Secure Web Gateway

Management Console Reference Guide

Version 11.5

Legal Notice

Copyright © 2013 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: support@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
10.2	March, 2012	Version Release
11.0	December, 2012	Version Release
11.5	November, 2013	Version Update

Formatting Conventions

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

Formatting Conventions

Format and Symbols	Meaning
Blue Underline	A blue underline indicates a 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 check box names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in this format indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, or to introduce a new term.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.
	This symbol indicates information that applies to the task at hand.
	This symbol denotes a suggestion for a better or more productive way to use the product.
	This symbol highlights a warning against using the software in an unintended manner.
	This symbol indicates a question that the reader should consider.

About This Guide

The Management Console Reference Guide provides detailed explanations of the features, screens and fields of the Secure Web Gateway (SWG) Management Console. Where useful, it also provides conceptual information.

The main sections in this Guide are organized according to the main menu options of the Management Console, and topics within each section follow the sub-menu flow.

This document is a screen reference guide, and although some procedures are described, more hands-on procedure descriptions on implementing SWG at a site are provided in the *Secure Web Gateway User Guide*.

SWG Documentation Set

The SWG documentation set includes the following guides:

- *Secure Web Gateway Installation Guide*

- *Secure Web Gateway Setup Guide*

- *Management Console Reference Guide*

- *Secure Web Gateway User Guide*

- *Secure Web Gateway User Security Policies In-Depth Guide*

- *Secure Web Gateway User Identification Guide*

Table of Contents

Table of Contents
vii

1 Introduction to the SWG Management Console

The Secure Web Gateway (SWG) Management Console provides administrators with tools for managing the entire SWG deployment using a Web browser

This section contains the following topics:

- Getting Started in the Management Console

- Features and Use of the Management Console

- Basic Management Console Tasks

- Management Wizard

- Dashboard

1.1 Getting Started in the Management Console

Before performing any preliminary tasks, ensure that:

- SWG is installed. For installation instructions, see the S*ecure Web Gateway Installation Guide*.

- SWG is set up using the Limited Shell. For setup instructions, see the *Secure Web Gateway Setup Guide*.

- The License key for SWG is available.

- The Policy Server IP is added to the Proxy Server Exceptions in the Internet settings to ensure optimum performance (optional).

- The organization's security requirements are defined and prepared for implementation.

To log into the Management Console for the first time:

1. If you are logging into the Management Console for the first time, make sure the License key is available. For more information, see License.

2. In your Web browser, go to **https://<appliance IP address>**.

   If an alert message identifies a security issue with the Website (for example, its security certificate), continue to the Website even if the message warns that this is not recommended.

   The Login window is displayed.

3. Enter the administrator user name (default: **admin**) and password (default: **TrustwaveSWG**).

   The Change Password window is displayed.

   The password must be changed when logging in to SWG for the first time.

4. Enter the following:

   - **Old Password** — The current administrator password

   - **New Password** — A new password

   - **Confirm Password** — Reenter the new password

5. Click **Change Password**.

   The License window is displayed.

6. In the License window, enter the License key and click **Continue**.

   The Trustwave SWG Welcome screen is displayed.

7. Configure the Mail Server via **Administration | System Settings | Mail Server**. For more information, see Mail Server.

Welcome Screen

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

This screen provides quick links to several frequently-used activities. Note that you can also display these links in the Home page, if required. For more information, see Customizing the Home Page.

1.2 Features and Use of the Management Console

This section describes the main GUI features and functionality.

- Management Console Screen

    - General Screen Usage and Navigation

    - Menu Bar

    - Toolbar

    - Tree Pane

- General Screen Usage and Navigation

    - Keyboard Shortcuts

1.2.1 Management Console Screen

The Management Console Screen contains the following areas:

- General Screen Usage and Navigation

- Menu Bar

- Toolbar

- Tree Pane
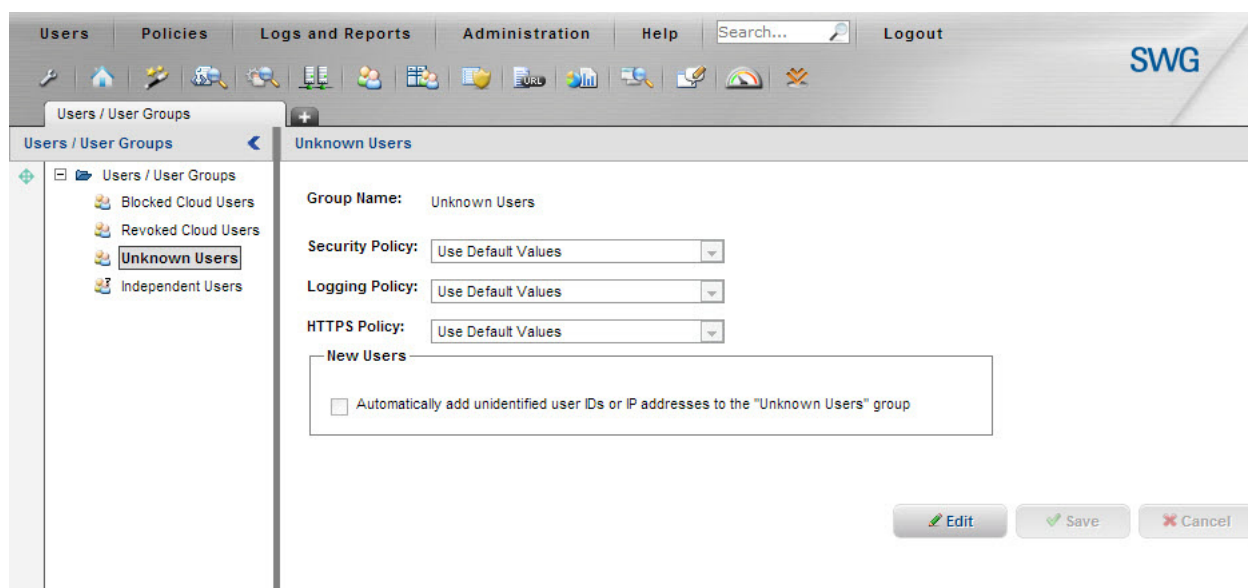
1.2.1.1 Menu Bar

The Menu Bar at the top of the screen provides access to SWG device features. The main sections of the *Management Console Reference Guide* are organized according to these menu options.

| Users | Policies | Logs and Reports | Administration | Help | Search... | Logout |

Clicking a Menu Bar icon, and then clicking lower level sub-menus or options, is the primary screen navigation method.

The Menu Bar contains the following:

- Users — Provides options for the system administrator to define users, import users from external sources, arrange them into groups, and assign them Security and other Policies.

- Policies — Provides configuration options for User and Device Policies.

- Logs and Reports — Provides monitoring and reporting on blocked or suspicious content. A Dashboard presents real-time information on the status of the Secure Web Gateway and SWG Devices.

- Administration — Provides the main bulk of administrative, monitoring and configuration on SWG devices and other scanning abilities. You can also perform system backups and restore from here; set High Availability, set alerts for system administrators and retrieve Security and Maintenance Updates, and Cloud configuration.

- Help — Provides links, manuals and other resources for Secure Web Gateway.

- **Search** — Provides a semantic search of SWG features. The user can search for any object, menu item or rule name in the system using this one search box, accessible on every page of the application. If an item is not found, for example, if it is not a Trustwave object, the user can select **More results** from the list.

- **Logout** — Logs out of the SWG Management Console.

1.2.1.2 Toolbar

The Toolbar below the Menu Bar provides quick access to frequently-used features and functions:

Toolbar Icons

Icon	Shortcut to	Description
	Edit Toolbar Buttons	Enables you to choose which icons are displayed on the toolbar. Click this button and then select or clear the check boxes to display or hide the relevant tools.
		You can also go to the **Toolbar** tab in **Administration | System Settings | Administrative Settings**. For more information, see Customizing the Toolbar.
	Home	Opens the SWG Home page. This page can:
		• Provide quick links to recent and frequently used activities in the Management Console.
		• Display notification of pending system updates and changes, both automatic and those requiring user action.
		• Display a selection of logs and reports.
		You can arrange the Home page to suit your needs. For more information, see Customizing the Home Page.
		Note that this is a limited view, and the data shown is dependent on the permissions of the current user.
	Management Wizard	Enables you to access the **User Groups** and **Log Entry** Wizards.
		User Groups Wizard: Used for group management including assigning users to the group.
		Log Entry Wizard: Enables administrators to display the details regarding a particular transaction ID. It is intended for handling customer queries where, for example, the customer gets an end-user message regarding a blocked transaction. The administrator can enter the transaction ID and display the details regarding the transaction, and then proceed to handle it accordingly.
		For more information, see Management Wizard.
	Web Logs	Directs you to the Web Logs screen for monitoring transactions.
	System Logs	Directs you to the System Logs screen for monitoring transactions.
	SWG Devices	Directs you to the SWG Devices screen for device configurations.

Toolbar Icons

Icon	Shortcut to	Description
	Users	Directs you to the Users/User Groups section. The Users tab is used to administer users and groups and assign policy configurations.
	LDAP	Directs you to the LDAP screen where LDAP groups are imported and assigned specific Security, HTTPS and Logging Policies. User authentication is also performed here.
	Security Policies	Directs you to the Security Policy – Advanced section. View or edit Security Policies.
	URL List	Directs you to the URL Lists option. Include specific URLS or regular expressions (allowed or blocked) to enforce organization security policy.
	Reports	Directs you to the Reports options in the Logs and Reports section. Analyze the activity and performance of the system based on data stored in the Reports database.
	Scanning Options	Directs you to Scanning Options section. Enables the caching of results of scanned files and display of a Status page during the download process.
	Block/Warn Messages	Directs you to the Block/Warn Messages section. Enables the editing of messages that are sent to end users in the event that a URL site has been blocked by SWG or requires user approval or coaching action.
	Dashboard	Opens the Dashboard – the one-stop System Monitoring component of the Management Console that enables you to monitor all Devices in real time. For more information, see Dashboard.
	Commit Changes	Distributes and implements your saved changes in the system devices. For more information, see Committing Changes.
	Expand/ Collapse	Hides and shows the tree pane.
	Refresh	Refreshes the current screen.
	Help	Opens the Help.

Icons in certain definition screens

	Adds rows.
	Displays options that let you add or delete specific rows.

1.2.2 General Screen Usage and Navigation

Most windows are used for defining and configuring. Some windows provide only information, and cannot be updated. Some windows provide lists of information that are editable.

Main Window

The Main Window is where you define or view the details of a feature. Note the following:

- **Window Instance Tab.** This consists of two parts, enabling you to work on multiple window instances.

    - Clicking the tab opens another window instance. By default, the **Home** page is displayed. You can navigate to another location in the new window.

    - The labeled tab identifies the lowest level menu option used for accessing the particular window. When multiple windows are opened, you can move from window to window by clicking the appropriate tab.

- Check the Status bar at the bottom of the Console window to see the path to the currently displayed tab. The Status Bar also provides information on system status, and login and version details.

- Some list screens have an icon that displays the details of the item when clicked. For example, the Update Management screen provides a list of available updates.

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

- After defining or configuring a component and performing a **Save**, you must click **Commit Changes** in the toolbar to synchronize the Policy Server and the scanners.

- Many definition/configuration windows contain tabs, with each tab containing fields relevant to that tab.

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

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

- A grayed-out field or button (for example, the **Edit** button) means that the user is not allowed to perform the relevant update.

Tree Pane

Many screens display a tree structure pane to the left of the main window.
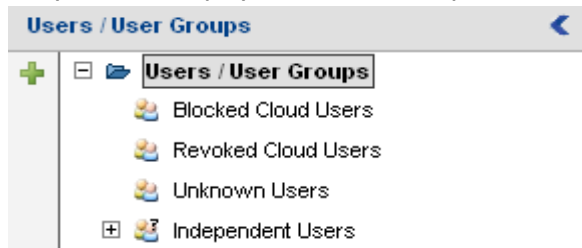
Note the following points about the tree:

- Different levels in the tree generally represent different items, and therefore selecting different levels in a tree will generally change the screen display in the main window.

- Right-clicking a tree item often presents a context menu of action options. These might vary according to the level of the clicked item.

- A grayed-out right-click option or icon means that the user is not allowed to perform the operation.

- Many tree panes have action icons to the left of the tree entries. You can select an entry in the tree, and then click the appropriate action icon. Pop-up tooltips provide a description of each icon.

1.2.2.1 Keyboard Shortcuts

You can use keyboard shortcuts to perform various actions in the Management Console.

Keyboard Shortcuts

Keyboard Shortcut	What it does
F2	Activates (same as clicking) Edit
ESC	Activates (same as clicking) Cancel
Alt+u	Opens the Users menu
Alt+p	Opens the Policies menu
Alt+s	Opens the Logs and Reports menu
Alt+n	Opens the Administration menu
Alt+l	Opens the Help menu
Keyboard arrows	• When used in a menu, navigates inside the menu • When used in a tree, navigates inside the tree

1.3 Basic Management Console Tasks

This section describes the following:

- Logging In and Out of the Management Console

- Changing Your Password

- Committing Changes

- Customizing the Toolbar

- Working in Multiple Windows

- Customizing the Home Page

1.3.1 Logging In and Out of the Management Console

To log into the Management Console:

1. In your Web browser, enter `https://<appliance IP address>`.

2. If an alert message identifies a problem with the Website (for example, its security certificate), continue to the Website (even if the message warns that this is not recommended).

3. In the displayed Login window, enter the user name and password, and click **Login**.

   The Trustwave SWG Welcome screen is displayed. This screen provides quick links to several frequently-used activities. Note that you can also display these links in the Home page, if required.

To log out of the Management Console:

1. Close the browser.

Or

2. Click the **Logout** main menu option, and at the confirmation prompt, click **OK**.

1.3.2 Changing Your Password

All users can use this procedure to change their own passwords.

Administrators can change the passwords of the administrators they manage in the Administrator definition screen (accessed via Administration | Administrators).

1. Select **Administration | Change Password**.

2. Enter your old password.

3. Enter your new password. Then reenter the new password in the **Confirm Password** field.

4. Click **Change Password**.

1.3.3 Committing Changes

To distribute and implement changes that you have saved, you must click the **Commit Changes** button in the toolbar.

You can click the button after each **Save**, or you can wait and then click the button when it is convenient to distribute and implement the changes.

1.3.4 Customizing the Toolbar

1. In the main menu, select **Administration | System Settings | Administrative Settings**.

2. In the main window, select the **Toolbar** tab.

3. Click **Edit**.

4. Ensure that only the icons that you want displayed are selected.

5. Click **Save**.

> Alternatively, you can click the icon in the toolbar, and in the drop down list, select or clear the items that you want to display or hide. Then click **Update**.

