6b010a007d	2019-04-26 04:16:39	prodtester2	24.9.36.4	prodgroup2	http://gag.com	shopping	Blocked		10.127.98.101			
		5cc25b9374b010a0077	2019-04-26 04:16:35	prodtester2	24.9.36.4	prodgroup2	http://teams.microsoft.c...	information tech...	Bypass		10.127.98.101			
		5cc25b9e77010a0078	2019-04-26 04:16:25		24.9.36.4		https://urs.microsoft.co...	information tech...	Bypass	200	10.127.98.101			
		5cc25be890b3010a0082	2019-04-26 04:16:24		24.9.36.4		https://urs.microsoft.co...	information tech...	Bypass	200	10.127.98.101			
		5cc25be8a551010a007c	2019-04-26 04:16:24		24.9.36.4		http://urs.microsoft.co...	information tech...	Bypass		10.127.98.101			

- View details of an individual request, and then hover the pointer over the **Sandbox Report** value to show the analysis information.

Web Request

URL: <http://52.18.58.97/tpusers/qaautomation/truecontenttype/standalonejavascript/swfobject.js>

Protocol: MIME Type: APPLICATION/JAVASCRIPT

Status: Job Type: HASH

Category: Job Status: SUCCESS

Action: Threat Score: 1/100

Analysis Type: Submission Started: 2019-04-26 04:18:41

Inbound/Outbound: Submission Ended: 2019-04-26 04:19:25

Content Type: MD5: 8c2ec4bc2c9a39bc34f92223077c6

X-Forwarded-For: SHA1: 4d4c6c77a63258ee7be5e8377a1ed97311bc45652

Social Media: SHA256: 73e3bd3b6c7912059b2b90a808881418b06ed8b18924638eb907e90442b9

Sandbox Report: 97c542b0-3104-4a43-a13f-297a6b0f4941

Sandbox Active: Yes

Sandbox Pass and Scan: --

Time: 2019-04-26 04:17:27

Transaction ID: 5cc25c2774170100007a

User: prodtester2

IP: 24.9.36.4

Group: prodgroup1

Quota: --

Security Engine: --

Engine Result: URL_CAT: 0, TYPE_DETECTOR: Standalone JavaScript, URL_CAT: 0

Scanner: 10.127.98.101

DLP Condition: --

Malware Rule: --


Virus: --

Infected: --

Policy Name: trustwave default cloud security policy

POLICY CHANGE REQUEST

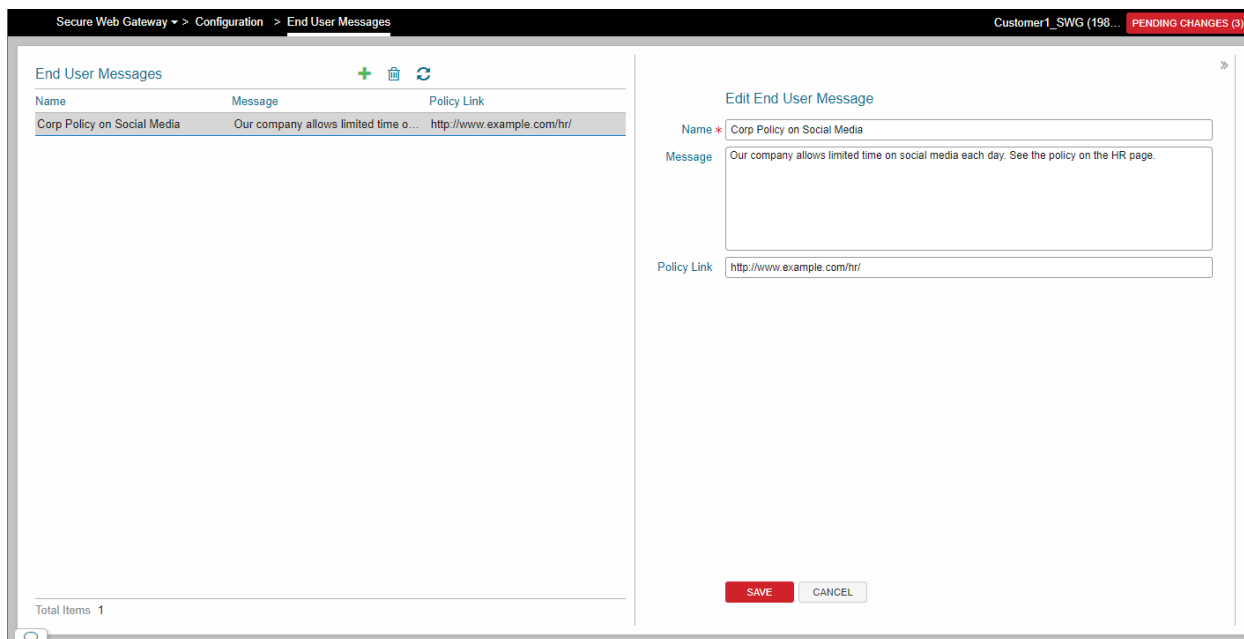
VIEW / RESET QUOTAS

- To see the analysis report on a new page, click **more details**.
- On the analysis report page, click the download icon  to download the report.

4.10 End User Messages

SWG Cloud allows you to create and manage custom messages which you can assign to policies or rules. This will present your message to the end user when they are blocked from something. These messages can replace text placeholders in SWG Cloud's end-user displays.

End user messages are created independently and can be reused in several policies and rules. Each message may contain text and a link to a policy document, web site, or some other information. At a minimum, each message requires a name.



To create or edit an end user message:

6. For a new end user message:
 - a. Click the **Add** icon above the **End User Messages** list. The **Add End User Message** drawer opens.
 - c. In the **Name** field, enter the name of the message.
7. For an existing location, click the end user message. The **Edit End User Message** drawer opens.
8. Enter the message into the **Message** field.
9. If there is a related URL, enter the URL into the **Policy Link** field. Be sure to include the protocol, e.g. https://.
10. Click **Save**.

4.11 URL Lists

SWG Cloud allows you to create and manage lists of URLs for use in policies and rules. You can add URLs to each list one at a time or import multiple URLs from a UTF-8 formatted text file. Once a list is created, it cannot be deleted if it is in use.

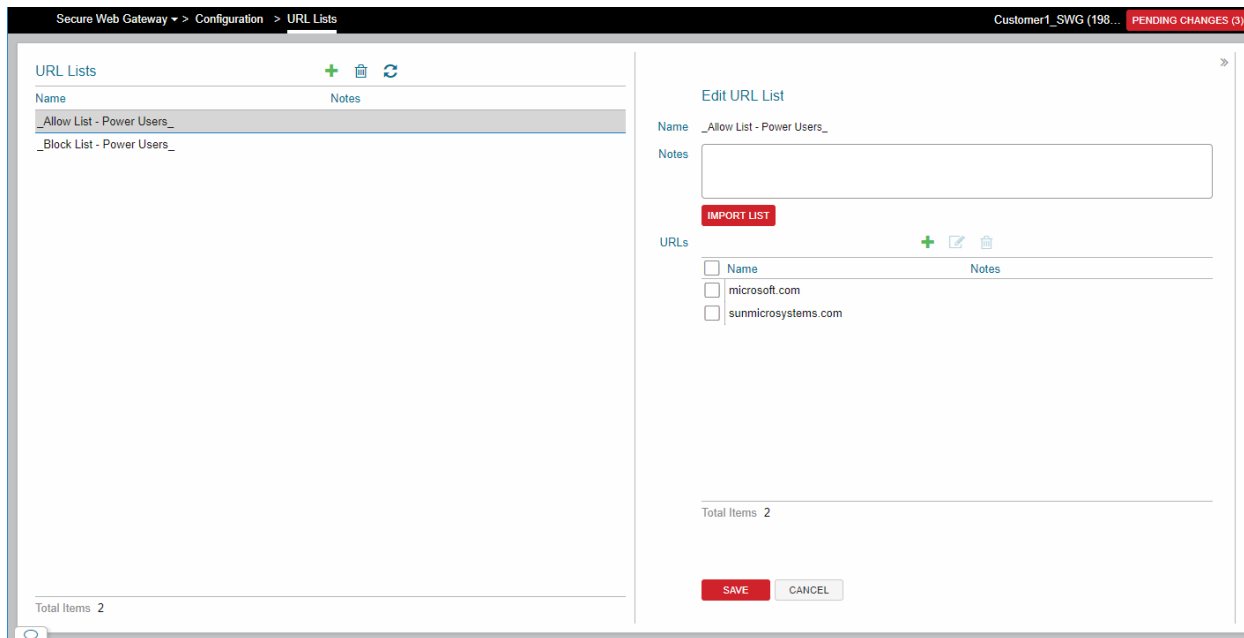
When you add a URL (either individual or via importing) the URL:

- must omit its protocol

- can start with a wildcard * (i.e. matches any subdomain)
- can include a path part
- cannot be a duplicate

When you import a file of URLs, the file must contain one valid URL per line and can either replace or merge with the current list of URLs.

SWG Cloud automatically creates URL lists for each policy that you configure in Content Controls or Policies. You can manage these lists either here or in the **Content Controls** page. (See chapter 3.)



To create or edit an URL list:

1. For a new URL list:
 - a. Click the **Add** icon above the **URL Lists** list. The **Add URL List** drawer opens.
 - b. In the **Name** field, enter the name of the list.
2. For an existing URL list, click the list. The **Edit URL List** drawer opens.
3. Explain the purpose of this list in the **Notes** field.
4. To import a pre-existing list:
 - a. Click **Import List**.
 - b. On the **Import URL List** dialog, click **Choose File**.
 - c. Navigate to, select, and open the UTF-8 formatted text file that contains your list of URLs.
 - d. On the **Import URL List** dialog, select where the file should replace or merge with the existing list of URLs. (Your choice does not matter if this is a new list.)

- e. Click **Upload**.
5. To add or edit individual URLs:
 - a. Click the **Add** icon above the **URLs** list. Alternatively, highlight an existing URL and click the **Edit** button.
 - c. In the new dialog, enter or edit the URL in the **Name** field. SWG Cloud requires that this URL follows the same requirements as the URLs in an imported file.
 - d. Explain the purpose of this URL in the **Notes** field.
 - e. Click **Submit**.
6. Click Save.

4.12 Time Frames

You can define time periods to use in policies and rules. Time frames can include one or more time “slots” or ranges. Ranges can apply to specific days or can span more than one day. No time frames exist by default.

The screenshot shows the 'Time Frames' configuration page. On the left, a table lists existing time frames:

Name	Summary	Notes
Lunchtime	Monday, Tuesday, Wednesday, Thursday, Friday - 12:00-13:00	

Below the table, it indicates 'Total Items 1'. On the right, the 'Edit Time Frame' dialog is open for the 'Lunchtime' frame. It contains the following fields and options:

- Name ***: Lunchtime
- Notes**: (empty text area)
- Time Slots ***: A table with checkboxes for days and their corresponding start and end times.

Start Day	Start Time	End Day	End Time
<input type="checkbox"/> Monday	12:00	Monday	13:00
<input type="checkbox"/> Tuesday	12:00	Tuesday	13:00
<input type="checkbox"/> Wednesday	12:00	Wednesday	13:00
<input type="checkbox"/> Thursday	12:00	Thursday	13:00
<input type="checkbox"/> Friday	12:00	Friday	13:00
- Total Items**: 5
- Buttons**: SAVE (red), CANCEL (grey)

To create or edit a time frame:

1. For a new time frame:
 - a. Click the **Add** icon above the **Time Frames** list. The **Add Time Frame** drawer opens.
 - b. In the **Name** field, enter the name of the time frame.
2. For an existing time frame, click it. The **Edit Time Frame** drawer opens.
3. Explain the purpose of this time frame in the **Notes** field.