1.3.5 Working in Multiple Windows

If you are working in a window and want to access another window, you need not close your current window. You can open multiple tabs, each acting as a self-contained window.

*   To open a tab that contains a window, click the icon. By default, the **Home** page opens. Navigate to the desired location in the new window.

*   To move between windows, click the tab of the target window.

*   To close a window, click to the right of the tab name.

1.3.6 Customizing the Home Page

The Home page provides quick access to frequently-used SWG features and reports. Click **Home** in the toolbar to open the page.

The page comprises three panes that you can customize according to your needs:

Click the icon in one or more panes and select an option from the drop down menu. These selections will be available the next time you open the Home page.

You can also click the link at the top right of a pane to open the selected view as a full page.

1.4 Management Wizard

Management Wizards simplify the use of the Management Console by providing the Administrator with quick access to the most frequently-used features. The use of one-click wizards eases the management of customer transactions and the configuration of user groups and security policies.

Buttons on the bottom right of the Wizard screens can be used to navigate through the wizard or to create new entities. You can click to drill down to obtain further details concerning a selected entity.

To access the Management Wizards screen, click in the toolbar. Then click either **User Groups Wizard** or **Log Entry Wizard**.

1.4.1 User Groups Wizard

To display the User Groups Wizard, click to display the Management Wizard; then click .

The Management Wizard **User Groups** list screen is displayed. This screen displays the list of existing User Groups (predefined and user-defined). From this window, you can:

- Add a new user group: Click at the bottom-right of the window. For more information, see Wizard – User Group Details Screen.

- Display the details of an existing user group: Click the group's icon, and choose **Group Details**. (**Note**: This option is not available for **Independent Users**, since it is technically not a group and does not have group details defined for it.) For more information, see Wizard – User Group Details Screen.

- Display the list of users in a user group: Click the group's icon, and choose **Group Users**. (**Note**: This option is not available for **Blocked Cloud Users** and **Revoked Cloud Users**, since these groups cannot contain users.) For more information, see Wizard – Users List Screen.

- Delete a user-defined User Group: Click the group's icon, and choose **Delete Group**. (**Note**: You cannot delete a predefined User Group.)

1.4.1.1 Wizard – User Group Details Screen

The Management Wizard **User Group Details** screen is used for viewing and editing which Security, Logging, and HTTPS policies are assigned to the group. Depending on the group, the screen might also be used for viewing and editing additional group details.

You can display this screen either by clicking , or by clicking and choosing **Group Details** from the Management Wizard **User Groups** screen.

Note the following:

- If you are creating a new user group, you must specify a group name and fill in the definition.

- If you are editing an existing group, you must click **Edit**.

- After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

Fields in the User Groups Detail Screen

Fields in the User Group Detail Screen

Field	Description
Group Name	Unique name you assign to the group. Mandatory for a new group.
Security Policy / Logging Policy / HTTPS Policy	Particular Security, Logging, and HTTPS policies to be assigned to users belonging to the group.
The following field appears only in the **Unknown Users** group.	
New Users area	This area contains the following check box: **Automatically add unidentified user IDs or IP addresses to the "Unknown Users" group** Selecting this check box ensures that the User ID or IP of any subsequent Unknown Users who browse through SWG will be added to the group. This simplifies the process of later defining those users in the system.
The following fields appear only in user-defined User Groups.	
Issue Mobile Security Client Certificates to new group members	Select this check box if the Policy Server should automatically issue certificates to all NEW users added to this group. **Note:** This check box is: • disabled until, and only relevant if, you implement the Cloud in **Internal** mode (under **Administration | Cloud | Configuration**). For more information, see Cloud Configuration. • generally intended for use with cloud-dedicated User Groups, and is most effective if selected before you populate the group for the first time. If you check this option, existing users already in the group will not be issued certificates. To issue certificates to those users, in the **Users	Users/User Groups** screen, right-click the group node and choose **Issue Mobile Security Client Certificates to non-provisioned users**.
Prevent user from disabling Mobile Security Client	Relevant only if you implemented the Cloud in **Internal** mode; otherwise it is ignored. Select this check box if group members should not be allowed to disable the Mobile Security Client agent on their machines.
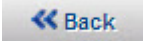
Field	Description
Enable automatic Mobile Security Client upgrade	Select this check box if you want Mobile Security Client upgrades to be implemented automatically.
IP Ranges	Identifies IP ranges (**From IP/To IP**) that are included in the group. Clicking the ➕ icon enables you to add IP ranges. **Note the following:** • An explicitly defined user under the group whose IP does not fall in the defined IP range is treated as a member of the group, as regards policy enforcement and certificate issuance. • An undefined user who falls in the IP Range is treated as a member of the group as regards policy enforcement, but not as regards certificate issuance (such a user cannot be a cloud user). • A user who is explicitly defined as a member of one group, but whose IP falls in the range defined for a different group, is treated as a member of the group in which the user is explicitly defined, as regards policy enforcement and certificate issuance.

Navigation

From this screen you can navigate as follows:

- To return to the previous display, click **≪ Back**.

- To display the list of users in the group, click **Users ≫**. For more information, see Wizard – Users List Screen.

- To display the details of a specific policy, click the ≡≫ icon next to the policy, and choose **Policy Details**. The Management Wizard Policy Details window for the policy is displayed. For more information, see Wizard – Policy Details Screen.

- To create a new policy of a specific type, click the ≡≫ icon next to the policy type, and choose **Add New Policy**. An empty Management Wizard Policy Details window is displayed. For more information, see Wizard – Policy Details Screen.

- To display the list of rules in a specific policy, click the ≡≫ icon next to the policy, and choose **Policy Rules**. The Management Wizard Policy Rules window for the policy is displayed. For more information, see Wizard – Rules List Screen.

1.4.1.2 Wizard – Users List Screen

The Management Wizard **Users** list screen (**Management Wizard | User Groups | Users**) displays the list of users in a selected User Group.

You can display this screen either by clicking ▤≫ and choosing **Group Users** in the **User Groups** screen, or by clicking [Users ≫] in the **User Group Details** screen. (**Note**: These options are not available for the **Blocked Cloud Users** and **Revoked Cloud Users** groups, since these groups cannot contain users.)

Actions and Navigation

From this window, you can do any of the following:

- To return to the previous display, click [◀◀ Back] .

- To add a new user, click [New +] . For more information, see Wizard – User Details Screen.

- To display the details of an existing user, click the user's ▤≫ icon, and choose **User Details**. For more information, see Wizard – User Details Screen.

- To delete a user from the group, click the user's ▤≫ icon, and choose **Delete User**. At the confirmation prompt, confirm the deletion.

1.4.1.3 Wizard – User Details Screen

The Management Wizard **User** details screen is used for viewing and editing a number of user details, including email address, which Security, Logging, and HTTPS policies are assigned to the user, and user IP and name identifiers.

You can display this screen either by clicking [New +] , or by clicking ▤≫ and choosing **User Details** from the Management Wizard **Users** list screen.

Note the following:

- If you are defining a new user, you must specify a user name and fill in the definition.

- If you are editing an existing user's details, you must click **Edit**.

- When done editing, click **Save**. To commit the changes, click ⌄ **Commit Changes** in the toolbar.

Fields in the User Details Screen

Fields in the User Details Screen

Field	Description
User Name	Unique name assigned to the user. Mandatory.
Email	User's email address (relevant for cloud user notifications).
Security / Logging / HTTPS policy	For I**ndependent Users**: The particular Security, Logging, and HTTPS policies that should be assigned to the user. For all other users, these are protected fields, and the displayed/ assigned values are those assigned to the parent group.
Identifiers	Value(s) that can be used to identify the user. To specify an identifier, click the ➕ icon, select the type (**IP** or **User Name**), and then specify the value for that identifier. Repeat as necessary. Clicking the 📋 icon next to an Identifier displays options for deleting the identifier or adding a new identifier to the bottom of the list.

Navigation

From this screen you can navigate as follows:

- To return to the previous display, click ⟨⟨ **Back** .

- To display the details of a specific policy, click the ▤≫ icon next to the policy, and choose **Policy Details**. The Management Wizard Policy Details window for the policy is displayed. For more information, see Wizard – Policy Details Screen.

- To create a new policy of a specific type, click the ▤≫ icon next to the policy type, and choose **Add New Policy**. An empty Management Wizard Policy Details window is displayed. For more information, see Wizard – Policy Details Screen.

- To display the list of rules in a specific policy, click the ▤≫ icon next to the policy, and choose **Policy Rules**. The Management Wizard Policy Rules window for the policy is displayed. For more information, see Wizard – Rules List Screen.

1.4.1.4 Wizard – Policy Details Screen

The **Policy Details** screen displays the policy name and description of a policy, and provides a list of Users and User Groups that are assigned this policy.

You can display this screen for an existing policy assigned to a User Group or User, or when creating a new policy to be assigned to a User Group or User.

This screen is displayed when you click ▤≫ next to the specific policy (or policy type) in either the **User Group Details** screen or the **User Details** screen, and then choose either **Policy Details** or **Add New Policy**.

Note the following:

- If you are defining a new policy, you must specify a policy name.

- If you are editing an existing policy's details, you must click **Edit**.

- When done editing, click **Save**. To commit the changes, click ⌄ **Commit Changes** in the toolbar.

> You cannot create or edit predefined **Security**, **HTTPS** or **Logging** policies; you can only create and edit user-defined policies.

Fields in the Policy Details Screen

This option is only displayed for security policies.

<div align="center">Fields in the Policy Details Screen</div>

Field	Description
Policy Name	Name of the specific policy
X-Ray	Defines whether the Policy is X-Ray. (X-Ray means the policy is logged but no action is taken)
User Groups/ Users using this policy	Security Policies can be assigned to different User Groups and Users. This section displays which Users have this particular Policy assigned to them. For more information on assigning Policies to Users, see Users/User Groups.

Navigation

From this screen you can navigate as follows:
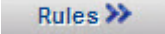
- To return to the previous display, click ≪ Back .

- To display the list of rules in the policy, click Rules ≫ . For more information, see Wizard – Rules List Screen.

For more information, see Policies.

1.4.1.5 Wizard – Rules List Screen
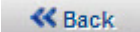
The Management Wizard **Rules** list screen displays the list of rules in a selected Policy.

You can display this screen by doing either of the following:

- clicking ▤≫ and choosing **Policy Rules** by a policy in the **User Group Details** screen or in the **Users Details** Screen.

- clicking [Rules ≫] in the **Policy Details** screen.

Actions and Navigation

From this window, you can do any of the following:

- To return to the previous display, click [« Back] .

- To add a new rule, click [New ✚] . For more information, see Wizard – Rule Details Screen.

- To display the details of an existing rule, click the rule's ▤≫ icon, and choose **Rule Details**. For more information, see Wizard – Rule Details Screen.

- To display the list of conditions defined to the rule, click the rule's ▤≫ icon, and choose **Rule Conditions**. For more information, see Wizard – Conditions List Screen.

- To delete a rule, click the rule's ▤≫ icon, and choose **Delete Rule**. At the confirmation prompt, confirm the deletion.

- To change the position of the rule in the rule list (rules are checked for triggering in sequence, so the position is significant; for more information, see Rule Logic, Priority, and Enforcement), do the following:

  a. Click the rule's ▤≫ icon, and choose **Move Rule to**.

  b. Click the ▤≫ icon of the rule that appears either after or before the target location of the moved rule, and choose either **Before this Rule** or **After this Rule**, accordingly.

1.4.1.6 Wizard – Rule Details Screen

The Rule Details screen provides the definitions for specific rules.

You can display this screen either by clicking [New ✚] , or by clicking ▤≫ and choosing **Rule Details** from the Management Wizard **Rules** list screen.

> ⓘ You cannot create or edit rules in predefined **Security**, **HTTPS** or **Logging** policies; you can only create and edit rules in user-defined policies.

Note the following:
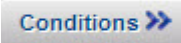
- If you are defining a new rule, you must specify a rule name and fill in the definition.

- If you are editing an existing rule's details, you must click **Edit**.

- When done editing, click **Save**. To commit the changes, click ⊻ **Commit Changes** in the toolbar.

Fields in the Rule Details Screen

Security, **HTTPS**, and **Logging** policy rule definitions have rule name and description fields, a select check box, and three tabs for defining the rule details: **General**, **Applies**, and **Except**. For information on the fields in these tabs, see Security Rule Details, HTTPS Rule Details, and Logging Rule Details, respectively.

Navigation

From this screen you can navigate as follows:

- To return to the previous display, click 〈〈 Back .

- To display the list of conditions in the rule, click Conditions 〉〉 . For more information, see Wizard – Conditions List Screen.

1.4.1.7 Wizard – Conditions List Screen
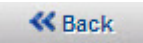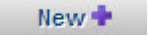
The Management Wizard **Conditions** list screen displays the list of conditions in a selected rule.

You can display this screen by doing either of the following:

- clicking ≣〉〉 and choosing **Rule Conditions** in the **Rules** List screen.

- clicking Conditions 〉〉 in the **Rule Details** screen.

Actions and Navigation

From this window, you can do any of the following:

- To return to the previous display, click 〈〈 Back .

- To add a new condition, click New ✚ . For more information, see Wizard – Condition Details Screen.

- To display the details of an existing condition, click the condition's ≣〉〉 icon, and choose **Condition Details**. For more information, see Wizard – Condition Details Screen.

- To delete a condition, click the condition's ≣〉〉 icon, and choose **Delete Condition**. At the confirmation prompt, confirm the deletion.

1.4.1.8 Wizard – Condition Details Screen

The Condition Details screen provides the details for a specific condition. For information on creating new Conditions for use in policies, see Condition Elements.

You can display this screen either by clicking New, or by clicking ⬛≫ and choosing **Condition Details** in the Management Wizard **Conditions List** screen.

> You cannot create or edit conditions in predefined **Security**, **HTTPS** or **Logging** policies; you can only create and edit conditions in user-defined policies.

Fields in the Condition Details Screen

The actual items listed in condition details varies with the condition.

Fields in the Condition Details Screen

Field	Description
Condition Name	Displays the Condition name. If you are defining a new condition, choose the required condition from the drop down list.
Applies To	You can select which options are to be included or excluded. In other words, you can either choose to apply this rule to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select/Deselect All	Choose to select/deselect all the items in the Condition.

For information specific to a particular condition, see Condition Elements.

Actions and Navigation

- When adding a new condition, you must select the condition name. This will impact the fields and values displayed in the screen.

- To edit an existing condition details, you must click **Edit**.

- After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

- From this screen you can navigate as follows: To return to the previous display, click Back.

1.4.2 Log Entry Wizard

The Log Entry Wizard simplifies the handling of customer queries concerning blocked transactions.

End-user messages always provide a transaction ID. When reporting or querying a blocked transaction, the user notifies the administrator when the transaction occurred and provides the transaction ID. The administrator then uses the transaction ID to track down the transaction in the Log Entry Wizard.