4. Click the **Add** icon above the **Time Slots** list. Alternatively, highlight an existing time slot and click the **Edit** button.
 - a. Choose where the time frame extends over a single day or multiple days.
 - b. For a **Same Day Timeslot**, select which days of the week the time slot occurs and in the **Time Range** field enter the **Start** and **End** times.



Note: If you choose multiple days, they will be recorded as separate time slots in the **Time Slots** list.

- c. For a **Span Multiple Days Timeslot**, select which days of the week the time slot begins and ends on and then the times for each of those days.



Tip: If you want multiple time slots that span multiple days, create a time slot for each one.

- d. Click **Submit**.
5. Click **Save**.

4.13 App Profiles

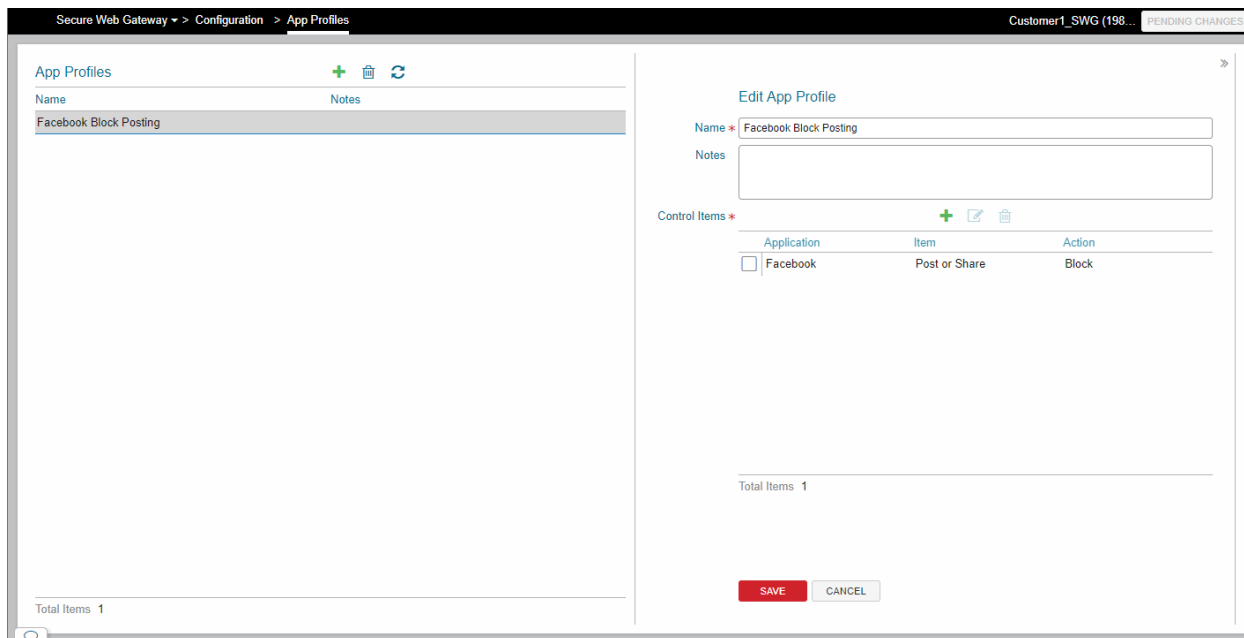
You can create lists of actions which SWG Cloud will allow or prohibit actions in common web applications such as Facebook or OneDrive. This type of application control is called an app profile. Each app profile has a name, description, and list of control items. App profiles are used in rules and policies.

A profile consists of one or more control items. The items can apply to the same application or different applications. For example, you can create a profile to restrict uploading to several cloud storage services (such as Amazon Drive, Google Drive iCloud, and OneDrive). You can create a profile to restrict several Facebook actions (such as Comment, Post, Chat send). Depending on what you choose, SWG Cloud can allow, block, or x-ray (allow and log for the item for reporting) the action. For a list of applications and explanations of the available actions for each, see Appendix C.


Few app profiles exist by default.



Caution: If you have excluded applications from scanning, you may not be able to apply App Profiles to those applications.



To create or edit an app profile:

1. For a new app profile:
 - a. Click the **Add** icon above the **App Profiles** list. The **Add App Profile** drawer opens.
 - b. In the **Name** field, enter the name of the app profile.
 2. For an existing location, click the app profile. The **Edit App Profile** drawer opens.
 3. Add relevant information to the **Notes** field such as the purpose of this time frame or a change ticket number.
 4. Click the **Add** icon above the **Control Items** list. Alternatively, highlight an existing control item and click the **Edit** button.
 - a. In **Action**, choose SWG Cloud should do with the application:
 - Block – stop the application from performing the specified item
 - Allow – let the application perform the item specified
 - X-Ray – let the application perform the item specified and record the occurrence in SWG Cloud's log
 - b. In the **Application** field, choose the application you want to control.
 - c. In the **Item** field, select the application item (action) you want to control.
-  **Note:** See Appendix B for a complete list of applications and their related items.
- d. Click **Submit**.
 5. Click **Save**.

5 Policy and Rule Precedence

SWG Cloud evaluates requests and takes action using a defined precedence.

The default policy is the base customer policy. This is the policy that an unidentified end user from the customer receives. If the user's Identity (User, Group, or Location) is not associated with any exceptions or child policies (that is Named Policies), then this policy is enforced.

5.1 Line Item Exceptions

You can make exceptions to policies for a specific Identity by creating a Line Item Exception. Line Item Exceptions are created using the Configuration section of the interface. Exceptions are defined by the part of the policy being changed, the Identity, the Action to be taken, and any other elements that apply to this part of the policy.

- Line Item Exceptions contain a single rule of a single rule type and are assigned to **one identity**.
- All Line Item Exceptions that have the same identity are considered a single Policy Node.
- The group of Line Item Exceptions that make up a Policy Node are defined as Policy Nodes that do not inherit from other nodes. They are evaluated first - so they could be considered "the lowest node".
- There is a text field (for notes or comments) for each Line Item Exception that allows you to record and later view the reason for the exception.
- Since Line Item Exceptions still enforce Security, several items must be taken into consideration. The End User Messages for Security Engine rules are taken from the highest priority matching Line Item Exception or Named Policy (or the default policy if no other policy matches the user identity).

5.2 Named Policy

Named Policies are defined as a group of all rule types that can inherit from default policy or other Named Policies.

- A Named Policy is considered a Policy Node.
- All child policies created after the default policy are "Named Policies". Multiple Named Policies can be created from a single parent. There is no set limit for levels of child policies. When a Named Policy is created, all policy elements are inherited from the parent policy. There are no Named Policies without a parent.
- A name is required for all Named Policies and must be provided at time of creation.
- You can assign Identities to the Named Policy. Any type of Identity can be assigned to a Named Policy, such as users, groups, or locations.
- An Identity can be assigned to one Named Policy only.

5.2.1 Out of Office Policy

An Out of Office Policy is a special-case Named Policy that has an Identity associated with it defined as "all IPs that are not defined IPs or IP Ranges for that customer". This policy inherits from the default policy but can have no children. This gets precedence with IP identity-based policies, which means that it is evaluated after all other matching identities but before the default policy.

- The Out of Office Policy can be set before any IPs or ranges are defined for that customer, but until there is an IP or range defined the policy it cannot be applied to any traffic.
- Identities cannot be added to this policy manually.
- It is possible to add and remove exceptions to and from this policy.

5.2.2 Policy Node

A Policy Node is a Named Policy or the collection of "Line Item Exceptions that are assigned to the same Identity". Named Policies include the special cases of default policy and Out of Office Policy.

5.3 Priority

The priority of outcomes, or actions, is generally from most restrictive to less restrictive. Priority is assessed for conflicts that arise from two rules acting on the same entity.

This can occur for multiple rule types concurrently. For example, a URL in two categories may have different outcomes. The chosen outcome is governed by priority



Priority order is Whitelist, Block, Coach, Allow, X-Ray, and Pass.

Table 5: Actions by Rule Type

Rule Type	Whitelist	Block	Coach	Allow	X-Ray	Pass
Security Engines (Security Engine settings are global and cannot be disabled or changed by tenant/customer)		✓				
Custom URLs	✓	✓	✓	✓	✓	✓
URL Categories		✓	✓	✓	✓	✓
DLP		✓	✓	✓	✓	✓
Application Control		✓		✓	✓	✓
File Download		✓		✓		✓
User Agents		✓		✓		✓

5.4 Inheritance

Rules are inherited from the root (top) node down. Inherited rules are active at the child level (scope). Inheritance is automatic and immutable.

- Rules can have "Prohibit Override" applied to them so that an identical rule cannot be created to override it. Items where override is allowed in child policies are shown with an unlocked  icon next to the item.
- Inherited rules can be overridden by the child node.
- There is no notion of ordinal precedence of rules.
- Evaluation occurs from the bottom up (sub nodes first.)
- Items that are inherited have a visual representation showing whether they are inherited or explicitly set in the policy. Multiple levels of parents and children are possible. Items inherited from a parent policy are shown with a  icon next to the item.

5.4.1 Prohibit Override

SEG Cloud enables and enforces the ability to set multiple levels of policy elements where override is prohibited. For example, you can prohibit the override of policies on a URL Category to block at all times for all users in the parent policy. All child policies inherit the complete policy and allow changes to everything except the element where override is prohibited.

5.5 Hierarchy

Rule precedence occurs from the bottom up. In general, User specific rules are evaluated first, followed by group rules, location rules, Named Policies, and the default policy.

5.6 Identicality

Rules are considered identical if their functions and inputs (arguments) are identical. Identical rules cannot coexist within the same scope, that is, at the same policy level. Users cannot author identical rules at any scope. Users can author identical rules at different scopes, that is, parent and child policy. The child rule then overrides the parent rule.

- Proving identicality requires the ability to discern rule arguments and determine if they are identical. For instance, it is necessary to recognize that *.google.com and mail.google.com are not identical. It is also necessary to determine which rule is more specific.
- Groupings of items in a rule are broken down into individual items for testing Identicality. This applies to URLs in URL Lists and Application/User Action combinations in Application Profiles.

Inherited rules can be overridden in a child policy. An identical rule in a child policy overrides the rule in the parent policy. When overridden, the child rule supersedes the parent rule.

- Rules that override a parent rule can be deleted. The parent rule will then be active at the child level.

- Parent rules can be effectively ignored or removed in the child policy by creating an identical rule in the child policy and selecting an Action that takes no action on that rule. This is equivalent to the current action named **Pass**.

5.6.1 Testing Rules for Identicality

Identicality requires that the base rule and all arguments are compared and deemed identical.

- **Actions:** Actions are not considered in the test for Identicality. For example, Rule_XYZ=Block and Rule_XYZ = Allow are identical. Outcomes are not subject to the Identicality test.
- **User Messages:** User messages are not considered in the test for Identicality. For example, Rule_XYZ ->MessageA and Rule_XYZ ->MessageB are identical. Outcomes are not subject to the identicality test.
- **Time Frame:**
 - Time frames are not considered in the test for Identicality. For example, Rule_XYZ ->TimeFrameA and Rule_XYZ ->TimeFrameB are identical.
 - Rules may have multiple Time frames, but are identical during the overlap of time frames.
- **Custom URL:** Rules containing URLs are identical **if** their specified URL expressions are identical.
- **URL Category:** Rules containing URLs categories are identical **if** their specified URL categories are identical.
- **File Type:** Rules containing File Types are identical **if** their specified File Types are identical.
- **File Extension:** Rules containing File Extensions are identical **if** their specified File Extensions are identical.
- **File Size:** File Size is not considered in the test for Identicality.
- **DLP Rules:** Rules containing DLP categories are identical **if** their DLP categories are identical and their DLP Destination URL expression is identical.
- **User Agent:** Rules containing User Agents are identical **if** the User Agent RegEx is identical or the User Agent String is identical.
- **Application Control:** Rules containing Application Controls are identical **if** the Application and User Action are identical.

5.6.2 Applying the Identicality Basic Principle to Time Rules

The basic principles state: "Users cannot author identical rules at any scope". For time frames, this applies to overlapping times. Users cannot author identical rules at any scope where both rules would be active at the same time.

Identical rules with overlapping schedule periods are resolved by the Hierarchy Principle, which states that "Rule precedence occurs from the bottom up" and therefore the child policy overrides the parent policy during any overlapping time period of identical rules.

For example:

- Custom_URL is set to *block* in the parent for all times (meaning no time frame is applied)
- Custom_URL is set to *allow* in the child for 12pm to 1pm every day.
- User visits Custom_URL and identity matches the child policy.
- Result: Custom_URL is *allowed* from 12pm to 1pm (due to the Hierarchy Principle) and Blocked at all other times (again due to the Hierarchy Principle - since there is only one valid rule during those times, the parent rule is enforced).
- Rules with different (non-overlapping) time frames can coexist whether authored at the same scope (both in the child) or different scopes (in a parent and a child).

5.7 Specificity

Precedence for rules with "overlapping" arguments is determined by the degree of argument specificity.

For example, `mail.google.com` is a more specific argument than `*.google.com`. If these rules exist in the same scope then the outcome would be that for `mail.google.com`

5.7.1 Testing Arguments for Specificity

- **URL:** The more qualified domain name wins, and if they are equal then the one with the most matching path segments prevails.
- **URL Lists:** URLs in a URL list are treated as multiple rules. There is no specificity problem - Conflicts are resolved by the Priority Principle
- **File Restrictions:**
 - True file type
 - Single file types take precedence over file type groups. For example, `word-doc` takes precedence over `office-docs`
 - See Appendix B for true file type groups
- **File Extensions:**
 - Single file extensions take precedence over File extension groups. For example, `.zip` takes precedence over "Archive" group.
 - See Appendix A for file extension groups
 - Wildcards for file extensions cannot be input by the user
- **File Size:** File size is limited to a single rule per policy level. There is no specificity problem. File size rule overrides parent by the Hierarchy Principle if the size argument is changed.
 - There is no precedence between the file restriction types. The Priority Principle determines the outcome of multiple matching rules.
- **URL Categories:** There is no specificity problem - Conflicts are resolved by the Priority Principle.
- **URL Categories and Custom URLs/URL Lists:** Custom URLs and Custom URL Lists are more specific than URL Categories.
- **Application Control:** Each Application/User Action in an Application Profile is treated as an individual rule. There is no specificity problem - Conflicts are resolved by the Priority Principle.

- **DLP:**
 - There is no specificity problem - conflicts are resolved by the Priority Principle.
 - DLP policies can contain URL arguments - specificity conforms to the URL test.
- **User Agents:**
 - User agents can be defined (predefined) by Trustwave as regular expressions.
 - User agents can be defined by users as explicit strings with wildcards. Wildcards can be leading, trailing, or contained within the string.
 - Wildcards must be entered explicitly.
 - Conflicts with two User Agent definitions are resolved by the Priority Principle.

5.8 Stopping Logic

Evaluation of policy happens by evaluating each Policy Node that matches the end-user's identity until a stopping point is reached. The order of Policy Node evaluation is determined by the Specificity Principle applied to identity as described above. After all rules are evaluated in a Policy Node, if any explicit Actions are triggered, then the appropriate Action is used and the policy evaluation stops. If after all rules in a Policy Node are evaluated and no explicit Actions are triggered, the next Policy Node is evaluated. This continues until all Policy Nodes matching identity are evaluated. If there is still no explicit action at that time, then the transaction is allowed.

- Explicit Actions: Whitelist, Block, Coach, Allow
- Non-explicit Actions: X-Ray, Pass

For example:

- End user is "User1" and a member of "Group1" and "Group2"
- "Group1" has been set as a higher priority than "Group2"
- Line Item Exception 1 has User1 assigned
- Line Item Exception 2 has User1 assigned
- Named Policy 1 has User 1 assigned
- Line Item Exception 3 has Group1 assigned
- Line Item Exception 4 has Group1 assigned
- Named Policy 2 has Group1 assigned
- Line Item Exception 5 has Group2 assigned
- Line Item Exception 6 has Group2 assigned
- Named Policy 3 has Group2 assigned
- End user browses the web.

- Line Item Exception 1 and Line Item Exception 2 are evaluated (as a Policy Node)
 - Stopping Point: If there is an explicit Action from either Line Item Exception, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Named Policy 1 is evaluated (getting Actions for all Rule Types that match)
 - Stopping Point: If there is an explicit Action, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Line Item Exception 3 and Line Item Exception 4 are evaluated (as a Policy Node)
 - Stopping Point: If there is an explicit Action from either Line Item Exception, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Named Policy 2 is evaluated (getting Actions for all Rule Types that match)
 - Stopping Point: If there is an explicit Action, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Line Item Exception 5 and Line Item Exception 6 are evaluated (as a Policy Node)
 - Stopping Point: If there is an explicit Action from either Line Item Exception, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Named Policy 3 is evaluated (getting Actions for all Rule Types that match)
 - Stopping Point: If there is an explicit Action, use the Action that has precedence and stop. If there are no explicit Actions, continue.
- Default policy is evaluated (getting Actions for all Rule Types that match)
 - Stopping Point: If there is an explicit Action, use the Action that has precedence and stop. If there are no explicit Actions, Allow and stop.

6 Policy Test

After you configure your SWG Cloud policies, you can test them against URLs, websites, and IP addresses on the **Policy Test** tab.

Secure Web Gateway > Policy Test Customer1_SWG

Execute Policy Test

URL * IP Address

User Agent * Date & Time

User Group

Policy Test Result

Category

Action Rule

Configurations

Policies

Scanner Details

Details

Scan Type	Rule Type	Rule	File Name	File Size	Action
Request	URL List	Social Media Sites		0	
Request	File Extension	Web Pages - Empty_File_Name		0	
Request	File Extension	Empty File Extension - Empty_Fi		0	
Request	Authentication Method	Identify by headers		0	
Request	URL Category	Online Communities		0	
Request	URL Category	Web Logs/Personal Pages		0	
Response	File Type	Web Page - HTML Web Page		584379	

6.1 Start with a Simple Test

Enter a complete URL (including the protocol) and click **Go**. SWG Cloud will access the site, test for any malicious behavior and the default policy, and return a variety of information. (Not all of this information appears for every site.)

- The site status (such as whitelisted or blacklisted)
- The SWG Cloud Category applied to the site (if any)
- Action Rules that applied
- A list of redirections made while accessing the site (if any)
- Detailed Configuration and Policy results. To see details, expand the sections by clicking the arrows.

You can save these results to a file in JSON format by clicking **Save to File**. Afterwards reset the form, by clicking **Reset**.

6.2 Tests for Complex Rules and Policies

You can also execute more complex tests that includes the following options. By default, SWG Cloud tests the default policy and looks for malicious behavior. By adding more information, you can test other rules or policies and see if they limit access to sites according to user ID, groups or time.



Tip: Run multiple tests for positive results (the access is allowed) and negative results (access is correctly denied). You can enter and change this information as many times as you want to ensure that your rules work.

- User Agent – Enter the web browser or application name that you want to simulate in the test.
- User – Enter the name of the user you want to imitate. To see a list of available users, see **Configuration | Users**.

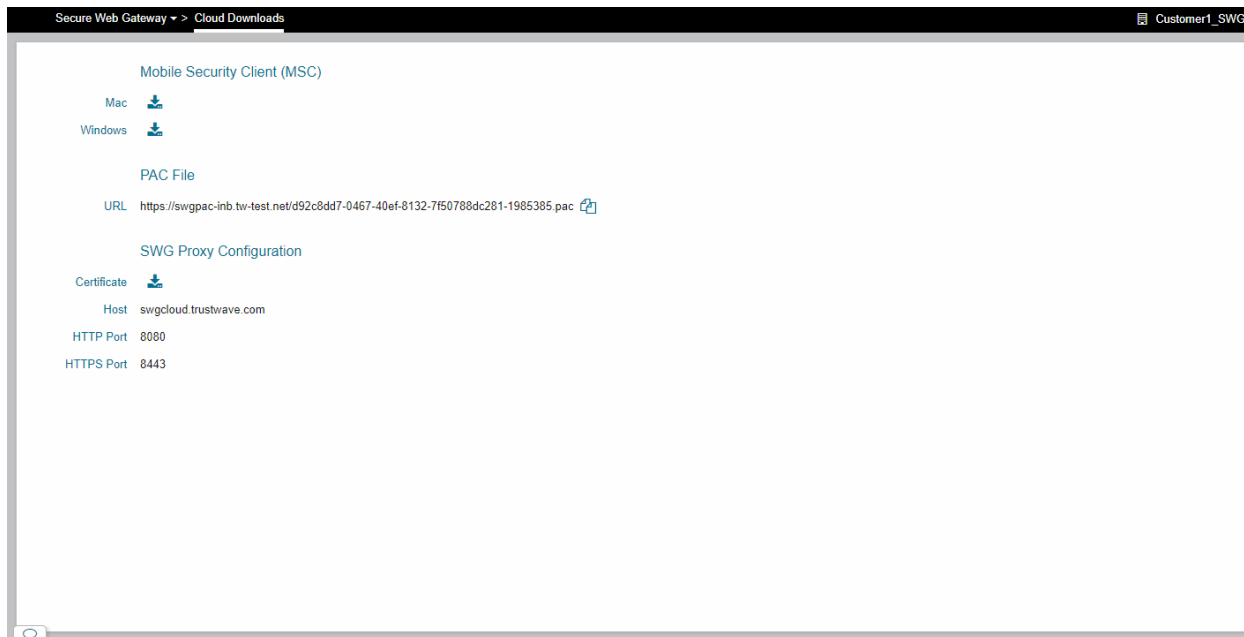


Note: The username does not have to exist in SWG Cloud. SWG Cloud can infer usernames, groups, and IP addresses from transaction logs. Including this information provides SWG Cloud with context so that the policy test can return information about why a transaction with that context is allowed, blocked, or more.

- IP address – Enter an IPv4 or IPv6 address to the server you want to test your policy against
- Date and Time – Use this setting to test rules or policies that include a time frame. Use the format yyyy-mm-dd hh:mm. The default is the day and time you opened the page.
- Group – Enter a group that you want to imitate int the test. To find available groups, start typing.
- URL – the address of the site you want to test your policy against.

7 Cloud Downloads

After your configurations are set and policies tested, it is time to enforce SWG Cloud's policies on the web traffic coming into your organization. You can do this by downloading and installing the Mobile Security clients to use the SWG Cloud service as a web proxy and are available on the **Cloud Downloads** tab.



Caution: Both the MSC and PAC files are customized to their SWG customer. If your TrustKeeper account can configure more than one SWG customer, be sure to select the correct customer (at top right of the page) before downloading or copying the items on this page.