The wizard provides all related Web log and user group information, and quick access to policy information. Administrators can then easily perform different tasks in connection with these logs.

To display the Log Entry Wizard, click ![icon] to display the Management Wizard; then click ![icon] .

To find a log entry in the Log Entry wizard, enter a Transaction ID and click **Next**.

The wizard **Transaction Details** screen is displayed.

The tree in this screen has two nodes:

- **Details node** — selecting this node displays the same tabs and fields as the Web Logs Transaction Entry Details Window:

    - Transaction Tab

    - User Tab

    - Policy Enforcement Tab

    - Content Tab

    - Scanning Server Tab

    However, the wizard provides additional navigation options.

- Request and Response Details node

1.4.2.1 Transaction Tab

The **Transaction** tab of the Log Entry wizard contains the same fields as the Details Pane: Transaction Tab in the Web Logs Transaction Entry Details window, and like that tab, it lets you copy the URL to your clipboard, and update a URL list with the URL site listed in the tab.

1.4.2.2 User Tab

The **User** tab of the Log Entry wizard contains the same fields as the Details Pane: User Tab in the Web Logs Transaction Entry Details window.

However, the Wizard contains an **Unknown Users** button (that is not displayed in the Web Logs Transaction Entry Details window).

- To display the details window for the **Unknown Users** group, click the **Unknown Users** button.

The wizard definition screen for the Unknown Users group is displayed. For a description of the usage and fields in this screen, see Wizard – User Group Details Screen.

Once the wizard **Unknown Users Group** details window is displayed, you can:

- Click ⬛⟫ next to a policy, and choose options to display the policy details, to display the list of rules in the policy, or to create a new policy, in the appropriate wizard screens. Once you are in those wizard screens, you can continue to navigate to other wizard screens. For more information, see Wizard – Policy Details Screen and Wizard – Rules List Screen.

- Click the **Users** button to display the list of users in the Unknown Users group, in the appropriate wizard screen. Once you are in that wizard screen, you can continue to navigate to other wizard screens. For more information, see Wizard – Users List Screen.

1.4.2.3 Policy Enforcement Tab

The **Policy Enforcement** tab of the Log Entry wizard contains the same fields as the Details Pane: Policy Enforcement Tab in the Web Logs Transaction Entry Details window.

However, in the wizard (unlike the Web Logs Transaction Entry Details window) the Security Policy Name and Security Rule Name values appear as buttons.

To display the wizard Security Policy Details screen, or the wizard Security Rule Details screen, click the appropriate button.

Note the following:

- Once you have navigated to the Security Policy details, you can navigate to the wizard Rule list, and continue navigation from there.

- Once you have navigated to the Security Policy Rule Details, you can navigate to the wizard Conditions List, and continue navigation from there.

For more information, see Wizard – Policy Details Screen and Wizard – Rules List Screen.

1.4.2.4 Content Tab

The **Content** tab of the Log Entry wizard contains the same fields as the Details Pane: Content Tab in the Web Logs Transaction Entry Details window.

However, in the wizard (unlike the Web Logs Transaction Entry Details window), a number of the values for the fields in this tab are links. To display a window with relevant information, click the link. For information regarding the listed conditions types, see Condition Details for Security Policy Rules. For information regarding the listed scanning engines, see Scanning Engines.

1.4.2.5 Scanning Server Tab

The **Scanning Server** tab of the Log Entry wizard contains the same fields as the Details Pane: Scanning Server Tab in the Web Logs Transaction Entry Details window, and like that tab, it lets you display the details of the relevant Scanning server.

1.4.2.6 Request and Response Details

The **Request and Response Details** screen of the Log Entry wizard contains the same fields as the Transaction Entry: Request and Response Phases display in the Web Logs Transaction Entry Details window.

For each transaction, the content is scanned on both the request and/or the response phase depending on the nature of the content and the nature of the rule that it triggered.

The information displayed in these panes depends on the nature of the transaction and is useful in determining why the transaction was blocked.

1.5 Dashboard

The SWG Dashboard presents crucial information, in real-time, on the status of the Secure Web Gateway and the SWG Devices within it. Its purpose is to keep System Administrators fully informed at all times.

The **Updates Available** icon in the top left corner is enabled when there are Security or other updates for your system. You can install updates via Administration | Updates and Upgrades | Management. For details, see Updates and Upgrades.

To access the Dashboard, click in the toolbar. To close the Dashboard, click .

The screen has two main areas for displaying graphs and charts:

- Devices Area

- Messages Area

Note the following:

- Rolling over the top level of a graph offers basic information at a glance.

- Tooltips are available on top of the graph for specific point information.

Setting time periods for the display

Each area of the Dashboard contains mechanisms to set the time period for which the data will be calculated and displayed:

- **Period Selection** — Select a range of time from which to draw information. A drop down list lets you select options for: **12 hour time period**, **daily**, **weekly**, **monthly**, or **yearly**.

Once a graph is displayed, the following additional controls are enabled to provide a more detailed analysis:

- **Graphic Slide-pointer** — Slide the pointer to the desired time frame.

- **Interactive zoom** — Mark the time frame range on the graph by placing the cursor over the area and then left-clicking the mouse.

1.5.1 Devices Area

The Devices area of the Console contains the following areas:

- Gauges Area

- Performance Area

- Device Utilization Area

1.5.1.1 Gauges Area

The Gauges area displays the following gauges.

- **Threat Level Gauge** — Shows the risk factor to which your organization is exposed. This risk calculation is based on the number of blocked transactions compared to the general traffic.

  This gauge has a **Threat Level** link. Clicking this link opens the Total Threat Level Display, which graphs the risk factors involved.

- **RPS Gauge** — Shows the total requests per second (RPS). For this purpose, a request is defined as any new request sent through the Secure Web Gateway server; therefore, each object on a Web page generates a request.

  For example, for a Web page containing 10 objects (images, applets, etc.), the graph will indicate 11 requests: 1 for the request that the browser issued for the Web page, and 10 individual requests for the 10 objects.

1.5.1.1.1 Total Threat Level Display

To display the Total Threat Level in graphic format, click the **Threat Level** link in the **Threat Level** gauge.

The graph indicates the number of transactions (y-axis) of different categories passing through the organization over a period of time (x-axis). The following transaction categories are graphed:

- Anti-Virus

- Behavior Analysis

- URL Lists

- URL Categorization

- Blocked DLP

- Blocked in Total

Below the graph is a chart that provides the following three risk level values for each of those transaction categories:

- **Current** — Number of blocked transactions for that particular category at this moment in time.

- **Average** — Average number of blocked transactions, per category, at a particular time relative to the time period chosen. For example, per day, maximum of 24 hours.

- **Maximum** — Largest number of blocked transactions at a particular time relative to the time period chosen. For example, per day, maximum of 24 hours.

To close the display, click .

1.5.1.2 Performance Area

The Performance area to the right of the Gauges area displays a graph and chart of performance status for the Devices you select over the Time period you select.

Use the drop down list to select the relevant device. Set the Time period as desired.

Performance status is measured by requests per second. The following types of values are provided:

- **Current** — Number of blocked transactions for that particular category at this moment in time.

- **Average** — Average request per second during a specific time slot relative to the time period chosen.

- **Maximum** — Maximum requests per second at a specific time slot relative to the time period chosen.

1.5.1.3 Device Utilization Area

For each Device (Policy Server, Scanning Server, All in One), the following information is provided:

Device Utilization Fields

Field	Description
Group Name	The Device Group name.
Device Type	Defines the type of Device such as Scanning Server or All in One.
IP	IP Address of the Device.
Status	Device status is either active or pending. Pending appears while the device is still in the Commit stage.
Date/Time	Date and Time that the last Status update was received.
RPS	Requests per Second, as shown on the Performance graph.
Device Utilization	Clicking the **More Information** button next to a device displays various Device Utilization Graphs and Charts that show utilization information for the device. The button can be green or red, depending on the message alert status per particular device: • **Red** — Major or critical alerts have been issued for the device and have not been acknowledged by the user. Messages are acknowledged in the Messages Chart. Once acknowledged, the button changes to green. • **Green** — No major or critical alerts have been issued for the device, or a major alert has been acknowledged changing the button from red to green.

1.5.1.3.1 Device Utilization Graphs and Charts

The Device Utilization Graphs display is accessed by clicking **More Information** . The button can be green or red, depending on whether alerts have been issued for the device.

For each device, a number of graphs display relevant information to the system administrator, allowing real-time viewing on any overload for any particular device.

Each graph shows both the **Average** and Current (for a selected time period, such as 24 hours) and a **Maximum** at any one given time period.

Data can be accessed as far back as 12 months, or as recent as within the last 12 hours, by moving the slider across the Period selection option (bottom right of the graph).

HTTP and HTTPS connections are constantly monitored. Information in this graph enables the administrator to see the overall load on the system.

Trustwave's scanning server protocol limits are: 16384 open connections for HTTP/ICAP, and 4096 connections for HTTPS. Too many open connections can indicate a growing environment that may require additional scanning servers.

The following graphs are available (links provide additional information):

Device Utilization Graphs and Charts

Graph Name	Description
CPU Utilization	Measures the percentage of CPU being used over time (System, Nice, Kernel, User, Idle, Wait).
Memory Usage	Measures the memory in bytes being used (Used Real, Buffers, Cached, Unused Real, Used Swap).
HTTP(s) Connection Count	Number of http/https requests that go through the proxy.
Cache Memory Usage	The amount of memory that the caching server is using.
Cache Hit Ratio	Number of cache hits reported by the caching server.
Partition Disk / Cache	The amount of disk space the caching server is using for cached data.
Network Throughput	Network utilization on the appliance, divided into **Received** and **Transmitted**, measured in bytes.

If the Device is not working or is experiencing any other error then the appropriate error message is displayed in the Messages area of the Device Utilization screen.

Messages include the following information, and can be filtered by whether they are read or unread:

Device Utilization Messages

Message Field	Description
ACK	Acknowledge check box. Select to denote that you have read this message.
Note	Click the icon to add a personal note about the particular message.
Severity	Warning, Minor, Major, or Critical as defined by SNMP messages.
Date/Time	Date and Time the message was generated.
Source	Device IP address.
Message	Message text.

CPU Utilization

Includes the following information:

- **System** — Percentage of CPU time spent processing system-level code.

- **Nice** — Number of 'ticks' (typically 1/100s) spent processing reduced-priority code.

  On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

- **Kernel** — Number of 'ticks' (typically 1/100s) spent processing kernel-level code.

  On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

- **User** — Percentage of CPU time spent processing user-level code.

- **Idle** — Percentage of processor time spent idle.

- **Wait** — Number of 'ticks' (typically 1/100s) spent waiting for I/O.

  On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

> For more information, see http://net-snmp.sourceforge.net/docs/mibs/ucdavis.html.

Memory Usage

Includes the following information:

- **Used Real** — Amount of memory that has been reserved for processes.

- **Buffers** — Total amount of real or virtual memory currently allocated for use as memory buffers.

- **Cached** — Total amount of real or virtual memory currently allocated for use as cached memory.

- **Unused Real** — Total amount of real/physical memory currently unused or available.

- **Used Swap** — Amount of swap memory used.

1.5.2 Messages Area

This area displays SNMP messages that appear for errors or critical circumstances.

The Message area includes a drop down menu that offers three different viewing selections:

- **Show All** — Shows all messages, whether read or unread

- **Noticed** — Shows only messages that have been read

- **Unnoticed** — Shows only messages that have not yet been read

The Message window also includes Notation capabilities as well as the following informational fields:

Fields in the Message Window

Message Field	Description
ACK	Acknowledge check box. Enable this check box to denote that you have read this message.
Note	Click the icon and add a note for yourself about the message.
Severity	Critical, Major, Minor, Warning, Normal or Unknown, as defined by SNMP messages.
Time	Date and Time the message was generated.
Source	Device IP address.
Message Text	Message text. The last 30 updated messages are displayed.

You can delete individual message lines by clicking the **Delete** button on the left of the row. To delete all messages, click the **Delete** button in the header row.

2 Users

This section contains the following topics:

- Users/User Groups

- User Lists

- User Grouping and Certificate Management

- Authentication Directories

You manage users via the **Users** main menu option. The **Users** menu enables you to:

- Define users in the system, assign them policies, and manage those users.

  The process used for performing this task depends on the category to which the users belong:

  - Regular (Non-LDAP) users — As described in Users/User Groups.

  - LDAP users — As described in LDAP.

- Create User Lists which can be used when defining Security, HTTPS, and Logging Policy rules, to identify to which users the rules should or should not apply — As described in User Lists.

- Identify and manage cloud users — As described in User Grouping and Certificate Management.

- Manage Directory sites — As described in Authentication Directories.

> This task is relevant only if you are implementing Authentication-type Identification Policy (for more information, see Identification Policy.)

2.1 Users/User Groups

The menu option **Users | Users/User Groups** enables you to create and define User Groups and users as needed.

You do not have to create Groups — you can create users without Groups, but groups help simplify the process of user definition.

For example, when you create a User Group, you assign it policies (**Security**, **Logging**, and **HTTPS**), that automatically apply to all users who are members of that group. This means that you do not have to make individual policy assignment for each user in the group.

The **Users/ User Groups** option displays two panes:

- **Tree Pane** — Lists existing User Groups and users. The tree's root node is **Users/User Groups**.

- **Main Window** — Displays the details of the currently selected User Group or user.

The tree includes the following pre-defined groups:

- **Independent Users** — This is where you create users who do not belong to a User Group. You can assign each independent user whatever Security, Logging, and HTTPS policy is most relevant for that user. For more information, see Independent Users.

- **Unknown Users** — Used for assigning appropriate Security, Logging and HTTPS policies to unidentified users who are browsing through SWG. For more information, see Unknown Users Group.

- **Blocked Cloud Users/ Revoked Cloud Users** — Two Cloud User Group nodes for assigning policies to users whose certificates are blocked or revoked. For more information, see Blocked/ Revoked Cloud Users Groups.

To create a user-defined User group, right-click the **Users/User Groups** (root) node in the tree, and choose **Add Group**. For more information, see User-defined User Groups.

> Before creating User Groups and assigning them policies, you can alter which policies are set as site-wide defaults. For more information, see User/Device Policy Relevance and Default Policy Assignments.

This section contains the following topics:

- User Groups

- Users

2.1.1 User Groups

This section contains the following topics:

- Options On User Group Nodes

- User-defined User Groups

- Blocked/Revoked Cloud Users Groups

- Unknown Users Group

- Independent Users

- Moving Users Screen

2.1.1.1 Options On User Group Nodes

Not all options are available from all group nodes.

Options on the User Group Nodes Tree

Right-Click Option	Does the following
Add User	Adds a user to the User Group.
Issue Mobile Security Client cert to non-provisioned users	Issues a certificate to all non-provisioned users (those users to whom a certificate has not yet been issued) in the group. (Operational only when cloud configuration is defined in **Internal** mode. For more information, see Cloud Configuration.)
Send emails to provisioned users	Sends instructions (usually Mobile Security Client installation instructions) in emails to all provisioned cloud users in the group. Operational only when cloud configuration is defined in **Internal** mode. For more information, see Cloud Configuration.)
Download Group Users Certificate	Downloads the certificates that have been issued to users in the groups. (Operational only when cloud configuration is defined in **Internal** mode. For more information, see Cloud Configuration.)
Delete Group	Deletes the group and all of its users.
Move Users	Displays a window that lets you move users in the group to another group. For more information, see Moving Users Screen.

2.1.1.2 User-defined User Groups

You can create a User Group by selecting the **Users | Users/User Groups** menu option, right-clicking the **Users/User Groups** node and choosing **Add Group**.

The main window displays the fields of the User Group definition.

To edit the details of an existing User Group, select the group's node, and then click **Edit** in the main window.

Note that some fields in the User Group definition are relevant only if you have configured a cloud server in Internal Mode (for more information see Cloud Configuration).

If you configure a cloud server in Internal mode, it is recommended that cloud users be placed in a group (or groups) in which all members are cloud users.

After creating/editing a User Group, click **Save**.

User-defined User Group Screen Fields

Field	Description
Group Name	Unique name you assign to the group. Mandatory.
Security Policy / Logging Policy / HTTPS Policy	Particular policies (Security/Logging/HTTPS) to be assigned to users belonging to the group.
Issue Mobile Security Client Certificates to new group members	Select this check box if the Policy Server should automatically issue certificates to all NEW users added to this group. **Note:** This check box is: • disabled until, and only relevant if, you implemented the cloud in **Internal** mode (under **Administration | Cloud | Configuration**). For more information, see Cloud Configuration. • generally intended for use with cloud-dedicated User Groups, and is most effective if selected before you populate the group for the first time. If you select this option, existing users already in the group will not be issued certificates. To issue certificates to those users, right-click the group node and select **Issue Mobile Security Client cert to non-provisioned users**.
Prevent user from disabling Mobile Security Client	(Relevant only if you implemented the cloud in **Internal** mode; otherwise it is ignored). Select this check box if group members should not be allowed to disable the Mobile Security Client agent on their machines.
IP Ranges	Identifies IP ranges (**From IP**/**To IP**) that are included in the group. Clicking the ✚ icon enables you to add IP ranges. Note the following: • An explicitly defined user in the group whose IP does not fall in the defined IP range is treated as a member of the group, as regards policy enforcement and certificate issuance. • An undefined user who falls in the IP Range is treated as a member of the group as regards policy enforcement, but not as regards certificate issuance (such a user cannot be a cloud user). • A user who is explicitly defined as a member of one group, but whose IP falls in the range defined for a different group, is treated as a member of the group in which the user is explicitly defined, as regards policy enforcement and certificate issuance.

2.1.1.3 Blocked/Revoked Cloud Users Groups

The predefined **Blocked Cloud Users** group and **Revoked Cloud Users** group do not contain users.

However, their definitions enable you to identify which policies should be assigned to cloud users whose certificates are blocked or revoked.

For more information on the blocking or revoking of cloud user certificates, see User Grouping and Certificate Management.

- To display the definitions for these groups, select the **Users | Users/User Groups** menu option, and then click the group in the tree pane.

- To edit the fields in the screen, click **Edit** to edit the fields.

  - The Group Name field is disabled.

  - You can edit which Security, Logging, and HTTPS policies to apply.

  - Although editable, the IP Ranges fields in these groups are irrelevant and will be ignored.

- To save the changes, click **Save**.

2.1.1.4 Unknown Users Group

The **Unknown Users** group is used to assign appropriate Security, Logging and HTTPS policies to unidentified users who are browsing through SWG.

You can also ensure that the user IDs or IP addresses of such users will be added to the group. This makes it easier to later move these users to other User Groups if desired. For information on moving users to a different User Group, see Moving Users Screen.

To display the definitions for the **Unknown Users** group, select the **Users | Users/User Groups** menu option, and then select the **Unknown Users** group node in the tree pane.

To edit the fields in the screen, click **Edit** to edit the fields. To save the changes, click **Save**.

In the Unknown Users Group window, the **Group Name** is a protected field.

<div align="center">Unknown Users Group Screen Editable Fields</div>

Field	Description
Security Policy / Logging Policy / HTTPS Policy	Particular policies (Security/Logging/HTTPS) to be assigned to unknown users.

New Users — Automatically add unidentified user IDs or IP addresses to the "Unknown Users" group

Selecting this check box ensures that the User ID or IP of any subsequent Unknown Users who browse through SWG will be added to the group. This simplifies the process of later defining those users in the system.

2.1.1.5 Independent Users

You can create/define users who will not belong to a group by adding them under the **Independent Users** node.

Because the users under the **Independent Users** node do not belong to a group:

- these users are not automatically assigned a group's policies. Instead, you assign policies to each individual user under the node.

- the **Independent Users** node does not require the details found in other groups.
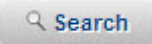
Therefore, when you choose the **Users | Users/User Groups** menu option and select the **Independent Users** node in the tree, no details screen is displayed in the main pane.

2.1.1.6 Moving Users Screen

To move users from a source group to a different target group, right-click the source User Group node in the tree, and choose **Move Users**. (This is especially useful for moving users from the Unknown Users group to a different group.)

The main window then displays fields for moving the users currently located in the source group. The name of the source group appears at the top of the window, and as a protected name in the **Group Name** field.

Move User Display Screen Fields and Buttons

Field	Description
Find All	Used for specifying search criteria. Useful if the group contains a large number of users. After specifying search criteria in this field, click **Search**. To clear the search results, click **Clear**.
Move Users	List of users, each with a check box, in the Source Group. You should select the users that you want to move. (Selecting the check box on the gray, top line that says **Name**, will select/clear all users.)
Move To	Target group into which you want to move the users. Choose the group from the drop down list.
Previous/Next buttons	Pages through a source group with many users.
	Clicking these buttons performs the search on the value in the **Find All** field, or clears the search results, respectively.

2.1.2 Users

To add a user to a User Group, right-click the group node in the tree and select **Add User**. Note, however, the following exceptions:

- You cannot add users to the **Blocked Cloud** or **Revoked Cloud Users** groups.

- You cannot manually add users to the **Unknown Users** group. Instead, you should select the **New Users — Automatically add unidentified user IDs or IP addresses to the "Unknown Users" group** check box in the Unknown Users definition screen, and new, unknown users will automatically be added.

To edit the definition of an existing user, select the user in the tree. In this case, you must click **Edit**.

After creating or editing a user, click **Save**.

To delete a user, right-click the user in the tree and choose **Delete User**.

To move users from one group to another, see Moving Users Screen.

This table describes the fields in the User Details screen.

User Details Screen Fields

Field	Description
User Name	Unique name assigned to the user. Mandatory.
Email	User's email address (relevant for cloud user notifications).
Security / Logging / HTTPS policy	For I**ndependent Users**: The particular policies (Security/ Logging/HTTPS) that should be assigned to the user. For all other users, these are protected fields, and the displayed/ assigned values are those assigned to the parent group.
Identifiers	Value(s) that can be used to identify the user. To specify an identifier, click the icon, select the type (**IP** or **User Name**), and then specify the value for that identifier. Repeat as necessary. Clicking the icon next to an Identifier displays options for deleting the identifier or adding a new identifier to the bottom of the list.

2.2 User Lists

The User Lists feature enables you to define lists of LDAP/Trustwave Users and Groups. These lists can then be used when you define Security, HTTPS, and Logging Policy rules, to identify those users to which the rules should or should not apply.

You define User Lists in the User Lists screen, accessed via the **Users | User Lists** menu option.

The User Lists screen contains two panes — a tree pane that lists existing User Lists, and the main window where you define the User List. The top node in the tree pane is the **User List**s node.

Working in the User List Screen

To add a new User List, right-click the **User Lists** node in the tree and select **Add List**.

To edit an existing list, select the list in the tree, and in the main window, click **Edit**.

After defining a list, click **Save**. To commit the list, click **Commit Changes** in the toolbar; the list will then be included in the list of User Lists that appear in the **Apply To** tab and **Exception** tab of Security, HTTPS and Logging policy rules.

To delete a list, right-click the list and choose **Delete List**.

To see which policy rules a list is used in (that is, has been selected in), right-click the User List and choose **Used In**. For more information, see Used-In Window.

2.2.1 Fields in the User List Screen

In the **Name** field, specify an identifying name for the User List (mandatory).

The main User List window contains the following tabs:

- Selected Members Tab

- LDAP Groups Tab

- LDAP Users Tab

- Trustwave User Groups Tab

- Trustwave Users Tab

2.2.1.1 Selected Members Tab

The Selected Members tab is a summary tab that lists the details of the User List that you defined in the other tabs. No definition takes place in this tab.

2.2.1.2 LDAP Groups Tab

The **LDAP Groups** tab lets you select LDAP Groups to be included in the User List. All LDAP Users in a selected group will automatically be included in the list.

User List Screen – LDAP Groups Tab Fields and Buttons

Field/Button	Description
Find All field **Search button** **Clear button**	To filter the display on a particular value, specify the value in the **Find Al**l field, and click **Search**. To clear the filter and re-display the full list, click **Clear**.
Select check box	Before checking which items in the table below to include in the list, and if helpful, select/clear this check box to select/clear all the check boxes in the table.
table of items	Select items in this table for inclusion in the list.
check box	Select the check box of each item to be included in the list.
Domain	Domain of the LDAP Group.
Name	Name of the LDAP Group.
Next/Previous buttons	Use these buttons to navigate through the list if the list spans multiple pages.

2.2.2 LDAP Users Tab

The **LDAP Users** tab lets you select LDAP Users to be included in the User List.

Selected items are cumulative. For example, an LDAP user who was not selected in the LDAP User tab, but who belongs to an LDAP Group that was selected in the LDAP Group tab, **will** be included in the list.

User List Screen – LDAP Users Tab Fields and Buttons

Field/Button	Description
Find All field **Search button** **Clear button**	To filter the display on a particular value, specify the value in the Find All field, and click **Search**. To clear the filter and re-display the full list, click **Clear**.
Select check box	Before checking which items in the table below to include in the list, and if helpful, check/clear this check box to select/clear all the check boxes in the table.
table of items	Select items in this table for inclusion in the list.
check box	Select the check box of each item to be included in the list.
Domain	Domain of the LDAP Group.
Name	Name of the LDAP Users.
Next/Previous buttons	Use these buttons to navigate through the list if the list spans multiple pages.

2.2.2.1 Trustwave User Groups Tab

The **Trustwave User Groups** tab lets you select Trustwave User Groups to be included in the User List. All Trustwave Users in a selected group will automatically be included in the list.

User List Screen – Trustwave Users Group Tab Fields and Buttons

Field/Button	Description
Find All field **Search button** **Clear button**	To filter the display on a particular value, specify the value in the Find All field, and click **Search**. To clear the filter and re-display the full list, click **Clear**.
Select check box	Before checking which items in the table below to include in the list, and if helpful, select/clear this check box to select/clear all the check boxes in the table.
table of items	Select items in this table for inclusion in the list.
check box	Select the check box of each item to be included in the list.
Users Group	Name of the Trustwave User Group.
Next/Previous buttons	Use these buttons to navigate through the list if the list spans multiple pages.

2.2.2.2 Trustwave Users Tab

The **Trustwave Users** tab lets you select Trustwave Users to be included in the User List.

> Selected items are cumulative. For example, a Trustwave user who was not selected in the Trustwave Users tab, but who belongs to a Trustwave User Group that was selected in the Trustwave User Group tab, **will** be included in the list.

User List Screen – Trustwave Users Tab Field and Buttons

Field/Button	Description
Find All field **Search button** **Clear button**	To filter the display on a particular value, specify the value in the Find All field, and click **Search**. To clear the filter and re-display the full list, click **Clear**.
Select check box	Before checking which items in the table below to include in the list, and if helpful, select/clear this check box to select/clear all the check boxes in the table.
table of items	Select items in this table for inclusion in the list.
check box	Select the check box of each item to be included in the list.
User	Name of the Trustwave user.
Next/Previous buttons	Use these buttons to navigate through the list if the list spans multiple pages.

2.2.3 Used-In Window

The Used-In window displays the list of Security, HTTPS, and Logging policy rules in which a User List is used (that is, selected in the **Apply To** tab or **Exception** tab).

To display the Used-In window for a User List, right-click the list in the tree and choose **Used In**.

From the User In window, you can navigate the policy or rule definition page of a rule that uses the list, by clicking the for the detail line and choosing the appropriate option.

After viewing the rules in which a list is used, perform any other action to close the Used In display (for example, select the User List node to re-display the User List details).

The fields in the Used-In window are not editable. The following table describes the fields in the window.

User In Screen Fields

Field/Button	Description
Name	Name of the User List. This name appears in the title bar of the window.
Select check box	Before checking which items in the table below to include in the list, and if helpful, select/clear this check box to select/clear all the check boxes in the table.
Used In table	List of Policies/Rules in which the list is used. The table includes the following elements:
	To navigate to the definition of the policy or rule listed in the detail line, click this icon and choose **Navigate to Policy Page** or **Navigate to Rule Page**.
Policy Name	Policy that contains the rule that uses the User List.
Rule Name	Rule that uses the User List.

2.3 User Grouping and Certificate Management

> This screen is relevant only when the cloud is configured to work in **Internal mode**. (In **PKI mode**, cloud users are certified and managed externally.)
>
> Many options and features described in this section are non-operational if the cloud is not configured in **Internal** mode. For information on cloud configuration, see Cloud Configuration.

You display the User Grouping and Certificate Management screen by selecting the **Users | User Grouping and Certificate Management** menu option. The screen contains fields for filtering the display.

This screen is primarily used to issue certificates for individual cloud users, and to manage the certificates of these cloud users — for example, if there are problems with specific users or certificates, the administrator must take appropriate action (such as blocking or revoking a certificate).

You can also perform a number of other cloud certificate management functions from this screen.

> If you want all users in a User Group or LDAP group to be issued certificates, you need not issue them individually via this screen. Instead you can issue them at the group level as follows:
>
> - To have certificates issued to all NEW users added to the group, click **Users | Users/User Groups**, then in the left pane select the group, and then in the right pane select **Issue Mobile Security Client Certificates to new group members**.
>
> - To issue certificates to existing users who were in the group before you selected that check box, right-click the group node in the tree and select **Issue Security Client Certificates cert to non-provisioned users**.
>
> You can also perform the following certificate related tasks at the group level, by right-clicking the group node and choosing the appropriate action:
>
> - Send emails with instructions (usually Mobile Security Client installation instructions) for all users in the group.
>
> - Export all certificates belonging to users in the group.
>
> For more information, see User-defined User Groups and/or LDAP Groups.
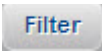
The following table describes the fields in the User Grouping and Certificate Management display.