The Mobile Security Client (MSC) forces a client's system to use SWG Cloud service from any location. It contains an internally bundled Proxy Auto-Config (PAC) file in the same system location that is used to define a PAC file. SWG Cloud also provides the PAC file for you to install yourself. To install the MSC, see section 5.1. To use the PAC file, see section 5.2.

7.1 Mobile Security Client

The Trustwave Mobile Security Client is the preferred redirection method for SWG Cloud and is available for Windows and MacOS. MSC allows SWG Cloud to control access for users' Internet access. MSC is an application that securely re-directs HTTP traffic from the user's computer to the SWG multi-tenant cloud servers.

The service identifies and authenticates users and machines using SAML or user names via request headers. MSC supports transparent identification. MSC enforces the browser configuration and MSC configuration to avoid user tampering. The MSC can be enabled or disabled.

You can also choose to enable automatic upgrades to the MSC client software. MSC will check for updated software hourly, and apply the changes as required.




Tip: To prevent users from uninstalling the MSC, see **Configuration | Settings** or per-user rules in **Configuration | Users** which are described section 4.4.

Table 6: Supported Versions of Platforms and Operating Systems

OS	Internet Explorer	Edge	Safari	Firefox	Chrome
Windows 7, 8, 8.1	11	N/A	N/A	55.0.3	60.0.3112
Windows 10	11.540.15632	40.15063	N/A	55.0.3	60.0.3112
MacOS X Mountain Lion	N/A	N/A	6.2.8	47.01	49.0.2623
MacOS X Mavericks	N/A	N/A	10.1.2	55.0.3	60.0.3112
MacOS Yosemite, El Capitan, Sierra	N/A	N/A	10.1.2	55.0.3	60.0.3112

To install the MSC:

1. On the **Cloud Downloads** tab, click the **Downloads** icon  for the appropriate type of operating system.
 - a. For Windows:
 - i. When the download is complete, open the file.
The **Trustwave Mobile Security Client Setup** wizard opens.
 - ii. In the **Installer Language** dialog, select a language and click **OK**.
 - iii. On the **License Agreement** page, mark the **I accept the terms of the License Agreement** checkbox and click **Install**.
 - iv. When the installation is complete and the wizard instructs you to, click **Finish**.
 - b. For MAC:
 - i. Save the file and double click it to open.



Caution: For macOS Sierra and later operating systems, downloading the MSC installer for Mac from the Platform causes the system to quarantine the install file and it will fail when run.

To resolve this, the file must be removed from quarantine before running the installation. After removal, the installer can be distributed within the organization using an internal server, where the installer is placed for distribution, or via email or Group Policy Object (GPO) and silent installation.

The terminal command to remove the attribute is:

```
xattr -rd com.apple.quarantine [path/to/downloaded/installer/tgz/file]
```

After removal, the archive can be uncompressed. Double-click the installer to run it.

- ii. Right click and open the **MobileSecurityClient-[version]-installer.mpkg** file.
- iii. If a warning appears, click **Open**.
The **Install Mobile Security Client** wizard opens
- iv. Click through the wizard to its end.
- c. On the **Welcome to the Mobile Security Client Installer** page, click **Continue**.
- d. On the **Software License Agreement** page, click **Continue**.
- e. When asked, click **Agree** to accept the End User License Agreement.
- f. On the **Select a Destination** page, click **Continue**.
- g. On the **Standard Install** page, click **Install**.
- h. If asked, enter the username and password that you use to log into your computer.
- i. In the confirmation, click **Continue Installation**.
- j. On the next page, click **Restart**.

7.2 PAC File

To use the PAC, copy and paste the URL provided into your browser proxy configuration settings. You can use Windows Group Policy or similar tools to push the setting to networked computers.



Note: You can also download the file and serve it from your network or a local disk. However, if you or Trustwave make any changes in the SWG Cloud PAC configuration, you must then update all local copies.

To configure additional settings in the PAC file, see the **Configuration | Settings | Advanced** tab which is described in section 4.1.3.

Appendix A: List of Provided Web Site Categories

Trustwave maintains and updates these categories frequently. Below is a list of the available Web site categories as of the publication of this document. An asterisk (*) denotes a category which contains patterns.

Category	Description
Adware	<p>Sites that promote or offer software that collects information about users to display target advertisement based on user browsing patterns and/or install advertising toolbars with the user's knowledge and consent.</p> <p>Sample sites: www.toolbardearquitectura.com, www.toolbarnet.com, www.bahaitoolbar.com</p>
Alcohol	<p>Sites promoting the use of alcohol, including drink recipes, home brewing methodology, advertisements, etc.</p> <ul style="list-style-type: none"> • Sites promoting the use of alcohol for consumption purposes, including pubs, bars, breweries, alcohol manufacturers • Sites which contain drink recipes, bartenders' guides, or drinking games • Sites which advertise or contain advertisements for alcohol <p>Informational sites such as essays on drunk driving or court transcripts WILL NOT be added to this category.</p> <p>Sample sites: www.budweiser.com, www.samueladams.com, www.jackdaniels.com</p>
Animals/Pets	<p>Sites that provide information or promote animal/pet care, breed, veterinary care, boarding, adoption, and care info.</p> <p>Sample sites: www.petsonsale.com, www.westminsterkennelclub.org, www.2buyhorses.com</p>
Art	<p>Non-commercial websites that promote, exhibit, and/or display works of art, artists, and provide instruction on the creation of art excluding the following:</p> <ul style="list-style-type: none"> • Explicit Art • Sites for artists, art galleries, or museums • Sites containing art instruction, graphics tutorials, and art schools (which should also be saved in Education) <p>Sample sites: www.lacma.org, www.guggenheim.org, www.metmuseum.org</p>
Bad Reputation Domains	<p>Sites that appear on one or more security industry blacklists for repeated bad behavior, including hosting malware and phishing sites, generating spam, or hosting content linked to by spam email.</p>

Category	Description
Banner/Web Ads	<p>Banner ads served from third party servers and URLs that track online analytics and/or website traffic for marketing report purpose.</p> <p>Sample sites: www.coremetrics.com, www.siteminer.com, www.valueclickmedia.com, www.mointel.com</p>
Books & Literature	<p>Sites that discuss and promote books, literature, and periodicals distributed with the intention of providing entertainment.</p> <ul style="list-style-type: none"> • Authors' sites, publishers' promotional sites (not "How To Publish" or "Let Us Publish Your Book") • Online books (i.e., Project Gutenberg, eBooks, etc.) • Books on Tape • Literary Reviews • Fan-Fiction or other short fiction works • Written screenplays/scripts (movies, tv, or drama) <p>Sample sites: www.bookbrowse.com, www.ebooks.com, www.danbrown.com</p>
BotNet	<p>Sites used by botnet herders for command and control of infected machines. Sites that known malware and spyware connects to for command and control by cyber criminals. These sites are differentiated from the Malcode category to enable reporting on potentially infected computers inside the network.</p>
Chat	<p>Sites offering chatrooms and chat services as well as chat sites accessed via a web browser, excluding the following:</p> <ul style="list-style-type: none"> • Instant Messaging • Chat logs • IRC client downloads • IRC channel listings or channel information <p>Sample sites: www.chatweb.net, www.chat-avenue.com, www.javachatrooms.net</p>
Child Pornography	<p>Sites that promote, discuss or portray children in sexual acts and activity or the abuse of children. Pornographic sites that advertise or imply the depiction of underage models and that do not have a U.S.C. 2257 declaration on their main page. As of March 13, 2007, all sites categorized as child porn are actually saved into the URL Library in the Porn category and are automatically submitted to the Internet Watch Foundation for legal verification as child pornography (http://www.iwf.org.uk/). If the IWF agrees that a site and/or any of its hosted pages are child pornography, they add it those URLs to their master list. The master list is downloaded nightly and saved into the URL Library in the Child Pornography category.</p>

Category	Description
Comics	<p>Sites that distribute, display, discuss and promote comics, comic books, and cartoons. These include on-line cartoons and official websites of comic strips.</p> <ul style="list-style-type: none"> • Web comics • Flash/Online animations and cartoons • Comic publishers (should also be saved in literature) <p>Sample sites: www.dccomics.com, www.marvel.com, www.xkcd.com</p>
Community Organizations	<p>Sites of non-profit, charity, and community involvement organizations, i.e., YMCA, March of Dimes, Big Brothers/Sisters, Boy/Girl Scouts, etc.</p> <p>Sample sites: www.habitat.org, www.pointsoflight.org, www.national.unitedway.org</p>
Criminal Skills	<p>Sites that promote crime or illegal activity such as credit card number generation, illegal surveillance and murder.</p> <p>Sites which commercially sell surveillance equipment will not be saved.</p>
Dating/Personals	<p>Contains those websites that are related to personal ads, dating sites, dating services, relationships, introductions, etc.</p> <ul style="list-style-type: none"> • Personal ads, dating services, dating tips, “how-to find a mate” sites • Sites which promote introductions for purposes of finding friends or other relationships • Sites for escort services should be saved in Porn. <p>Sample sites: www.friendfinder.com, www.match.com, www.eharmony.com</p>
Domain Landing	<p>Registered hosted pages with no significant appreciable content other than current owner info, solicitation for URL buyers, and or links to seller info.</p> <p>Sample sites: www.234aa.info, www.mt50ad.com, www.mbakery.com</p>
Dubious/Unsavoury	<p>Sites of a questionable legal or ethical nature. Sites which promote or distribute products, information, or devices whose use may be deemed unethical or, in some cases, illegal.</p> <ul style="list-style-type: none"> • Warez • Unlicensed mp3 downloads • Radar detectors • Street racing <p>Sample sites: www.thepayback.com, www.strangereports.com</p>

Category	Description
Dynamic DNS Servers	<p>Domains used by Dynamic DNS service providers for IP aliasing. Domains in this category should almost always be wildcarded, as they are typically assigned to end users with a customizable sub-domain.</p> <p>Sample sites: www.dynip.com, www.changeip.com, no-ip.info</p>
Edge Content Servers/Infrastructure	<p>Sites that host images, media and static secondary content for web sites. Sites in this category represent Internet “infrastructure”; they provide web companies with high-bandwidth delivery of arbitrary content. Typically, this content is never directly accessed by the end user. The user’s web browser automatically accesses these sites based on links embedded in the page of the original web site.</p> <p>Sample sites: edgefcs.net, speedera.net, akamai.net</p>
Education	<p>Websites of schools, learning centers, universities, and trade schools. Sites that promote and discuss materials and information that aid in teaching.</p> <ul style="list-style-type: none"> • Teaching institutions/workshops/technical institutes • Teaching aids, such as lesson planning guides • Teacher supplies (should also be saved in shopping) • Career development education • .edu sites <p>Sample sites: www.harvard.edu, www.usc.edu, www.bryman.edu</p>
Educational Games	<p>Sites that offer games related to education such as reading, spelling, math, etc.</p> <ul style="list-style-type: none"> • Developmental games • Games with educational value <p>Sample sites: www.aplusmath.com, www.discoveryschools.com, funschool.kaboose.com</p>
Employment	<p>Sites geared toward job seekers, such as online job bulletin boards, classified ad sites, resume-listing services, head hunting firms, etc.</p> <ul style="list-style-type: none"> • Resume building sites • Cover-letter writing sites <p>Sample sites: www.monster.com, www.careerbuilder.com, www.dice.com</p>