The top row of the display (the row with the drop down selection lists for Domain, Name and Status columns) is the filtering row. To filter the display, select desired values and click the **Filter** button. To clear the filter, click the ✖ button.

Selecting the **Select** check box enables certificate actions, such as Issue, Revoke, and so on to be applied concurrently to multiple users based on selection criteria, including group names.

User Grouping and Certificate Management Display Fields and Buttons

Field	Description
Domain	Domain filtering field. Note that this field contains the following selection values: • a domain value for each cloud LDAP group. • the value **Local Users**, which includes all users belonging to cloud User Groups. • the value **All**, which includes all users belonging to cloud User Groups and LDAP groups.
Name	User name.
User Group	Filters the users by group; All, independent users, or unassigned LDAP users.
Email	User's email address.
Cert Expiration	Certificate expiration date.
Status	Filters on (and displays) certificate status. Filters on: • **All** — Does not filter on Certificate Status (filtering value only). Shows users in cloud LDAP groups and cloud User Groups. • **Blocked** — User's certificate has been blocked (as described in User Grouping and Certificate Management). • **Expired** — User's certificate has expired. • **Non-Issued** — User has not been issued a certificate. • **Pending** — User will get a certificate after you click ⬇ (Commit). • **Revoked** — User's certificate has been revoked (as described in User Grouping and Certificate Management). • **Valid** — User's certification is valid (that is, none of the above statuses).
Filter	Filters the display according to the values selected in the drop down lists.
✖	Clears the filter to re-display the full list.
▶≡	Displays a context menu that enables you to choose the action to be performed on the particular user.

User Grouping and Certificate Management Display Fields and Buttons

Field	Description
Export All Certificates	Exports the certificates for all cloud users into a zipped directory structure organized by folders representing the user groups (defined in the **Users | Users**/**User Groups** screen). **Note:** This requires that the CA Authority be defined (in **Administration | Cloud | Configuration**). For more information, see Cloud Configuration.
Previous/Next buttons	Pages through lists of users.

To perform the management actions you can perform on users in the Cloud User lists, click ⬛ for the particular user, and choose the appropriate option.

Manage User Options Available in the User Grouping and Certificate Management Screen

Option	Description
Issue new certificate	Issues a new certificate — generally to replace a revoked certificate.
Block certificate	Blocks, but does not revoke, a certificate. Choose this option to temporarily block a certificate that is suspected of being compromised. Once you determine if it has or has not been compromised, you can then Allow or Revoke it accordingly.
Revoke certificate	Permanently revokes a certificate. Once revoked, a certificate can never be used again, and a new certificate will have to be issued.
Allow certificate	Unblocks a blocked certificate. Choose this option if you determine that a blocked certificate has not been compromised.
Export certificate	Exports a user's certificate to an external file.
Send provisioning email	Re-sends previously issued certificate information. This option is useful if the initial certificate was lost.

2.4 Authentication Directories

The **Users** menu option contains two options:

- LDAP

- Realm

2.4.1 LDAP

One way to create large numbers of users is to import them from LDAP directories on LDAP Servers.

You can work with LDAP directories by selecting the **Users | LDAP** menu option. When you select this menu option, the window displays a tree pane on the left, and a main details pane on the right.

The top node of the tree pane is called **Directories**.

Underneath the **Directories** node is a node called **Settings and Defaults**, described below.

Directly underneath the **Settings and Defaults** node (but at the same level) are nodes for each type of LDAP server supported by Trustwave. Trustwave provides support for the following LDAP servers:

- **Sun ONE**

- **IBM Tivoli**

- **Microsoft AD** (Active Directory)

Generally, you will use one type of LDAP server, though nothing prevents you from using more.

Underneath the appropriate LDAP server, you add and configure directories that point to the LDAP server directories from which you want to import LDAP users. LDAP users can be imported only from LDAP directories pointed to by the directories that you have added and configured.

To create an LDAP directory, right-click the appropriate LDAP Server node (for example, **Sun ONE**) in the tree, and choose **Add Directory**.

The tree also contains a **Custom** node, where you can define directories for LDAP servers for which SWG has no pre-definitions, but which you can customize yourself.

After you have configured LDAP directories, it is highly recommended that you import and configure LDAP groups. When configuring LDAP groups, you can assign them policies that will be applied to LDAP users that are members of the group. (You can also configure several other parameters.)

Adding LDAP groups to a directory is not, in itself, sufficient; For the changes to be applied, you must perform an **Import LDAP Users** operation after adding the LDAP groups.

> You **must** (re-)perform LDAP user import following any changes that you make to the LDAP tree structure (for example, adding/removing groups, changing their order), or the changes will not be applied.

You can import LDAP users in the following ways:

- You can define a schedule for automatically updating LDAP directories with LDAP users, in the **Settings and Defaults** node screen display.

- You can manually import LDAP users at any time, at any of several levels:

  - **Directory (root node) level** — Imports all users from all LDAP server directories that you defined.

  - **Specific directory level** — Imports all users from the specific directory.

Imported LDAP users whose groups you did not import are treated as Unassigned LDAP users. You can select a Security, Logging, and HTTPS policy to be assigned to all Unassigned LDAP users; this is also done in the **Settings and Defaults** screen display.

This section contains the following topics:

- Settings and Defaults Screen

- LDAP Directory Screen

- Add LDAP Group Screen

- LDAP Groups

2.4.1.1 Settings and Defaults Screen

You display the Settings and Defaults screen by selecting the **Users | LDAP** menu option, and then clicking on the predefined **Settings and Default** node in the tree.

This screen contains two tabs — one for defining a schedule for periodically reading updates/changes from LDAP directories, and one for assigning policies to unassigned LDAP Users.

Click **Edit** to edit the values in the screen. Click **Save** to save the changes.

This section contains the following topics:

- Fields in the Scheduled Settings Tab

- Fields in the Unassigned LDAP Users Tab

2.4.1.1.1 Fields in the Scheduled Settings Tab

The **Scheduled Settings** tab in the Settings and Defaults screen is used to define a schedule for periodically reading updates/changes from LDAP directories.

Settings and Defaults Screen – Scheduled Settings Tab Fields

LDAP Import Schedule check box	Select this check box if a schedule for the automatic import of LDAP users should be implemented.
Run daily at: <time>	Select this radio button and set the time for the daily import.
Run every: <interval>	Select this radio button and set the hourly schedule for the import.

2.4.1.1.2 Fields in the Unassigned LDAP Users Tab

The **Unassigned LDAP Users** tab in the Settings and Defaults screen is used to assign policies to unassigned LDAP users (LDAP users whose groups have not been defined within the system).

Settings and Defaults Screen – Unassigned LDAP Users Tab Fields

Field	Explanation
Security Policy	Select the Security policy to be assigned to Unassigned LDAP users.
Logging Policy	Select the Logging policy to be assigned to Unassigned LDAP users.
HTTPS Policy	Select the HTTPS policy to be assigned to Unassigned LDAP users.

2.4.1.2 LDAP Directory Screen

To create a "local" LDAP directory (that is, a "local directory" that corresponds to and points to a directory on the LDAP server), first display the LDAP tree (select the **Users | LDAP** menu option). Then right-click the appropriate LDAP Server node (for example, **Sun ONE**), and choose **Add Directory**.

This displays the LDAP Directory screen in the main pane, where you can define the directory details.

To edit the details of an existing directory, select the directory node in the tree. Then in the main window, click **Edit**.

The LDAP Directory screen contains two tabs, one for defining the general details of the directory, and the other for defining Search parameters.

In addition to these two tabs, the screen displays the following fields, not included in the tabs:

- **Name** — Unique name assigned to the LDAP directory (two LDAP directories cannot have the same name). Mandatory.

- **Do not check configuration settings on next save** — Leave this check box cleared if you want the configuration settings to be checked when you do a save.

After defining the details, click **Save** to save the definition.

After creating and defining the LDAP directory, you can then import LDAP groups from this directory.

This section contains the following topics:

- Fields in the General Tab

- Fields in the Advanced Settings Tab

- LDAP Nodes Options

2.4.1.2.1 Fields in the General Tab

The **General** tab in the LDAP directory screen is used for defining the general details of the LDAP directory.

Note that when setting security for the LDAP directory in this tab, if there is a demand for increased security, you can choose to use Secure Socket Layer (SSL) protocol while connecting to the LDAP server. (SSL increases security through the use of cryptography, digital signatures, and certificates.).

LDAP Directory Screen – General Tab Fields

Field Name	Description
Address	Each directory is identified with an IP address or hostname, for example, 10.194.20.15.
	If the LDAP server does not listen to the default LDAP port, you can specify the port by adding:port_number after the IP address or hostname. For example: 10.194.20.15:636.
	Multiple addresses can be specified (click the ➕ icon).
Base DN	This is the DNS domain component name (e.g., dc=Trustwave, dc=com).
Realm / Domain	Directory's identifier in the authentication process between the browser and the scanning server (e.g., Trustwave). **Note:** If the directory type is **Microsoft Active Directory**, do not specify a **Realm/Domain**; instead, the value will be automatically detected.
User	Authorized User DN for connecting to the directory. **Note:** If the directory type is **Microsoft Active Directory**, enter the user's account name (i.e., the name that appears on emails before the @company.com), instead of its DN.
Password	Password for entering into your organization's directory. **Note:** LDAP passwords cannot include the < , > or space characters. Do not use non-English characters if you will be using the Kerberos authentication method.
Use Secure Connection	Use Secure Socket Layer (SSL) protocol to encrypt data transmission while connected to the LDAP server. Disabled by default.

LDAP Directory Screen – General Tab Fields

Field Name	Description
Ignore Certificate Validation	This option is available only when **Use Secure Connection** is enabled. Note that an appropriate certificate should be imported (for more information, see User Grouping and Certificate Management). Note the following: • If the Policy Server should NOT validate the certificate before starting the SSL session, select this check box. • If the Policy Server should validate the certificate on each connection, leave this check box cleared. (If the certificate is invalid, user import fails and an event, such as a log, trap or email, is created.)

2.4.1.2.2 Fields in the Advanced Settings Tab

A number of Advanced Settings apply to LDAP Directories. These have default values, that you can adjust in the **Advanced Settings** tab of the LDAP directory screen.

LDAP Directory Screen – Advanced Settings Tab Fields

Field Name	Description
User Identifier Attribute	This parameter defines the attribute which indicates a user's unique identifier. The value for this attribute is compared to the username provided by the proxy authentication. Default values are as follows: • Microsoft AD – sAMAccountName • IBM Tivoli – eraliases • Sun ONE – uid If left blank, users/groups will be identified by their DNs.
Email Attribute	Attribute that is used to indicate a user's email.
User Object Filter	Defines in LDAP syntax the filter that will be used to identify user objects. Default values are as follows: Microsoft AD - (&(objectclass=person)(objectclass=user)(!objectclass=computer)) IBM Tivoli - (&(objectclass=person)(objectclass=organizationalPerson)) Sun ONE - (&(objectclass=person)(objectclass=organizationalPerson))
Group Identifier Attribute	Defines the attribute which indicates a group's unique identifier. (The Management Console will use the value of this attribute when displaying group names and assigning policies.) Default values are as follows: • Microsoft AD – sAMAccountName • IBM Tivoli – ou • Sun ONE – cn If left blank, users/groups will be identified by their DNs.
Group Object Filter	Defines in LDAP syntax the filter that will be used to identify group objects. Default values are as follows: • Microsoft AD – (objectclass=group) • IBM Tivoli - (&(objectclass=organizationalunit)(objectclass=erOrgUnitItem)) • Sun ONE - (objectclass=groupofuniquenames)
Connection Timeout	Set the maximum number of seconds for an unanswered LDAP query, after which users will not be imported. If set to 0, the system default (120) will be used.

LDAP Directory Screen – Advanced Settings Tab Fields

Field Name	Description
Group User Hierarchy Method	Requires specification of at least one of the following attribute types.
memberOf Attribute	Attribute of a user entity that holds the list of groups in which the user is a member. Default values are as follows: • Microsoft AD – memberOf • IBM Tivoli – erparent • Sun ONE – not supported **Note:** If this radio button is selected: • a value for this method must be specified (it should not be left blank). • if a value is specified for the other method, that value is ignored.
member attribute	Attribute of a group entity that holds the list of members of a selected group. Default value is: • For Sun ONE – uniqueMember **Note:** If this radio button is selected: • a value for this method must be specified (it should not be left blank). • if a value is specified for the other method, that value is ignored.
Set Default	Returns all the parameters above to their default values.

2.4.1.2.3 LDAP Nodes Options

The following table describes the options that are available in the tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option.

LDAP Group Node Options

Option	Explanation
Check connection	When selected, SWG tries to connect and log in to the LDAP directory. In doing so, it checks the address specified in the LDAP directory **Address** field, and the credentials and security definitions, if relevant (i.e., certificate or keytab).
Set Importable	If multiple LDAP directories have the same Base DN, users can only be imported from one of them; the other directories are disabled (i.e., grayed out). Normally, users are imported from the directory in that set that was created first.
	To import the users from one of the disabled directories, before performing the import of LDAP groups and/or LDAP users, right-click the directory from which you want to perform the import, and select this option.
Import LDAP users	Imports the LDAP users. Those users whose groups have been added to the tree will be imported as members of those groups. The remaining users will be treated as Unassigned LDAP Users. For more information, see Fields in the Unassigned LDAP Users Tab.
Add Groups	Enables the import of LDAP groups. For more information, see Add LDAP Group Screen.
Remove Directory	Deletes the added directory.

2.4.1.3 Add LDAP Group Screen

It is recommended that you import LDAP groups before importing LDAP users.

To import LDAP groups for a directory:

- Right-click the LDAP directory in the tree and choose **Add Groups**. The main screen display changes to enable you to add LDAP Groups.
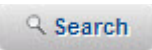
When the display is populated with details, it displays a checklist of available LDAP groups. You can choose which groups to import into the directory.

> The first time you choose **Add Groups** for an LDAP Server, the display is not populated with details. To populate the display, click the **Retrieve LDAP Groups** button.

When you import LDAP groups, they are automatically assigned site-default Security, Logging and HTTPS policies. You can change the policy assignments for the LDAP groups.

Adding LDAP Groups Screen Fields and Buttons

Field/Button	
Find All	Filtering field. You can use this field to specify a search string for matching LDAP Group names. **Note:** The search is case sensitive.
Search	Performs the search.
Clear	Clears the search results and restores the full list.
Retrieve LDAP Groups	Retrieves the list of groups from the LDAP server. **Notes:** • The first time you display this screen for an LDAP server, the display is empty until you click this button. • Groups that have been added to the tree will not be displayed in the retrieval results (to prevent
Select Users area	Area used for displaying the list of LDAP Groups
Select check box	Check box toggle which causes all or no check boxes on the page to be selected. **Note**: When you select a check box, a **Select all pages** option appears, letting you select all check boxes on all pages.
Users/Groups list	List of retrieved LDAP groups available for adding to the LDAP directory (i.e., retrieved LDAP groups that have not been added to a directory). To add LDAP groups to the directory, select the desired check boxes and then click **OK**.

2.4.1.4 LDAP Groups

Once you have added LDAP Groups, the nodes for the groups appear in the tree under the LDAP directory into which they have been added.

You can then assign policies and define other relevant parameters in the details screen that you can display for each group.

To display the details screen for an LDAP group, display the tree if it is not already displayed (by selecting the **Users | LDAP** menu option), and then select the particular LDAP Group node.

Note that if an LDAP user is included in more than one group, the policy that will be implemented will be the one that is assigned to the first group appearing in the list (group priority is listed from top to bottom).

Therefore, the relative positioning of groups in the LDAP Directory can be significant.

If necessary, you can change the position of LDAP groups in the tree, relative to each other by performing a **Move Group To** operation (as described in Options on LDAP Group Nodes).

This section contains the following topics:

• Fields in the LDAP Group Details Screen

• Options on LDAP Group Nodes

2.4.1.4.1 Fields in the LDAP Group Details Screen

Before you edit the details of an LDAP Group, you must click **Edit**. To save the changes, click **Save**.

LDAP Group Screen Fields

Field	Description
Security Policy / Logging Policy / HTTPS Policy	Particular policies (Security/Logging/HTTPS) to be assigned to users belonging to the LDAP group.
Issue Mobile Security Client Certificates to new group members	Select this check box if certificates should be issued to all new users added to this group (via an Import LDAP Users operation). This will make them cloud users.
	Note: This check box is:
	• disabled until, and only relevant if, you implemented the cloud in **Internal** mode (under **Administration | Cloud | Configuration**). For more information, see Cloud Configuration.
	• generally intended for use with cloud-dedicated LDAP Groups.
	• most effective if selected before you populate the group for the first time. (Users already imported into the group at the time that you select this check box will not automatically get certificates.)
Prevent user from disabling Mobile Security Client	(Relevant only for cloud users.) Select this check box if cloud members should not be allowed to disable the Mobile Security Client agent on their machines.

2.4.1.4.2 Options on LDAP Group Nodes

The following table describes the options that are available in the tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option.

LDAP Group Node Options

Right-Click Option	Does the following
Delete Group	Removes the group from the LDAP tree. (It will then be ignored during the Import LDAP User operation.)
The following fields are applicable only for when cloud configuration is defined in Internal mode. For more information, see Cloud Configuration.	
Issue Mobile Security Client cert to non-provisioned users	Issues a certificate to all non-provisioned users in the group.
Send emails to provisioned users	Sends instructions (usually Mobile Security Client installation instructions) in emails to all provisioned cloud users in the group.
Download Group Users Certificates	Downloads the certificates that have been issued to users in the groups.
Move Group To	Select this option to move the group to a different location in the tree. Then right-click the group immediately below or above the desired new location, and select one of the following options as appropriate (**Note**: the completed change will only take effect after you again perform another Import LDAP User operation):
Before This Group	Select this option (after choosing **Move Group To** for a group) to move that group to immediately before this group.
After This Group	Select this option (after choosing **Move Group To** for a group) to move that group to immediately after this group.

2.4.2 Realm

SWG performs authentication against Domain Controllers. SWG supports multiple Domain Controllers. These must be part of the realm or have a trust between them.

> You only need to provide site information to SWG if you are defining an Authentication type policy as your Identification Policy (for more information, see Identification Policy).
>
> In this case, you **must** provide SWG with the information about the site(s) **before** defining the Identification Policy.

The menu option **Users | Realm** displays the Realm window, which enables you to provide SWG with required information about sites that are used for Authentication and authorization.

This window displays a tree pane that lists the defined sites, and a main pane for displaying details about the current site.

- To add a new Site definition, display the Realm window, right-click the **Realm** (root) node, and choose **Add Site**. Then define the details in the General Tab and Kerberos Tab.

- To edit the details of an already-defined site, select the site node in the tree. Then click **Edit** in the General tab and Kerberos tab.

After creating/editing the details for a Site, click **Save**.

To delete a Site, right-click the site node in the tree and choose **Delete Site**.

2.4.2.1 General Tab

Realm Screen Fields

Field Name	Description
Site Name	User-assigned name for the site that will be used in the authentication process between the browser and the Scanning Server/Authentication Device.
Active	If the site should be activated, ensure that this check box is selected.
Domain Name	Realm domain name. Must be the actual identifier of the resource. For example, NTY.
Domain Controller Selection Method	Method to be used for domain Controller selection. Valid values: • **Primary-Backup**: (Default). Selects the Primary Domain Controller, and if that Domain Controller is unavailable, there will be an automatic shift to the Backup Domain Controller. • **Load Balancing**: Domain Controller will be selected by round-robin looping through the Domain Controllers until an appropriate, available Domain Controller is found.
Domain Controller	To add a detail, click the ➕ icon.
Name	Name of the Domain Controller. This is the hostname entered either as an IP address or DC name. (It should be written without periods.) The Domain Controller has a user list and password used for authentication.
Force NTLM v2	Select this check box if the Domain Controller will use NTLM-v2. (if cleared, it will use NTLM v1. Default.) **Note:** When NTLM v2 is selected in the Domain Controller field, all subsequent entries must follow suit.
Trusted Domains	Domains that have an established trust for authentication by the primary domain controller (specified in **Site Name** field). To add a detail, click the ➕ icon.

2.4.2.2 Kerberos Tab

SWG supports the Kerberos authentication mechanism, a network protocol that provides more secure and more effective user authentication for client/server applications than legacy protocols such as NTLM. Kerberos uses *tickets* to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos is primarily a client–server model that provides mutual authentication—both the user and the server verify each other's identity.

For more information, refer to the *SWG User Guide*.

To enable Kerberos authentication:

1. Right-click a realm Site node and select **Add Keytab**.

2. Enter the Keytab name and click **Upload SPN from keytab file**.

3. Browse to the file location, select the file and click **Import**.

   The SPN details are listed in the Kerberos tab.

   - **Keytab:** Key table. A file containing pairs of Kerberos principals and encrypted keys.

   - **SPN:** Service Principal Name. The name by which a client uniquely identifies an instance of a service running on a server.

   - **KVNO:** Key Version Number. When a user changes a password or an administrator updates the secret key for an

   - application server, this change is logged by advancing a counter. The current value of the counter identifying the key version is known as the Key Version Number. We can get the counter from the generated Keytab file.

4. Click **Save**.

3 Policies

Policies comprise the main rules of Internet behavior for the end-users in your organization, define secure behavior, and address the constraints imposed on Internet traffic.

This section contains the following topics:

- General Information
- User Policies
- Device Policies
- Condition Elements
- End User Messages

3.1 General Information

You access policies via the **Policies** main menu option.

This section contains the following topics:

- Policy Concepts
- Options in the Policies Tree

3.1.1 Policy Concepts

Policies consist of three hierarchic components: the Policy itself, Rules, and Conditions:

- A *Policy* consists of its rules. A rule definition contains an Action that specifies how to handle the information (for example, block or allow content).

- *Rules* have associated *conditions*, which determine whether a particular rule is activated. The most commonly used actions in rules are:

  - **Allow** — Allows the content to pass

  - **Block** — Blocks the content

SWG utilizes several different types of policies, each for different purposes. For each policy type, SWG provides a number of pre-defined policies. The following table briefly describes the available Policy types, and provides links to their descriptions. It also describes several related components.

These all appear in sub-menus of the **Policies** menu.

Policy Types (By Policies Sub-Menu)

Sub-Menu	Policy Type	Description
User Policies	Security Policy	A set of rules that determines how to handle Web content passing through the system. It focuses on pro-actively blocking active content and malicious code while allowing non-dangerous content through.
	Caching Policy	Contains rules that deal with access to HTTPS sites.
	Logging Policy	Defines which transactions will be logged, and the location to which the logged transactions will be sent.
Device Policies	Caching Policy	Defines the rules by which content is stored in the appliance for future use. By default, all HTTP traffic is cached.
	Device Logging Policy	Defines which device-related transactions will be logged, and the location to which the logged transactions will be sent.
	Identification Policy	Defines the methods to be used to identify or authenticate the user browsing through the system.
	Upstream Proxy Policy	Defines the upstream proxy settings that will be used for traffic scanned by the SWG system.
	ICAP Request and Response Modification Policies	ICAP is a lightweight Internet Content Adaption protocol for executing "remote procedure calls" on HTTP messages. ICAP Request Modification and ICAP Response Modification policies define which ICAP Services SWG requests, and how to handle ICAP Service error situations, when SWG acts as an ICAP client.
The following are not policy types but are available options from the Policies menu.		
	Default Policy Settings (from **Policies | User Policies**)	Adjustable default Security, HTTPS, and Logging policy assignments that will be automatically assigned to User Groups and LDAP Groups except where you specify different values on a group by group basis.
	Condition Elements	Configurable values that you can use to tweak the Policies to match your organization's needs.
	End User Messages	Lets you customize the Block Page and Warn Page messages sent to end-users as chosen in the Security and HTTPS Rules.

<div align="center">Policy Types (By Policies Sub-Menu)</div>

Sub-Menu	Policy Type	Description
	Block/Warn Messages	Lets you edit messages sent out to end-users from Security and HTTPS Rules.
	Message Template	Lets you redesign the message template used for displaying block and warn messages.

Policy Window

When you select a policy type in the **Policies** menu, the Policy window generally displays two panes:

- **Tree Pane** — The left pane displays a tree containing policies of the selected type. Under each policy are the rules that define the policy, and under the rules are the conditions that determine if the policy will be triggered.

  Right-clicking a node in the tree pane enables you to perform a number of actions. Available options depend on the level of the node that you right-clicked. For a description of these options, see Options in the Policies Tree.

  The status of rules and conditions in the tree is indicated by icons alongside their names. For a description of these, see Policy Tree Icons.

- **Definition (main) pane** — Displays the definition fields for the selected policy, rule, or condition.

Policy Tree Icons

Icons in the Policy tree include the following:

Icon	Description
	This icon attached to another icon means the policy, rule, or condition is locked. No changes are allowed.
	An Allow rule. A grayed icon means the rule is disabled.
	A Block rule. A grayed icon means the rule is disabled.
	A rule. A grayed icon means the rule is disabled.

Rule Editing and Rule Creation

In general, you cannot edit the predefined policies (or their components) that come with SWG (You can edit Identification Policy). You can either use the predefined policies as provided, or you can duplicate them and edit the duplicates.

You can also create new policies from scratch. To create a new Policy, you create the required rules on which the policy is built, and the required conditions that will determine if the rule is triggered.

69

Examples of rules in a Security Policy are **Block Access to Spyware Sites** or **Allow White-listed Executables**. A rule specifies a combination of conditions with a corresponding action (**User Response Action** for Security/HTTPS rules and **Logging Action** for Logging rules).

Rule Logic, Priority, and Enforcement

A rule in a policy can only be enforced if its conditions are satisfied.

A rule that is higher up in the tree has higher priority, and its conditions will be checked for possible rule enforcement before a rule that is lower down in the tree. Once a rule has been enforced, the other rules in the policy are no longer relevant and will not be evaluated.

Therefore, the order in which a policy's rules appear in the tree can be significant. Consider the following:

- Allow rules create a trust level — Content that comes after an Allow rule has been enforced is not scanned by any blocking rules that come after it. This can be a security problem. If a policy has both Allow and Block rules, it might be good policy to place the Allow rules after the block rules.

- The enforced rule determines the message appearing in Logs and Reports (and optionally sent to an end-user). Therefore, good practice suggests putting the more serious problems first.

  Example:

  Of two rules that might block a particular access, one deals with a specific virus, and the other deals with a suspicious file type.

  Clearly, the virus problem is the far more serious problem. Therefore, good practice would be to place the Anti-Virus rule higher up in the tree than the Suspicious File Type rule.

  Note that if any transaction is not matched specifically in the rules, it is allowed. In other words the Secure Web Gateway default behavior is ***Allow***.

User/Device Policy Relevance and Default Policy Assignments

Some types of policies are relevant only to Users. Other types of policies are relevant only to Devices. For more information, see User Policies and Device Policies.

- The following types of policies are relevant to Users: Security Policy, HTTPS Policy**,** and Logging Policy.

  You can assign specific policies of these types as site-wide defaults, which will then automatically be assigned to all User Groups that you create (these, in turn, will be assigned to all users in the group); but you can modify the assignments on a group by group basis.

- The following types of policies are relevant to devices (Scanning Servers) only: Identification Policy, Device Logging Policy, Upstream Proxy Policy, and Caching Policy.

  You can set specific policies of these types as site-wide defaults, which will then automatically be assigned to all Scanning Servers that you add; but you can modify the assignments on a device by device basis.

Exceptions to User Policy Rules

When defining the rules of polices that are relevant to users (rules in **Security, HTTPS**, and **Logging** policies), in addition to defining the basic definition of those rules, you can identify to which users those rules apply and to which users those rules do not apply.

One method of identifying these users is through the creation of User Lists (via **Users | User Lists**), which you can then select for application to the rules. For more information, see User Lists.

3.1.2 Relocating an Item in the Policies Tree

Within the Policies tree, you can re-order rules to a different location in the policy.

> **Warning:** The order in which rules appear in the tree can be significant. A rule that is higher up in the tree has higher priority, and its conditions will be checked for possible rule enforcement before a rule that is lower down in the tree.
>
> Once a rule has been enforced, the other rules in the policy are no longer relevant and will not be evaluated.

1. Right-click the item and choose **Move Rule to**.
2. Right-click the item above or below the location where you want to place the item being moved. Choose either **Before this Rule** or **After this Rule**, depending on your selection.

3.1.3 Options in the Policies Tree

The following table describes the options that are available in the **Policies** tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option. Many of these options can be performed only on user-defined policies, rules and conditions, and not on predefined policies, rules and conditions provided with SWG.