Category	Description
Entertainment	<p>All general entertainment sites excluding the following:</p> <ul style="list-style-type: none"> • Books & Lit • Comics • Movies & Television • Music Appreciation • Theater • Restaurants/Clubs <p>Sample sites: www.allfreeclipart.com, disneyworld.disney.go.com, www.ringophone.com</p>
Explicit Art	<p>Art websites that display art works containing graphic nudity, nude photography, sex acts and/or disturbing images.</p>
Fantasy Sports	<p>Sites that promote, discuss, provide advice on or provide automated management of fantasy sports teams and leagues.</p> <p>Sample sites: sportsillustrated.cnn.com/fantasy, games.espn.go.com, myfantasyleague.com</p>
Fashion	<p>Sites promoting and discussion of models, modeling, fashion and apparel in a non-commercial manner. May contain some R-rated material, or bikini pictures.</p> <ul style="list-style-type: none"> • Modeling portfolios • Modeling agencies • Modeling contests <p>Sample sites: www.fashion.net, www.fordmodels.com, www.ftv.com</p>
Financial Institutions	<p>Sites related to the financial trade, such as stock trading, financial news, online banking services, and trading exchanges.</p> <p>Sites for economics theory or business classes WILL NOT be saved in this category. These types of sites should be saved in Education.</p> <p>Sample sites: www.wellsfargo.com, www.fidelitymortgage.com, www.massmutual.com</p>

Category	Description
Fitness	<p>Sites promoting and discussing exercise, yoga, health clubs, nutrition and weight loss.</p> <ul style="list-style-type: none"> • Gyms • Fitness equipment • Nutrition supplements • Diet information <p>Sample sites: www.weightwatchers.com, www.24hourfitness.com, www.yoga.com</p>
Flash Video*	<p>This pattern will identify flash video. Will also cover any flash video embedded in web-pages.</p>
Free Hosts	<p>Sites hosted by consumer oriented free hosts or ISPs.</p> <p>Sample sites: www.110mb.com, www.freehostia.com, www.000webhost.com</p>
Freeware/Shareware	<p>Sites that provide repositories of shareware and freeware for download.</p> <p>Sample sites: www.tucows.com, www.freewarehome.com</p>
Gambling	<p>Sample sites: www.casino.com, www.bookmaker.com</p>
Games	<p>Sites related to computer or other games, such as game download sites, online games, video, and electronic games. Sites that advertise and host online games as well as sweepstakes and giveaways. Sites that offer cheat codes.</p> <p>Sites about board games will also be saved in this category.</p> <p>Sample sites: www.playstation.com, www.warcraft.org, www.gamefaqs.com</p>
Games Patterns*	<p>Patterns and URLs which block access to the following games:</p> <ul style="list-style-type: none"> • World of Warcraft • The Steam Network • Half-Life • Half-Life2 • Team Fortress • Counterstrike • Any other games accessed through the Steam Network • Second Life • LineageII

Category	Description
General Business	<p>Websites for businesses and commercial organizations where business is defined as an organization that provides goods and/or services for profit.</p> <ul style="list-style-type: none"> • Business to Business <p>Sample sites: www.pg.com, www.kraft.com, www.tyco.com</p>
Generic IM	<p>Web sites pertaining to Instant Messaging and the download of instant messaging clients.</p>
Generic Remote Access	<p>Web sites pertaining to the use of or download of remote access clients.</p>
Generic Streaming	<p>Web sites designed to offer streaming media.</p>
Google Chat*	<p>Patterns which block the use of Google Chat messaging client.</p>
Google Talk*	<p>Patterns which block the use of Google Talk messaging client.</p>
GoToMyPC*	<p>Patterns which block the use of GoToMyPC remote desktop services.</p>
Government	<p>Sites of governmental agencies at a national, state, local or international level.</p> <ul style="list-style-type: none"> • .gov <p>Sample sites: www.ca.gov, www.whitehouse.gov, www.europa.eu</p>
Hacking	<p>Sites discussing and/or promoting unlawful or questionable tools or information revealing the ability to gain access to software or hardware/communications equipment and/or passwords.</p> <ul style="list-style-type: none"> • Password generation • Compiled binaries • Hacking tools • Software piracy (game cracking)
Hate & Discrimination	<p>Sites that contain material related to the discrimination of any group of people based on race, religion, gender, nationality, etc.</p> <ul style="list-style-type: none"> • Sites which concentrate on violence or the destruction of human life, including a single person or an entire race/religion/gender/etc. • Sites focused on the superiority of one race/religion/gender/etc., while degrading others with use of propaganda or violent action. • Sites which discriminate or promote discrimination based on race/religion/gender/etc., or support and promote partisan historical opinion. <p>Sample sites: www.kkk.com, www.nazi.org, www.stormfront.org</p>

Category	Description
Health / Medical	<ul style="list-style-type: none"> • Sites of medical practices, hospitals, health insurance providers, nursing homes, and care centers. • Sites that promote and provide information on prescription medicines and over the counter treatments. • Sites offering information and references on health, medicine, preventative health care and other health-related topics. <p>Sample sites: www.webmd.com, www.bluecross.com, www.stjude.org</p>
Holistic	<p>Sites offering information on alternative medicines and natural healing.</p> <ul style="list-style-type: none"> • Homeopathic medicine • Acupuncture and acupressure • Chakra alignment • Feng Shui <p>Sample sites: www.holisticmed.com, www.findhealer.com, www.holistic.com</p>
Humor	<p>Sites whose primary purpose is for comedy, jokes, fun, etc.</p> <ul style="list-style-type: none"> • Any site containing jokes, sound files, or other material intended to be funny. <p>Sample sites: www.101funjokes.com, www.jokesandhumor.com, www.funny.com</p>
ICQ_and_AIM*	<p>Patterns which block the use of both the ICQ and AOL Instant Messaging clients.</p>

Category	Description
Illegal Drugs	<p>Sites that promote the use or purchase of illegal drugs. These may include offering marijuana, growing methods, techniques and products for testing clean for drugs, information on acid and/or “mushrooms,” and all other forms of narcotics.</p> <ul style="list-style-type: none"> • Promotes sale/use of illegal narcotics • Instructs on making or growing illegal narcotics • Promotes sale/use of paraphernalia for express use with illegal narcotics • Promotes illegal sale/use of LEGAL narcotics • Promotes techniques/products for testing clean with drug tests • Glorifies the effect of illegal narcotics • Promotes sale/use of questionably legal “supplements” with a narcotic effect • Sites which deal with information about illegal substances or their effects (i.e., police department page informing parents what to look for) WILL NOT be saved. <p>Sample sites: www.hightimes.com, www.homegrownfantasy.com, www.erowid.org</p>
Image Servers & Image Search Engines	<p>Web servers and search engines whose primary function is to deliver images, artwork, personal photos, photo galleries, and free images/pictures for commercial use. (Does not include adult content categorized elsewhere.)</p> <p>Sample sites: images.google.com, www.flickr.com, www.istockphoto.com</p>
Information Technology	<p>Sites containing reviews, discussions, distribution, and promotion of computer programs, software, systems and hardware. Sites that contain discussion, reviews, news, and advocacy on computers, technological devices, and general technology. Sites which offer information, resources, hosting and guides for the creation of computer software and websites.</p> <p>Sample sites: www.cnet.com, www.zdnet.com, www.slashdot.org</p>
Instant Messaging (IM)	<p>Sites that offer and enable the download of instant messaging.</p> <ul style="list-style-type: none"> • Client-based applications for IM • Central servers for IM applications <p>Sample sites: www.aim.com, www.icq.com, messenger.msn.com</p>
Internet Radio	<p>Sites that offer streaming radio internet programming and podcasts.</p> <ul style="list-style-type: none"> • Does not include downloadable music. <p>Sample sites: launch.yahoo.com/launchcast/, www.live365.com, www.shoutcast.com</p>

Category	Description
Internet Service Provider	Sites and guides to services that offer access to the Internet. Sample sites: www.aol.com/ , www.earthlink.com/ , www.netzero.net/
Invalid Web Pages	Sites where a domain may be registered but not content is served or the server is offline. Sample sites: tvoynfreeblog.com , newsexpress.de , chain-shoemould.com
Kids	Child friendly sites. Sites designed specifically for children. (Does not include educational games.) Sample sites: www.coloring-crafts.com , www.4krafytkidz.com , www.maisyfunclub.com
Legal	Sites pertaining to legal services, personal legal reference and on-line legal aid. <ul style="list-style-type: none"> • Law firms • Legal reference • Law libraries • Legal services (notaries, etc.) Sample sites: www.lawyers.com , www.lawreview.org , www.worldlawdirect.com
Lifestyle & Culture	Sites that contain material relative to an individual's personal, community or cultural identity, or organizational/club affiliations. <ul style="list-style-type: none"> • Sites on political or religious affiliation WILL NOT be saved. Sample sites: www.aboriginalculture.com.au , www.glaad.org , www.vegetarianteen.com
Local Community	Sites of community governmental agencies and sites that promote and announce community events and community involvement. <ul style="list-style-type: none"> • City websites • County websites • Chamber of Commerce Sample sites: www.toronto.com/section/community/ , www.dallascityhall.com , www.sanpedro.com
Malicious Code/Virus	Sites that promote, demonstrate and/or carry malicious executable, virus or worm code that intentionally causes harm by modifying or destroying computer systems often without the user's knowledge.
Meebo*	Patterns which block the use of the Meebo messaging client.

Category	Description
Message Boards	<p>Websites that offer message boards, bulletin boards, and forums. Websites which offer visitors the ability to discuss topics with one another via Internet message board software. Websites that provide downloads and customizations of web message board software.</p> <p>Also includes guestbook sites (i.e., Dreambooks)</p> <p>Sample sites: www.aimoo.com, www.messages.yahoo.com, www.boards.fool.com</p>
Military Appreciation	<p>Sites that pertain to individual appreciation, remembrance or dedication to military units and organizations.</p> <ul style="list-style-type: none"> • Veterans • Troop Support • Honoring military divisions <p>Sample sites: www.nmam.org, www.uso.org, www.oldglorytraditions.com</p>
Military Official	<p>Official websites of government backed military organizations. The entire .mil top-level domain.</p> <p>Sample sites: www.navy.mil, www.army.mil, www.usmc.mil</p>
Movies & Television	<p>Sites that discuss and promote film and television. This includes official sites of movies and television programs as well as those of film and television celebrities. Also included are personal fan sites of the aforementioned.</p> <p>Sample sites: www.movies.yahoo.com, www.tvguide.com, www.moviefone.com</p>
MSN_Messenger*	<p>Patterns which block the use of the MSN messaging client.</p>
Music Appreciation	<p>Sites that discuss and promote music, musicians, and the methods in which they are distributed. These sites include official websites of musicians as well as fan sites that promote musical subjects and artists.</p> <ul style="list-style-type: none"> • Playlists • Lyrics • Legal/Licensed mp3 distribution <p>Sample sites: launch.yahoo.com, www.artistdirect.com, www.vibe.com</p>
My Space IM*	<p>Patterns which block the use of the MySpace messaging client.</p>
News	<p>Websites that distribute news, current events, and headlines.</p> <p>Sample sites: www.cnn.com, www.dailyregister.com, news.yahoo.com</p>

Category	Description
Obscene/Tasteless	<p>Sites that contain explicit graphical or text depictions of such things as mutilation, murder, bodily functions, horror, death, rude behavior, executions, violence, and obscenities etc.</p> <p>Sites which contain or deal with medical content WILL NOT be saved.</p>
Online Auction	<p>Sites that offer access to online auctions where visitors can bid on various items. Since online auctions are rarely monitored, they may expose users to materials that would otherwise be filtered under categories such as Adult Content, Illegal/Questionable, etc. (Does not include classified advertisements, which is categorized under shopping or news.)</p> <p>Sample sites: www.ebay.com, www.ubid.com, www.bid-alot.com</p>
Online Classes	<p>Sites that provide access to classes conducted via the Internet.</p> <p>Sample site: www.virtualprofessors.com, www.courseadvisor.com, www.hpschooldesigntraining.com</p>
Online Communities	<p>Sites that promote online social networking. The content of such sites is mostly comprised of personal pages linked together in a social network that can be based on any criteria, such as schools, universities, business, or friendship.</p> <p>Sample sites: www.myspace.com, www.facebook.com, www.linkedin.com</p>
Online Greeting Cards	<p>Sites that offer e-greeting cards or e-postcards.</p> <p>Sample sites: www.bluemountain.com, www.yahoo.americangreetings.com, www.hallmark.com</p>
Online Trading/Brokerage	<p>Sites that facilitate online active trading of securities.</p> <p>Sample sites: www.etrade.com, www.tdameritrade.com, www.scottrade.com</p>
Paranormal	<p>Sites dealing with subjects of the paranormal. This includes topics such as mysticism, UFOs, Astrology, Numerology, the Occult, and conspiracy theories.</p> <ul style="list-style-type: none"> • Tarot • Crypto-zoology <p>Sample sites: www.paranormalnews.com, www.prairieghosts.com, astrology.yahoo.com</p>
pcAnywhere*	Patterns which block the use of the pcAnywhere remote desktop application.
Peer-to-Peer / FileSharing*	Patterns which block the use of peer-to-peer file sharing networks.

Category	Description
Phishing	Deceptive information pharming sites that used to acquire personal information for fraud or theft. Typically found in hoax e-mail, these sites falsely represent themselves as legitimate Web sites to trick recipients into divulging user account information, credit card numbers, usernames, passwords, social security numbers, etc. Pharming, or crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.
Political Opinion	Opinions dealing with political concerns such as party platforms, political reform, candidate advocacy, PACs, lobbying organizations, etc. <ul style="list-style-type: none"> • Campaign sites • “the president sucks” sites • Recall sites <p>Sample sites: www.gop.com, www.democrats.org, www.nra.org</p>
PoPo*	Patterns which block the use of the PoPo messaging client.
Pornography/Adult Content	<ul style="list-style-type: none"> • Sites that portray sexual acts and activity. • Sites that portray sexual acts or simulated sexual acts. • Sites with explicit nudity (including see-through clothing) that reveals in whole or part, nipples, bare butts, or sexual organs • Frontal nudity • Sex toys • Sites with links that lead to nude pictures • Sexual fluids • Explicit sex stories/writings • Oral activity on sexual parts • Bestiality • Bathroom fetishes • Any bizarre sex acts of objects with sexual organs • Porno videos for sale with explicit descriptions of tape and/or pictures • Swinger sites containing sexual pictures or descriptions • Any adult verification system sites that doesn't have sample pictures • Descriptions of sex sites that require credit card or payment or membership ID • Fetishes
Portals	Sites whose primary purpose is to offer entry point service to other Web sites via links sorted by topics and/or subjects. <p>Sample sites: www.top10links.com, www.dmoz.org</p>
QQ*	Patterns which block the use of the QQ messaging client.

Category	Description
QuickTime Video*	Patterns which block the streaming of QuickTime video content.
R Rated	<p>Services pertaining to anything that involves 18 and over material such as lingerie, swimsuits, and revealing pictures. Sites that are adult in nature without being explicitly pornographic.</p> <p>Sample sites: www.lingerie.com, www.maximonline.com, www.bikini.com</p>
Real Estate	<p>Sites pertaining to the buying, selling, renting, and leasing of properties.</p> <ul style="list-style-type: none"> • Commercial and residential properties. • Sites for home loans WILL NOT be saved in this category. (Should be saved in financial.) <p>Sample sites: www.realestate.yahoo.com, www.move.com, www.realtor.com</p>
Real Time Streaming Protocol*	Patterns which block access to videos served using Real Time Streaming Protocol
Recreation	<p>Sites pertaining to outdoor activities and non-competitive athletic activities, such as hunting, fishing, camping, hiking, rock climbing. Sites that pertain to hobbies, collecting, clubs and social organizations. Sites pertaining to horticulture, gardening and yard maintenance. Sites pertaining to decorating and crafting.</p> <p>Sample sites: crochet.about.com, www.gardenweb.com, www.treasureclub.net, www.thebackpacker.com, www.snowmobilefanatics.com</p>
Reference	<p>Reference collections including encyclopedias, atlases, historical data, biographies, how-to, etc. Sites which offer language tools and references such as dictionaries, thesaurus, and translators. Information resources on scientific subjects. Science subjects include: biology, physics, mathematics, chemistry etc.</p> <p>Sample sites: dictionary.reference.com, www.britannica.com, www.yellowpages.com</p>

Category	Description
Religion	<p>Sites that pertain to mainstream religious institutions such as churches, temples, mosques, etc.</p> <ul style="list-style-type: none"> • Church sites (service times, location, church event calendars, etc.) • Sites with religious opinion or “witnessing” • Sites that pertain to discussion and/or advocacy of religious organizations, religious opinion and opinions formed from a religious viewpoint. • Sites promoting cult subject matter, use of mind control, paranoia, fear, and any other type of psychological control or manipulation. • Important distinction for GCD: Falun related sites are categorized as Religion in Taiwan. <p>Sample sites: www.zencenter.org, www.olacathedral.org, www.tbala.org, www.catholic.org, www.jewfaq.org, www.buddhanet.net, www.rael.org, www.heavensgate.com</p>
Remote Access	<p>Sites that provide information about or facilitate access to information, programs, online services, or computer systems remotely.</p> <p>Sample sites: pcnow.webex.com, www.remotelyanywhere.com, www.gotomypc.com</p>
Remote Desktop*	Patterns which block the use of remote desktop protocol.
Restaurant	<p>Sites that provide information, promote, list, review, or advertise dining, catering services, restaurants, cafes, eateries, take-outs, and fast food.</p> <p>Sample sites: www.mcdonalds.com, www.blackangus.com</p>
Reviewed / Miscellaneous	<p>Random content that does not fall under current categories.</p> <p>Sample sites: www.cmc-network.com.au, www.booking-centre.net, destracking.com</p>
School Cheating	<p>Sites that offer materials which enable students to plagiarize or cheat in their academic endeavors.</p> <ul style="list-style-type: none"> • Sites that offer pre-written papers • Sites that offer complete summaries intended for circumventing research • Sites that offer answer keys • Sites that give methods of academic cheating • Sites that offer excerpts for the purpose of plagiarism <p>Sample sites: www.allfreeessays.com</p>

Category	Description
Search Engines	<p>Major portal sites that either search the Internet or have a directory-based database of sites. Includes all sub-URLs under the main site.</p> <p>Sample sites: www.yahoo.com, www.google.com, www.msn.com</p>
Secure Shell*	<p>Patterns which block the use of the Secure Shell (SSH) protocol.</p>
Self Defense	<p>Websites that offer information and advocacy of self-defense tools of a non-lethal nature. Techniques and products such as those designed to immobilize or harm a subject but not “intended” to cause death.</p> <ul style="list-style-type: none"> • Martial arts • Stun guns • Mace <p>Sample sites: www.ultimatejijitsu.com, www.safetyforwomen.com, www.selfdefenseproducts.com</p>
Self Help	<p>Sites that include information such as therapies, counseling services, motivation, conferences, articles, self-awareness, spirituality etc.</p> <ul style="list-style-type: none"> • Rape crisis centers • Sites that contain information on emotional and/or mental wellness. • Counseling services, conferences <p>Sample sites: www.stressless.com, www.oa.org, www.professional-counselling.com</p>
Shopping	<p>Sites that contain consumer oriented online shopping, online malls, classifieds, and online trading/auction services.</p> <p>Sample sites: www.amazon.com, shopping.yahoo.com, www.nordstrom.com</p>
Social Opinion	<p>Sites that contain opinion on a variety of social topics.</p>
Sports	<p>Sites for professional, collegiate, and other competitive baseball, basketball, hockey, football & soccer teams, sports magazines, sporting events such as winter & summer Olympics, etc.</p> <p>Also includes other competitive sports, such as NASCAR racing.</p> <p>Sample sites: espn.go.com, www.nba.com, sportsillustrated.cnn.com</p>
Spyware	<p>Sites that promote, offer, or secretly install software to monitor user behavior, track personal information, record keystrokes, and/or change user computer configuration without the user’s knowledge and consent for malicious or advertising purposes. Includes sites with software that can connect to “phone home” for transferring user information.</p>

Category	Description
Streaming Media	<p>Sites that offer “Internet TV” programming, streaming video, and other streaming media excluding:</p> <ul style="list-style-type: none"> • Internet Radio • Peer-to-Peer/File Sharing <p>Sample sites: www.apple.com/quicktime/, www.hulu.com</p>
Terrorist / Militant / Extremist	<p>Sites that contain information regarding militias, anti-government groups, terrorism, anarchy, etc.</p> <ul style="list-style-type: none"> • Anti-government/Anti-establishment • Bomb-making/usage (Should also be saved in criminal skills) <p>Sample sites: www.michiganmilitia.com, www.militiaofmontana.com, www.ncmilitia.org</p>
Theater	<p>Sites that promote and discuss live dramatic productions.</p> <p>Sample sites: www.chicagothemusical.com, www.lordofthedance.com, disney.go.com/theatre/</p>
Tickets	<p>Sites that offer ticket sales for entertainment: concerts, sporting events, races, expos, etc.</p> <p>Sample sites: www.ticketmaster.com, www.movietickets.com, www.sportstickets.net</p>
Tobacco	<ul style="list-style-type: none"> • Sites that sell or promote the use of tobacco related products. • Sites that sell cigarettes, cigars, chewing tobacco, etc • Sites that are specifically designed to glamorize the use of tobacco related products
ToToMoMo*	<p>Patterns that block the use of the ToToMoMo messaging client.</p>
Translation Services	<p>Websites that provide free online text and web page translation tools or web-based screen readers.</p> <p>Sample sites: babelfish.yahoo.com, www.freetranslation.com, www.webanywhere.cs.washington.edu</p>

Category	Description
Travel	<p>Sites that offer travel tickets and reservations, travel clubs, travelogues, visitor information bureaus, travel promotions, etc.</p> <ul style="list-style-type: none"> • Sites relating to traveling, such as travel agencies, cruise lines, airfare, etc. • Sites must be related to the travel industry; i.e., Disneyland will not be saved, but a page containing tourist travel information to Disneyland will. • Las Vegas hotels like the Bellagio should be saved in Travel. <p>Sample sites: www.expedia.com, www.travel.com, www.travelocity.com</p>
Vehicles	<p>Sites that discuss, promote, and offer information on cars, trucks, motorcycles, watercraft, aircraft, and other forms of transportation.</p> <ul style="list-style-type: none"> • Dealerships / car shows • Car parts and accessories • Street racing <p>Sample sites: www.ford.com, www.harley-davidson.com, www.cessna.com</p>
Video Sharing	<p>Sites that allow users to post, share and view videos. Usually, these sites should also be categorized as streaming media, and possibly R-rated. The video sharing category gives customers the ability to selectively block only viral video sites, which tend to affect productivity. The difference between video sharing and streaming media is that in video sharing the content is provided by a user community rather than the site operator.</p> <p>Sample sites: www.youtube.com, www.vimeo.com, video.yahoo.com</p>
Virtual Network Computing*	<p>Patterns the block the use of Virtual Network Computing (VNC) remote desktop applications.</p>
VoIP	<p>Sites that provide information and/or products to facilitate telephone calls using the Internet. VoIP (Voice over Internet Protocol) refers to a category of hardware and software that uses the Internet as a transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the PSTN.</p> <p>Sample sites: www.skype.com, www.lingo.com, www.vonage.com</p>
WangWang*	<p>Patterns which block the use of the WangWang messaging client.</p>
Weapons	<p>Sites that provide information and promote the collecting, maintenance, advocacy, and sales of legal firearms, knives, swords, and related items.</p> <p>Sample sites: www.remington.com, www.buckknives.com, www.swords.com</p>