Policies Tree Options

Node Level	Action	Description
Root Level (Policies)		
	➕ **Add Policy**	Available from the Root folder. Enables you to create a new Policy.
Policy Level		
	➕ **Add Rule**	Available from the Policy folder. Enables you to create a new Rule.
	✖ **Delete Policy**	Available from a specific Policy. Enables you to remove a Policy. Note that deleting a Policy will delete all the Rules and Conditions belonging to it.
	✔ **Set as Default**	Available from a Policy that is not the default policy. Enables you to change the default policy in the system.
	📄 **Duplicate Policy**	Available from a specific Policy. Enables you to clone a predefined Policy and customize it for your needs.
	Export to HTML	Available from a specific Policy. Enables you to export to HTML format – which you can then save or print as required.
	Export to XML	Available from a specific Policy. Enables you to export to XML format – which you can then save or print as required.
Rule Level		
	➕ **Add Condition**	Available from a Rule. Enables you to create a new Condition.
	Insert New Rule	Available from any rule. Enables you to insert a new rule into your Policy **above** the rule you are currently standing on.
	✖ **Delete Rule**	Available from a specific Rule. Enables you to remove a Rule from the Policy.
	✚ **Move Rule To** **Before this Rule** **After this Rule**	Available from a specific Rule. Select **Move Rule To** and then move the cursor to the desired position. Select **Before this Rule** or **After this Rule** to move the rule to the required location.
Condition Level		
	✖ **Delete Condition**	Available from a specific Condition. Enables you to remove a Condition from a Rule.

3.2 User Policies

This section contains the following topics:

- Security Policy
- HTTPS Policy
- Logging Policy
- Default Policy Settings

3.2.1 Security Policy

A Security Policy is a set of rules that determines how to handle Web content passing through the system. It focuses on pro-actively blocking active content and malicious code while allowing non-dangerous content through.

Trustwave's default Security Policies are designed to meet your individual organization's unique security needs. The policies include proactive, behavioral, real-time elements in order to provide better security when connecting to the Internet.

In general, you cannot edit the predefined policies (or their components) that come with SWG. You can either use the predefined policies as provided, or you can duplicate them and edit the duplicates.

This section contains the following topics:

- Types of Security Policies
- Security Policy Details
- Security Rule Details
- Condition Details for Security Policy Rules

3.2.1.1 Types of Security Policies

The **Policies | User Policies | Security** menu option provides access to the following types of Security policies intended for special, and specific-use needs:

- **Trustwave Default Security Policy** — Based on the Medium Security Policy of previous versions, this policy provides out-of-the-box rules and conditions that are designed to meet most organization's security needs. This policy will automatically be assigned to users in the system if no other policies have been assigned to them in the Users tab. They will also be assigned automatically to unknown users.

- **Full Bypass Policy** — Intended for end-users who should be permitted to surf through the Trustwave SWG appliance without any scanning. This policy contains one rule (Allow All) which bypasses scanning, ensuring that no items will be scanned by the Trustwave engines.

- **Cloud User Policies** — Intended for limiting the Web usage of specific cloud users. Trustwave provides two predefined cloud user policies:

- **Trustwave Blocked Cloud Users Policy** — Intended to temporarily block specific users from using the cloud.

- **Trustwave Revoked Cloud Users Policy** — Intended to revoke permission for specific users to use the cloud.

- **Trustwave X-Ray Policy** — Intended to evaluate the effect of a potential security policy on the system before you actually implement it as a security policy. If a transaction meets the required conditions, the rule is logged but not activated, and the transaction continues with evaluation of the next rule. This continues for all rules in the policy. In this way, X-Ray Policy ensures that transactions are evaluated against rules, but there is no blocking action or content change.

  The results of the X-Ray Policy, and rules within, can be assessed in the Logs View (under Logs and Reports).

  In non-X-Ray Security Policies, you can specify that specific rules act as X-Ray rules, meaning that for those rules only, the rule will be logged but not activated, for evaluation purposes.

- **Trustwave Emergency Policy** — Designed for immediate site-wide implementation in special emergency situations (for example, the Internet has encountered a massive infectious attack, or for cases where the organization has been infected by malicious code). The Emergency Policies prevent/minimize damage by blocking most of the network traffic while still enabling access to some predefined important Web sites, such as Windows Update. (**Note:** A Trustwave Emergency HTTPS Policy is available for sites where HTTPS is licensed.)

  For full details on Security Policies, see the *SWG Security Policies In-Depth Guide*.

- **Master Security Policy** — You can also implement an additional level of Security policy, if there is a need. Master Security Policy can provide an extra level of protection by allowing Super Administrators to force general administrators to use a specific security policy in addition to the security policy the administrator can assign to its users. For more information, see Master Security Policy — An additional Security Policy level.

3.2.1.2 Security Policy Details

Click any Security Policy to display the Policy Details in the right pane.

For non-predefined Security Policies, click **Edit** in the right pane to edit the fields on this screen.

Policy Details Screen Fields

Field	Description
Policy Name	Name of the specific policy
X-Ray check box	Defines whether the Policy is X-Ray. (X-Ray means the policy is logged but no action is taken)
Description	Contains a description of the policy.

Field	Description
User Groups/ Users using this policy	Security Policies can be assigned to different User Groups and Users. This section displays which Users have this particular Policy assigned to them. For more information on assigning Policies to Users, see Users/User Groups.

3.2.1.3 Security Rule Details

Click a Security rule to display the Rules Details in the right pane.

For non-predefined Security Rules, click **Edit** in the right pane to edit the fields on this screen. When **Enable Rule** is selected, the **Advanced Action** options become activated.

The Rules Details screen contains the following tabs, and several fields that are independent of the tabs:

- General Tab

- Apply To Tab

- Exception Tab

Security Rule Details Screen Common Fields

Field	Description
Rule Name	Specify a name for the Security rule. Mandatory.
X-Ray	Select this check box if the rule should be evaluated in the Logs only. In this case, the rule will be activated and logged, but no block, warn or explicit allow actions will be performed.
Description	Specify a description of the rule (optional).
Enable Rule	Select this check box to enable the rule (followed by **Commit**). When cleared, the rule is disabled.

In certain circumstances, X-Ray block rules might block traffic. This happens when the Web server replies with non-standard HTTP traffic. This is applicable only for X-ray rules and not for X-ray policies.

For more detailed information on each of the Security Rules, see the *SWG Security Policies In-Depth Guide*.

3.2.1.3.1 General Tab

Security Rule Details Screen – General Tab Fields

Field/Value	Description
Action	Action to be taken (**Block**, **Coach** or **Allow**) on positive evaluation of the rule:
Block	The Web content is blocked.
Coach	The Web content is temporarily blocked and the end-user receives a warning message that this site is not recommended and that his/her activities will be logged. The end-user can then decide whether to proceed.
Allow	The Web content is allowed and the selected **Advanced Action** is taken as described below.
Advanced Action	When **Allow** is selected you can choose one of the following **Advanced Action** options:
Allow content and scan containers	The content is allowed, but container files are opened and the contents are scanned. (This is the default option.)
Allow content and do not scan containers	Allows content through including container files, such as zip or rar files, without scanning inside them. Content is allowed through on request stage but may be stopped on response stage.
Bypass Scanning	Allows content through without any scanning at all on the request or response stage. This allows full streaming and is useful, for example, for sites which contain stock ticker streaming.
Do not display End-User Message	Withholds sending a block page to the end-user.
End-User Message	Defines which message is sent in the Page Block/Warn message. The end-user message list and associated text is managed via Block/Warn Messages. The end-user Message template can be modified via Message Template.

- The Coach action can be applied to URL Categories and URL Lists in an Outgoing direction only. Furthermore, only the following Conditions can be added: Time Frame, Header Fields, File Extension.

- The Allow-Advanced actions which allow container files through without scanning can be placed anywhere in your Security Policy.

3.2.1.3.2 Apply To Tab

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

The **Apply To** tab enables you to specify to which users the rule will be applied. This tab displays a preset number of choices, each with a radio button (you can select only one). One of the choices however, displays the complete list of site-defined User Lists and enables you to select any number of those lists. (User Lists are defined via the **Users | User Lists** menu option. For more information, see User Lists.)

Security Rule Details Screen – Apply To Tab Fields

Field	Description
All Users	Select this radio button to apply the rule to all users (default). **Note**: You can still specify exceptions (via User Lists) in the **Exception** tab.
All Recognized Users	Select this radio button to apply the rule to all identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
All Unrecognized Users	Select this radio button to apply the rule to all non-identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
Select User Lists	Select this radio button to apply the rule to the user groups/users that are listed in the User Lists that you select. Then select the User Lists by selecting their check boxes. You can still specify exceptions (via User Lists) in the **Exception** tab.

3.2.1.3.3 Exception Tab

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

The **Exception** tab enables you to specify exception to the users that satisfy the user criteria that you specified in the **Apply To** tab. This tab displays the complete list of site-defined User Lists, and allows you to select any number of those lists. (User Lists are defined via the **Users | User Lists** menu option. For more information, see User Lists.)

To specify exceptions to the users who satisfy the user criteria specified in the **Apply To** tab, select the appropriate User Lists by selecting their check boxes.

3.2.1.4 Condition Details for Security Policy Rules

Click a Condition to display the Condition details in the right pane.

For non-predefined Security conditions, click **Edit** in the right pane to edit the fields on this screen.

Some items in Condition lists for Security, HTTPS, or Logging policies are displayed as links, in blue underlined text. Clicking a link opens another page for the item that displays the parameters of the condition. For example, clicking the **Web Pages** link for the **File Extensions** condition displays the out-of-the-box list of suspicious file extensions. Condition parameters can also display as links to additional information.

Out-of-the-box lists are not editable and the Edit button on such pages is disabled. To change the parameters of an *editable* condition, click the **Edit** button and make the changes you require. For example, you could add or delete one or more file extensions in the File Extension Cache Bypass List.

> While in this drill-down mode, the SWG menu and navigation tree are disabled. To return to the Condition list, click the **Back** button or follow the path navigation at the top of the page.

Security Policy Rules Screen Condition Detail Fields

Field	Description
Condition Name	Displays name of Condition. If you are defining a new condition, choose the required condition from the drop down list.
Applies To	You can select which options are to be included or excluded. In other words, you can either choose to apply this rule to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select/Deselect All	Choose to select/deselect all the items in the Condition
Note: The items display differently according to the Condition you have chosen.	

The following Conditions are available for selection within the Security Policy rules:

- Active Content List
- Anti-Virus (McAfee/Sophos/Kaspersky)
- Application Control
- Archive Errors
- Behavior Profile (Binary)
- Binary VAD
- Content Size
- Data Leakage Prevention

- Digital Signature

- Direction

- File Extensions

- HTTP Method

- Header Fields

- IM

- Location

- Malware Entrapment Profile

- Parent Archive Type

- Protocol

- Spoofed Content

- Static Content List

- Time Frame

- True Content Type

- URL Filtering (Trustwave)

- URL Lists

3.2.1.4.1 Active Content List

The Active Content List condition contains active content objects such as ActiveX Controls and Java Applets that have already been scanned by SWG, and are located in the SWG Server Database or added by the Malware team at Trustwave. Each newly scanned Applet, Control or Executable is automatically added to the Auto-generated list, which is the only list that cannot be used in a rule. Items from the Auto-generated list may be moved to other lists, such as Allowed, Blocked or customer created lists in order to create exception rules.

This condition can be used to block or allow specific and known active content objects, without changing the Default Security Policy.

Allowed and Blocked lists can be modified via the Active Content List**.**

Security Policy Condition Rules – Active Content List Options

Option	Description
Allowed	List of trusted objects from the Auto-generated list which were identified as such by the administrator.
Auto-Generated	Content list and automatically generated signature and security profile, of all active content scanned by the Active Content engine.

Option	Description
Blocked	List of suspicious objects from the Auto-generated list which were identified as such by the administrator.

3.2.1.4.2 Anti-Virus (McAfee/Sophos/Kaspersky)

This condition is used to identify known viruses by using traditional (signature-based) third party Anti-Virus scanners such as McAfee, Sophos or Kaspersky.

The Anti-Virus engine appears in **Administration | System Settings | Scanning | Scanning Engines** but cannot be configured by the administrator.

Security Policy Condition Rules – Anti-virus Options

Option	Descriptions
The AV Engine could not scan this file	Refers to files that the Anti-Virus engine could not scan.
Virus Detected	Refers to files that contain a virus detected by the Anti-Virus engine.

3.2.1.4.3 Application Control

Business use of Web applications presents a number of security, compliance, and productivity challenges. Trustwave assists enterprises to mitigate these issues by providing granular control of common social media applications. SWG Application Control is supported for Facebook, LinkedIn, Google +, Twitter, and YouTube.

Administrators can define which specific activities to block for which groups of users, or even for which individual users.

A built-in set of Application Control Profiles is defined. The profile set can be easily adjusted to the organization's own definition.

You cannot edit a pre-supplied action list, but you can duplicate it and edit the duplicate. The **Edit** button on pre-supplied lists is disabled.

Application Control provides the following benefits:

- Visibility and control over applications

- Reduction in the risk of exposure of sensitive data

- Reduction in the vectors that can be utilized for attacks, and optimization of security scans by limiting allowed protocols and applications

- Optimization of bandwidth usage and improved productivity by limiting non-relevant application usage

Application Control Profiles

SWG provides a set of profiles that enable administrators to define how users can interact with Facebook, LinkedIn, Google +, Twitter, and YouTube social media applications. Once a profile is defined, it can be used as a condition in the rules with type "Application Control".

The default profiles are defined as:

- **Allow Read-only** - groups user activities that are not for viewing only

- **Allow Limited interactivity** - groups interactive activities

- **Block Chat** - Groups chat activities

- **Block Upload Pictures and Videos** - Groups uploading activities

Profiles contain Action Groups of relevant social media actions for each supported social media application. The actions included in these groups are continuously maintained. Where deemed necessary, the action lists will be extended or adapted to support more activities or additional applications. For more information, see the *SWG Application Control User Brief*.

> Application control of social apps embedded in other social media must be applied to the app itself. For example, user access and use of YouTube from within Facebook is controlled by the Action Group selections of YouTube, not of Facebook.

You cannot edit a pre-supplied action list, but you can duplicate it and edit the duplicate. The **Edit** button on pre-supplied lists is disabled.

To change the allowed actions of an *editable* list, click the **Edit** button and make the changes you require.

3.2.1.4.4 Archive Errors

The Archive Errors condition identifies compressed archive files (such as ZIP) which contain various errors.

The archive depth, maximum entries in container and maximum extracted content size can be edited via Archives.

Security Policy Condition Rules – Archive Error Options

Option	Description
Archive Depth – exceeded	Nesting depth (such as archives within archives) exceeds the predefined limit.
File could not be extracted	The file could not be extracted from the container.
Invalid format	Contains an invalid format.
Maximum Entries in Container – exceeded	Number of files in the container exceeds the predefined limit.
Maximum Extracted Container Size – exceeded	The expanded file size exceeds the predefined limit.

Option	Description
Password protected	The Archive is password protected.