Category	Description
Weather/Traffic	<p>Web sites that offer weather forecasts, weather updates, and traffic conditions/reports.</p> <p>Sample sites: www.weather.com, www.traffic.com, weather.yahoo.com</p>
Web Based Email	<p>Sites that offer online web-based e-mail services; this excludes ISPs, which provide standard POP or IMAP e-mail accounts, i.e., Hotmail, Yahoo Mail, etc.</p> <p>Sample sites: www.hotmail.com, www.gmail.com, mail.yahoo.com</p>
Web Based Storage	<p>Sites that offer storage for personal files on remote servers for backup or exchange purposes, i.e., Yahoo Briefcase, snapfish, PictureTrail, etc.</p> <p>Sample sites: www.filesanywhere.com, briefcase.yahoo.com, www.gotomypc.com</p>
Web Hosts	<p>Sites that offer domain names and Web space for hosting fee-based Web pages.</p> <p>Sample sites: www.bphosting.com, www.hoster.com, www.networksolutions.com</p>
Web Logs/Personal Pages	<p>Web sites from personal or non-commercial sources which feature commentary and articles written in a log or journal format (Blogs).</p> <p>Sample sites: www.mamasandbabas.com, www.philz-corner.com, www.hawkercentral.com</p>
Web-Based Newsgroups	<p>Sites that offer archives of Usenet postings.</p> <p>Sample sites: www.webnews-exchange.com</p>
Web-Based Productivity Apps	<p>Sites that host web-based applications for word processing, spreadsheets, collaboration, or project management. These sites have a potential for inadvertent data leakage and can be an impediment to efforts to enforce corporate standards for desktop applications.</p> <p>Sample sites: basecamphq.com, zoho.com, docs.google.com</p>
Web-based Proxies*	<p>URLs and patterns which block access to web-based proxies and anonymizers which are typically used to circumvent URL filtering.</p>
Windows Media Video*	<p>Patterns which block the streaming of Windows Media video files.</p>
Yahoo_IM*	<p>Patterns which block the use of the Yahoo messaging client.</p>

Appendix B: List of File Content Types

The table below shows file type selections that can be applied in SWG Cloud.



Tip: File type selection is made by "Container". A container can match one type, or a group of related types. You cannot create a rule for individual items listed in the "Contents" column.

Some types are present in more than one container. For example, Microsoft Word documents are in the Documents container, the Microsoft Office Document container, and the Microsoft Word Document container

Container (File type selection)	Contents matched
7z Archive	<ul style="list-style-type: none"> 7z compressed Archive
ACE Archive	<ul style="list-style-type: none"> ACE compressed Archive
Active binary content	<ul style="list-style-type: none"> ActiveX control Embedded ActiveX control Embedded Cabinet Archive Embedded Jar Archive Embedded Java Class executable File Jar Archive Java Class Microsoft Cabinet Archive
Active Textual Web Content	<ul style="list-style-type: none"> CSS File JavaScript JavaScript Object Notation MS Encoded JavaScript MS Encoded Standalone JavaScript MS Encoded Standalone VB Script MS Encoded VB Script Standalone JavaScript Standalone VBScript VBScript Web Page
ActiveX Control	<ul style="list-style-type: none"> ActiveX control
Adobe Director Application	<ul style="list-style-type: none"> Adobe Director Application
Adobe Flash Application	<ul style="list-style-type: none"> Adobe Flash Application
Adobe Flash Application	<ul style="list-style-type: none"> Adobe Flash Application compressed

Container (File type selection)	Contents matched
Audio File	<ul style="list-style-type: none"> • APE • Audio File • Audio file-wav • MIDI File • MP3 Audio File • Mpeg Audio File • Real Audio • Real Media
AutoCAD drawing	<ul style="list-style-type: none"> • AutoCAD drawing
BMP Image	<ul style="list-style-type: none"> • BMP Image
BZ2 Archive	<ul style="list-style-type: none"> • bz2 Archive
CAB Archive	<ul style="list-style-type: none"> • Microsoft Cabinet Archive
CAB Archive	<ul style="list-style-type: none"> • Embedded Cabinet Archive
CAP File	<ul style="list-style-type: none"> • CAP File
CFF File	<ul style="list-style-type: none"> • CFF File
CSS File	<ul style="list-style-type: none"> • CSS File
DIET compressed	<ul style="list-style-type: none"> • DIET compressed

Container (File type selection)	Contents matched
Documents	<ul style="list-style-type: none"> • AutoCAD drawing • Internet explorer cache • Lotus 1-2-3 • Microsoft Access Database • Microsoft Excel 2007 Binary Document • Microsoft Excel 2007 OpenXML Document • Microsoft Excel 97-2003 Binary Document • Microsoft Excel Document • Microsoft Office Document • Microsoft Outlook MSG Document • Microsoft PowerPoint Document • Microsoft Word 2007 OpenXML Document • Microsoft Word 97-2003 Binary Document • Microsoft Word Document • Netscape Communicator address book • OpenOffice Database • OpenOffice Formula Document • OpenOffice Graphics Document • OpenOffice Presentation Document • OpenOffice Spreadsheet Document • OpenOffice Text Document • Outlook express Archive • Outlook folder • Registry files • Rich Text Format • Web browser cookie files
DOS Executable File	<ul style="list-style-type: none"> • DOS executable
Embedded Active Content	<ul style="list-style-type: none"> • Embedded ActiveX control • Embedded Cabinet Archive • Embedded Jar Archive • Embedded Java Class
Embedded ActiveX Control	<ul style="list-style-type: none"> • Embedded ActiveX control
Embedded Archive	<ul style="list-style-type: none"> • Embedded Cabinet Archive • Embedded Jar Archive
Embedded Java Class	<ul style="list-style-type: none"> • Embedded Java Class
GIF Image	<ul style="list-style-type: none"> • GIF Image

Container (File type selection)	Contents matched
GZIP Archive	<ul style="list-style-type: none"> gz Archive
HPACK Archive	<ul style="list-style-type: none"> HPACK Archive
Icon image	<ul style="list-style-type: none"> Icon image
Image	<ul style="list-style-type: none"> Gif Image Icon image Image bmp Image png Jpeg Image PCX image data Tgif image data TIFF Image
INF File	<ul style="list-style-type: none"> INF File
Info-ZIP self-extract	<ul style="list-style-type: none"> Info-ZIP self-extract
JAM Archive	<ul style="list-style-type: none"> JAM Archive
Java Class	<ul style="list-style-type: none"> Java Class
Java Script	<ul style="list-style-type: none"> JavaScript JavaScript Object Notation MS Encoded Java Script MS Encoded Standalone JavaScript Standalone JavaScript
Java serialization data	<ul style="list-style-type: none"> Java serialization data
JNG video data	<ul style="list-style-type: none"> JNG video data
JPEG Image	<ul style="list-style-type: none"> JPEG Image
LHA Archive	<ul style="list-style-type: none"> LHA compressed Archive
LHA self-extract	<ul style="list-style-type: none"> LHA self-extract
Link File	<ul style="list-style-type: none"> link File
Lotus 1-2-3 document	<ul style="list-style-type: none"> Lotus 1-2-3
LZEXE compressed DOS executable	<ul style="list-style-type: none"> LZEXE compressed DOS executable

Container (File type selection)	Contents matched
LZEXE packer	<ul style="list-style-type: none"> LZEXE compressed
LZOP compressed data	<ul style="list-style-type: none"> LZOP compressed data
Macromedia Freehand 9 Document	<ul style="list-style-type: none"> Macromedia Freehand 9 Document
Mcrypt encrypted data	<ul style="list-style-type: none"> Mcrypt encrypted data
Microsoft Access Database	<ul style="list-style-type: none"> Microsoft Access Database
Microsoft Excel Document	<ul style="list-style-type: none"> Microsoft Excel Document Microsoft Excel 97-2003 Binary Document Microsoft Excel 2007 OpenXML Document Microsoft Excel 2007 Binary Document
Microsoft Excel Macro File	<ul style="list-style-type: none"> Microsoft Excel Macro File
Microsoft Office Document	<ul style="list-style-type: none"> Microsoft Excel 2007 Binary Document Microsoft Excel 2007 OpenXML Document Microsoft Excel 97-2003 Binary Document Microsoft Excel Document Microsoft Excel Macro File Microsoft Office Document Microsoft Office Scrap Object Microsoft PowerPoint Document Microsoft Word 2007 OpenXML Document Microsoft Word 97-2003 Binary Document Microsoft Word Document
Microsoft Office Document with Embedded Files	<ul style="list-style-type: none"> Microsoft Office Document with Embedded Files
Microsoft Office Document with Macros	<ul style="list-style-type: none"> Microsoft Office Document with Macros Microsoft Excel Macro File
Microsoft Office Scrap Object	<ul style="list-style-type: none"> Microsoft Office Scrap Object
Microsoft Outlook MSG Document	<ul style="list-style-type: none"> Microsoft Outlook MSG Document
Microsoft PowerPoint Document	<ul style="list-style-type: none"> Microsoft PowerPoint Document
Microsoft Word Document	<ul style="list-style-type: none"> Microsoft Word Document Microsoft Word 97-2003 Binary Document Microsoft Word 2007 OpenXML Document

Container (File type selection)	Contents matched
MIME Content	<ul style="list-style-type: none"> Mail eml File
MNG video data	<ul style="list-style-type: none"> MNG video data
MP4 Video Image	<ul style="list-style-type: none"> MP4 video image
MS Encoded Java Script	<ul style="list-style-type: none"> MS Encoded Java Script MS Encoded Standalone JavaScript
MS Encoded VB Script	<ul style="list-style-type: none"> MS Encoded VB Script MS Encoded Standalone VB Script
MS Windows Html Help Data	<ul style="list-style-type: none"> MS Windows Html Help Data
MSI installation package	<ul style="list-style-type: none"> MSI installation package
Ogg Container	<ul style="list-style-type: none"> Ogg Container
OpenOffice Database	<ul style="list-style-type: none"> OpenOffice Database
OpenOffice Document	<ul style="list-style-type: none"> OpenOffice Database OpenOffice Formula Document OpenOffice Graphics Document OpenOffice Presentation Document OpenOffice Spreadsheet Document OpenOffice Text Document
OpenOffice Formula Document	<ul style="list-style-type: none"> OpenOffice Formula Document
OpenOffice Graphics Document	<ul style="list-style-type: none"> OpenOffice Graphics Document
OpenOffice Presentation Document	<ul style="list-style-type: none"> OpenOffice Presentation Document
OpenOffice Spreadsheet Document	<ul style="list-style-type: none"> OpenOffice Spreadsheet Document
OpenOffice Text Document	<ul style="list-style-type: none"> OpenOffice Text Document
Other	<ul style="list-style-type: none"> Octet stream

Container (File type selection)	Contents matched
Packed Executables	<ul style="list-style-type: none"> • ASPack compressed • Diet compressed • Executable compressed with Packer • Executable compressed with Unknown Packer • FSG compressed • LZEXE compressed • PECompact compressed • Petite compressed • PKLITE compressed DOS executable • PKSFX packer • UPX compressed Win32 Executable
PCX image data	<ul style="list-style-type: none"> • PCX image data
PDF File	<ul style="list-style-type: none"> • PDF File
PGP signature	<ul style="list-style-type: none"> • PGP signature
PIF-Windows Program Information	<ul style="list-style-type: none"> • PIF-Windows Program Information
PKLITE compressed DOS executable	<ul style="list-style-type: none"> • PKLITE compressed DOS executable
PKSFX packer	<ul style="list-style-type: none"> • PKSFX packer
PKZIP self-extract	<ul style="list-style-type: none"> • PKZIP self-extract
PNG Image	<ul style="list-style-type: none"> • Image png
PostScript File	<ul style="list-style-type: none"> • PostScript File
Potentially Malicious Packers	<ul style="list-style-type: none"> • ASPack compressed • FSG compressed • PECompact compressed • Petite compressed
RAR Archive	<ul style="list-style-type: none"> • rar Archive
Real Audio	<ul style="list-style-type: none"> • Real Audio
Real Media	<ul style="list-style-type: none"> • Real Media
Rich Text Format	<ul style="list-style-type: none"> • Rich Text Format

Container (File type selection)	Contents matched
Scannable Active Content	<ul style="list-style-type: none"> • ActiveX control • CSS File • Embedded ActiveX control • Embedded Cabinet Archive • Embedded Jar Archive • Embedded Java Class • HTML Web Page • Jar Archive • Java Class • JavaScript • JavaScript Object Notation • MS Encoded JavaScript • MS Encoded Standalone JavaScript • MS Encoded Standalone VB Script • MS Encoded VB Script • Standalone JavaScript • Standalone VBScript • VBScript
SCR File	<ul style="list-style-type: none"> • SCR File
Standalone Java Script	<ul style="list-style-type: none"> • Standalone JavaScript • MS Encoded Standalone JavaScript
Standalone VB Script	<ul style="list-style-type: none"> • Standalone VBScript • MS Encoded Standalone VB Script
Streaming	<ul style="list-style-type: none"> • Adobe Flash Video • Adobe Flash Video stream • Generic Streaming • MP4 video image • RealAudio Streaming • Video WebM • Winamp Streaming
TAR Archive	<ul style="list-style-type: none"> • tar Archive
Text File	<ul style="list-style-type: none"> • ASCII Text • Log or Text File • UUEncoded Text
TGIF image data	<ul style="list-style-type: none"> • TGIF image data

Container (File type selection)	Contents matched
TIFF image	<ul style="list-style-type: none"> • TIFF Image
Trustwave defined PDF image	<ul style="list-style-type: none"> • Trustwave defined PDF image
Trustwave defined RTF Variant	<ul style="list-style-type: none"> • Trustwave defined RTF Variant
Unix compressed data	<ul style="list-style-type: none"> • Unix compressed data
Unix Executable files	<ul style="list-style-type: none"> • ELF executable
Unscannable archives	<ul style="list-style-type: none"> • ACE compressed Archive • ARC Archive • ARJ Archive • Arj self-extract • HPACK Archive • Info-ZIP self-extract • JAM Archive • LHA Archive • LHA self-extract • Lzop compressed data • PKZIP self-extract • Unix compressed data • Zoo Archive data
Upload Data	<ul style="list-style-type: none"> • Upload Data
UPX compressed Win32 Executable	<ul style="list-style-type: none"> • UPX compressed Win32 Executable
URL File	<ul style="list-style-type: none"> • url File
UUEncoded Text	<ul style="list-style-type: none"> • UUEncoded Text
VB Script	<ul style="list-style-type: none"> • MS Encoded Standalone VB Script • MS Encoded VB Script • Standalone VBScript • VBScript
Video Image	<ul style="list-style-type: none"> • JNG video data • MNG video data • MP4 video image • Quicktime image • Video image
VRML File	<ul style="list-style-type: none"> • VRML

Container (File type selection)	Contents matched
Web Form	<ul style="list-style-type: none"> Web Form
Web Page	<ul style="list-style-type: none"> HTML Web Page
WinAmp plug-in	<ul style="list-style-type: none"> WinAmp plug in
Windows Executable File	<ul style="list-style-type: none"> ASPack compressed Diet compressed Executable compressed with Packer Executable compressed with Unknown Packer Executable File FSG compressed LZEXE compressed DOS executable PECompact compressed Petite compressed PKLITE compressed DOS executable PKSFX packer PKZIP self-extract SCR File UPX compressed Win32 Executable Winamp plug in Winzip Win32 self-extracting Archive
Windows help files	<ul style="list-style-type: none"> MS Windows Help
Windows Metafile	<ul style="list-style-type: none"> Windows Metafile
Windows registry files	<ul style="list-style-type: none"> Registry files
WinZip Self-extracting Archive	<ul style="list-style-type: none"> WinZip Self-extracting Archive
XML File	<ul style="list-style-type: none"> XML File
Zip Jar Archive	<ul style="list-style-type: none"> Embedded Jar Archive Jar Archive Zip Archive
ZOO Archive data	<ul style="list-style-type: none"> ZOO Archive data

Appendix C: Application Control User Actions

User actions provided by the various social media applications supported in SWG are continuously maintained. Where deemed necessary, lists are extended or adapted to reflect changes or extend the functionality.

User actions for the following social media are described in this section:

- Amazon Drive
- Apple iCloud Drive
- Box
- Dropbox
- Facebook
- Google Drive
- LinkedIn
- Microsoft OneDrive
- Twitter
- YouTube

Table 7: Amazon Drive

Action	Enables the User to ...
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System	Work in file system. (Create files and folders, copy, move, rename, delete)

Table 8: Apple iCloud Drive

Action	Enables the User to ...
Delete Permanently	Permanently delete files or folders
Download	Download
Upload	Upload files or folders
Work in File System (Create folder, Move)	Work in file system (Create folder, move)

Table 9: Box

Action	Enables the User to ...
Assign Task	Create, edit, and delete tasks
Change User Settings	Change user settings
Comment	Create, edit, and delete comments
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create new files and folders, Copy, Move, Rename, Delete, Sync to computer)	Work in file system (Create files and folders, copy, move, rename, delete, mirror data stored on Box to your desktop)

Table 10: Dropbox

Action	Enables the User to ...
Change User Settings	Change user settings
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or previous versions
Share	Share a new or existing folder, Import contacts, Allow members to invite others, send invites, uninvite, unshare folder, leave folder, remove folder, share link, remove link, get link
Upload	Upload files or folders
Work in File System (Create new folder, Copy, Move, Rename, Delete)	Work in file system (Create new folder, copy, move, rename, delete)

Table 11: Facebook

Action	Enables the User to ...
Add Friend	Add someone to their friend list
Add People to Group	Add friends to a created group
App or Game Bookmarks	Open an app or game already installed by the user
Apps or Games Category	Display the apps or games within the App Center category
Chat Send	Send a chat or direct message
Comment	Post a comment or reply to a post
Create an Ad	Create an advertisement to be shown in Facebook
Create a Page	Create a new Facebook page
Create Event	Create an event and invite friends
Create Group	Create a group
Edit Picture	Edit a photo

Action	Enables the User to ...
Like	Mark posts/comments/pictures/video as liked
Message Delete	Delete a message, messages, or a full conversation
Poke	Send or respond to a poke
Post or Share	Post a new status or share a post from another user
Remove People from Group	Remove people from a previously created group
Upload Picture	Upload a photo
Upload Video	Upload a video
Video Chat	Chat with video
Write a Note	Create a note

Table 12: Google Drive

Action	Enables the User to ...
Connect Apps To Drive	Connect apps to Google Drive
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create folder, Create google docs, Copy, Move, Rename, Delete)	Work in file system (Create folder, create google docs, copy, move, rename, delete)

Table 13: YouTube

Action	Enables the User to ...
Add Video to Playlist	Add a video to the playlist
Delete Video	Delete an uploaded video
Edit Video	Edit a video
Like or Dislike a Video	Mark a video as liked or disliked
Play Video	Play a video
Playlist Settings	Save playlist settings, delete playlist, delete video from playlist
Post Comment or Vote Up/Down	Comment on a video or vote a comment up or down
Share	Share this video, embed, email
Report Video	Report a video as offensive
Subscribe or Unsubscribe	Subscribe or unsubscribe to channel
Upload Video	Upload a video
VideoManager.Videos	Manage properties of the videos uploaded

Table 14: LinkedIn

Action	Enables the User to ...
Add Connections (Invite Contacts) or Connect	Add people to the user's connections
Comment	Make a comment to a post
Delete Message(s)	Delete a message or messages
Export Connections	Export information about connections to a file
Follow (Channel, Company, Member)	Follow the posts that a specific company is posting
Join Group	Join a group
Like	Mark a post or comment as liked
Post a job	Post a job in order to recruit

Action	Enables the User to ...
Remove Connections	Remove a connection from the user's connections
Send Message	Send a message to the user's connection(s)
Share	Share something with other users

Table 15: Microsoft OneDrive

Action	Enables the User to ...
Delete Permanently	Permanently delete files or folders
Download	Download
Restore	Restore deleted files or folders
Share	Share files or folders
Upload	Upload files or folders
Work in File System (Create new files and folders, Copy, Move, Rename, Delete)	Work in file system (Create files and folders, copy, move, rename, delete)

Table 16: Twitter

Action	Enables the User to ...
Create List	Gather profiles into a list
Delete	Delete a tweet
Follow	Start following a user
Send Message	Send a direct message to another user
Tweet or Retweet	Tweet or retweet

Appendix D: User Agents

Table 17: Predefined User Agent regular expressions and groupings

Name in user interface	User Agent	Regular Expression
Firefox 1.x	Firefox 1.x	.*Firefox/1\[0-9].*
Firefox 2.x	Firefox 2.x	(.*Firefox/2\[0-9].*)(.*BonEcho/2\[0-9].*)
Older and Unsafe Browsers	Firefox pre-1.0	.*?(Firefox Firebird)/0\..*?
Older and Unsafe Browsers	Internet Explorer 2.x, 3.x and 4.x	.*\((compatible; MSIE (2\. 3\. 4\.)).*
Older and Unsafe Browsers	Internet Explorer 5.x	.*MSIE ?5\..*
Older and Unsafe Browsers	Netscape 2.x and 3.x	.*Mozilla/(2\. 3\.).*
Older and Unsafe Browsers	Netscape 6.x	.*?Netscape6.*?
Older and Unsafe Browsers	Opera 5.x and 6.x	.*Opera(/)?(5\. 6\.).*
Older and Unsafe Browsers	Opera 7.x	.*?Opera(/)?7.*?
Netscape 7.x	Netscape 7.x	.*?Netscape/?7.*?
Media Players	QTS	.*?QTS.*?
Media Players	QuickTime	.*?QuickTime.*?
Media Players	Real Media Player	(.*?RealMedia.*?)(.*?RealPlayer.*?)
Media Players	Windows Media Player	.*?NSPlayer.*?

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 three 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 headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit <https://www.trustwave.com>.