3.2.1.4.5 Behavior Profile (Binary)

This condition is used to identify binary files which perform forbidden operations and violate the Behavior Profile policy. Behavior Profiles are lists of actions that might be considered malicious or suspicious when executed by ActiveX Controls, Java Applets, executable files or other relevant files. Each Behavior Profile contains a different subset of these forbidden actions. Administrators cannot modify or delete the default Profiles. However they can duplicate Profiles which can then be customized.

The Binary Behavior profiles can be viewed, duplicated and edited via Binary Behavior.

The table below shows the default options in the Behavior Profile (Binary) condition:

Behavior Profile (Binary) condition - default options

Option	Description
Default Profile – Binary Behavior	Refers to the default Binary Behavior Profile.
Full Profile – Binary Behavior	Refers to the full profile (this includes the higher sensitivity profile and any new behaviors).
Higher Sensitivity Binary Behavior Profile	Refers to the Higher Sensitivity Profile which has every single item selected within the profile.
Medium Sensitivity Binary Behavior Profile	Refers to the Medium Sensitivity Profile which has items selected within the profile.
Suspected Malware	Contains behavior profile patterns that are specific to malicious software. This is a pre-defined Profile which is supplied with the Anti-Spyware module and cannot be modified or viewed by the administrator.
Unscannable Active Content	Refers to active content that has not been scanned.

3.2.1.4.6 Binary VAD

The Binary Vulnerability Antidote (VAD) condition scans binary files, looking for patterns of exploits.

The Binary VAD security level can be set using a slider. Available levels are **None**, **Basic**, **Medium**, **High**, and **Strict**.

3.2.1.4.7 Content Size

This condition is used to assign rules to specific file sizes. Content size is relevant for performance and stability, not necessarily security.

The administrator can create new content sizes as required via Content Size**.**

3.2.1.4.8 Data Leakage Prevention

This condition enables the administrator to monitor and prevent data leakage of confidential information.

The screen shows a list of pre-defined conditions from which to choose. The administrator can build new data leakage prevention conditions by using the Script Expression Editor. See Creating/Editing a Data Leakage Prevention Script.

3.2.1.4.9 Digital Signature

This condition enables the administrator to block (or allow) content where the digital signature is either missing or invalid. The missing or invalid Digital Signatures are maintained and updated by Trustwave and cannot be accessed by the administrator. Digital signatures provide an extra layer of security in determining the integrity of the content.

Security Policy Condition Rules – Digital Signature Options

Option	Description
Invalid Digital Signature	The digital signature is invalid. For example, it might be corrupted or it might have expired.
Missing Digital Signature	The binary object does not have a digital signature.

3.2.1.4.10 Direction

This condition enables the administrator to trigger a rule specifically on the request (Outgoing) or response (Incoming) phase of the transaction. For example, in HTTP, outgoing is the request phase, and in ICAP, outgoing is the REQMOD phase. If no direction is specifically applied – then the rule is checked on both the request and response phases.

Security Policy Condition Rules – Direction Options

Option	Description
Incoming	Information coming from the Internet to the end-user.
Outgoing	Information sent from the end-user to the Internet.

3.2.1.4.11 File Extensions

This condition refers to the requested content type, meaning, the file extension. This condition also includes potentially malicious multiple extensions (for example, txt.exe). This condition is normally enforced during the request phase.

The File Extensions condition can be modified via File Extensions.

3.2.1.4.12 HTTP Method

This condition is used in conjunction with the Social Media Posts rule. The HTTP Method is a content processor that provides the ability to select, through the security policy condition, possible values such as GET, POST, LOCK, and so on. This feature supports HTTP, ICAP, and HTTPS/SSL requests.

The list of supported HTTP Method types is predefined and not editable.

3.2.1.4.13 Header Fields

This condition is used to identify transactions based on request or response HTTP headers.

The Header Fields condition can be modified via Header Fields.

Security Policy Condition Rules – Header Field Options

Option	Description
Content-Disposition Executable	Defines malicious executables detected as spoofed executables.
Exclude by Headers	Provides a list for customers to add headers which identify applications (such as IM).
Firefox 1.x and 2.x	Defines specific browser versions of Firefox
Media Players	Defines Media Players header fields.
Netscape 7.x	Defines browser version of Netscape version 7.
Older and Unsafe Browsers	Defines a list of browsers based on older versions and those that are considered unsafe.
Partial Downloading	Refers to partial downloads of Internet content.
SSL	Defines SSL header fields. Pinpointing specific SSL headers enables the administrator to build specific rules regarding SSL content.
Trojans	Defines header fields suspected of being created by a Trojan Horse.

3.2.1.4.14 IM

This condition is used to identify an initialization of Instant Messenger transactions, which are tunneled through port 80. You can use this condition to log or block new IM sessions, but it cannot be used to track sessions that have been opened or scan the content of transferred files or messages. IM includes AOL, ICQ, MSN Messenger and Yahoo Messenger.

This list of supported IM types is predefined and not editable.

3.2.1.4.15 Location

This condition enables the administrator to block (or allow) content based on the location of the scanning server.

Security Policy Condition Rules – Location Options

Option	Description
Cloud	The scanning server is located in the Internet cloud.
Local	The scanning server is located in the enterprise.

3.2.1.4.16 Malware Entrapment Profile

Trustwave's Malware Entrapment scanning engine monitors security behaviors and profiles that are subsets of all available behaviors. The groups at various levels define language tokens, semantic patterns of Active Code, forbidden combinations of operations, parameters and programming techniques. These groups are created by security experts from the Malware team at Trustwave, and fed into the Malware Entrapment scanning engine, enabling the identification of malicious active content.

Malware Entrapment Profiles are divided into five different security levels: **None**, **Basic**, **Medium**, **High** and **Strict**. The security levels pertain to the efficacy with which these behavior profiles are enforced. The SWG system is pre-configured, by default, at the Medium security level. Administrators can set an appropriate security level on a per policy basis.

Each level consists of a Malware Entrapment profile, that is used to identify textual files which perform forbidden operations and violate the profile policy. Malware Entrapment profiles are lists of actions that could be considered malicious or suspicious when executed by Web pages, VB Script files, Java Script files or other relevant files.

3.2.1.4.17 Parent Archive Type

An archive file is considered a "parent" when it contains other files inside it, such as ZIP, CAB, and so on. This condition will not match files outside of archives or the archive files themselves.

This list of supported archive types is predefined and not editable.

When using the Parent Archive Type condition, at its Rule level, you can set the **Action** to **Allow** and then choose one of the **Advanced Action** options:

• Allow transactions and scan containers

This is the default option. The content is allowed, but container files are opened and the contents are scanned. File scanning is controlled by Archives, where **Archive Depth** configures the maximum depth level of nested archives.

• Allow content and do not scan containers

Allows content through including container files, such as zip or rar files, without scanning inside them. Content is allowed through on request stage but may be stopped on response stage, for example if the File Extensions condition is used.

• Bypass Scanning

Allows content through without any scanning at all on the request or response stage.

3.2.1.4.18 Protocol

The Protocol condition enables detection of different types of protocols and can block or allow them in conjunction with other conditions.

This list of supported protocols is predefined and not editable.

Security Policy Condition Rules – Protocol Options

Option	Description
FTP over HTTP	Protocol between a Web browser and an FTP endpoint/proxy.
HTTP	Protocol which usually uses port 80.
HTTP Tunneling	HTTP Tunneling forwards packet data in both ways, hence acting as a tunnel. It can also be used for delivering HTTPS traffic and for ICAP.
HTTPS	Protocol used between Trustwave's SSL appliance and the SWG appliance.
Native FTP	FTP Protocol which usually uses port 21.

3.2.1.4.19 Spoofed Content

This condition identifies potentially malicious file content using deception to appear harmless. The list of potentially malicious files and their spoofed type is provided by Trustwave. In addition to the spoofed content detected by the scanning engine, one can also block unscannable content.

Security Policy Condition Rules – Spoofed Content Options

Option	Description
Spoofed Content	Potentially malicious file content using deception to appear harmless.
Unscannable Data	Unscannable content.

3.2.1.4.20 Static Content List

This condition is used to identify known malicious objects based on their malicious behavior signatures.

These content and object lists are invisible to the administrator and are constantly updated by the Malware team at Trustwave.

Security Policy Condition Rules – Static Content List Options

Option	Description
Known Legitimate Content List	Content known to be safe.
Malicious Objects List	Malicious objects based on their malicious behavior signatures.

3.2.1.4.21 Time Frame

This condition is used to execute Policies during certain hours of the day or week. As such, rules based on this condition reflect the needs of your organization and focus on productivity rather than security.

These settings can be modified via Time Frame.

Security Policy Condition Rules – Time Frame Options

Option	Description
Business Hours	Monday through Friday, 9:00am to 5:30pm
Lunch Break	Monday through Friday, 12:30pm to 1:00pm
Weekend	Friday 5:30pm to Sunday 11:59pm

3.2.1.4.22 True Content Type

Unlike declared content type, such as file extension or MIME type, the True Content Type engine can detect types of files based on their actual structure and format. This condition can identify known file types even if they have a non-standard name.

The list of supported file types is predefined and not editable.

3.2.1.4.23 URL Filtering (Trustwave)

URL Filtering blocks or allows content based on analysis of its content, rather than its source. To this end, a proprietary Trustwave List Categorization engine is deployed as the URL Categories Filter in the Secure Web Gateway. SWG can also classify URL pages using TextCensor in cases where the URL Categorization engine fails to classify them. TextCensor is Trustwave's proprietary DLP and URL categorization engine.

> Every SWG deployment has only a single URL Categorization Engine License. The appropriate license is selected upon initial acquisition of the primary SWG license and is dependant on the number of Users.

The Trustwave URL Categories Filter identifies embedded URLs as opposed to some third party URL filters which cannot.

The filter offers a set of logical groupings to the categories they provide. This is used to simplify the policy settings and enable actions to be set by category group and not by every individual category. These category groups are also used for **Reports** and **Logging**, which provide the necessary information for administrators to set policies accordingly. (Block/Allow/Coach specific categories, such as Entertainment or Games).

3.2.1.4.24 URL Lists

This condition refers to predefined and configurable lists of URL addresses.

The administrator can use this condition to create blocking or coaching rules as required. These lists can be modified and created via URL Lists.

> The Trustwave Recommended Black List cannot be viewed.

3.2.2 HTTPS Policy

HTTPS policies focus on securing Internet Content on HTTPS sites. They provide the option to define which HTTPS sites are fully allowed, which are inspected, which request user approval to continue and which are blocked. The blocking mechanism is based on White Lists, URL categorization and checking to see if Certificates have errors or comply with validation criteria. The HTTPS Policies are only displayed for customers who have the required license. HTTPS Policies can be assigned per User Group or User.

This section contains the following topics:

- HTTPS Policies Tree

- HTTPS Policy Details

- HTTPS Rule Details

- Condition Details for HTTPS Policy Rules

3.2.2.1 HTTPS Policies Tree

The HTTPS Policies tree holds all the current HTTPS Policies within that definition, as well as the rules that make up these Policies and the conditions that make up the rules.

Trustwave provides two pre-configured default HTTPS policies:

- **Trustwave Emergency HTTPS Policy**: This was designed for emergency situations and contains two rules. This can be globally enabled via Default Policy Settings. This can also be enabled per User.

- **Trustwave HTTPS Policy**: This Policy contains just one rule which is designed to block any sites which contain faulty certificates.

> For full details on the Trustwave HTTPS Policy and Trustwave Emergency HTTPS Policy and their rules, see the *SWG Security Policies In-Depth Guide*.

Policies, rules, and conditions can be added, duplicated or deleted by right-clicking the relevant node. Trustwave's default HTTPS Policies cannot be modified or deleted. However, they can be duplicated to create new customizable policies.

3.2.2.2 HTTPS Policy Details

Click any HTTPS Policy to display the Policy Details screen in the right pane.

To edit the fields on this screen, click **Edit** in the right pane.

HTTPS Policy Details Screen Fields

Field	Description
Policy Name	Name of the specific HTTPS policy.
Description	Description of the policy.
User Groups	Policies can be assigned to different User Groups and Users. This section displays which Users have this particular Policy assigned to them. For more information on assigning Policies to Users, see Users/User Groups.

3.2.2.3 HTTPS Rule Details

Click an HTTPS rule to display the Rules Details screen in the right pane.

To edit the fields on this screen, click **Edit** in the right pane. Note that you cannot edit predefined policies.

The HTTPS Rules Details screen contains the following tabs, and several fields that are independent of the tabs:

- General Tab

- Apply To Tab

- Exception Tab

HTTPS Rules Screen Common Fields

Field	Description
Rule Name	Specify a name for the HTTPS rule. Mandatory.
Description	Specify a description of the rule (optional).
Enable Rule	Select this check box to enable the rule is enabled (following Commit). When cleared, the rule is disabled.

Selecting Add Condition defines the conditions for inclusion within the rule. See Condition Details for HTTPS Policy Rules for further information.

3.2.2.3.1 General Tab

HTTPS Rules Screen – General Tab Fields

Field/Value	Description
Action	Action to be taken (**Block HTTPS**, **User approval**, **Bypass**, or **Inspect Content**) upon positive evaluation of the rule:
Block HTTPS	Blocks HTTPS sites.
User approval	Sends an approval page to the end-user for each new HTTPS site that is accessed. This is sent for situations where user approval is required to decrypt traffic for this site. If the end-user chooses not to approve the transaction, the connection is closed.
Bypass	No HTTPS or Security scanning will take place.
Inspect Content	HTTPS rules and Security rules scanning is performed (default).
End-User Message	Displayed if the selected action is **Block HTTPS** or **User Approval**. This field defines which reason to use in the message sent to the end-user. The reason text and template can be edited. For more information, see End User Messages.
Do not display End-User message	Displayed if the selected action is **Block HTTPS**. Select this check box if a message should not be displayed to the end-user whenever a page is blocked.

After content is scanned by the HTTPS rules, the content will be subjected to security scanning.

3.2.2.3.2 Apply To Tab

The **Apply To** tab enables you to specify to which users the rule will be applied.

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

This tab displays a preset number of choices, each with a radio button (you can select only one). One of the choices however, displays the complete list of site-defined User Lists, and enables you to select any number of those lists. (User Lists are defined via the **Users | User Lists** menu option. For more information, see User Lists.)

HTTPS Rules Screen – Apply To Tab Fields

Field	Description
All Users	Select this radio button to apply the rule to all users (default). **Note**: You can still specify exceptions (via User Lists) in the **Exception** tab.

HTTPS Rules Screen – Apply To Tab Fields

Field	Description
All Recognized Users	Select this radio button to apply the rule to all identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
All Unrecognized Users	Select this radio button to apply the rule to all non-identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
Select User Lists	Select this radio button to apply the rule to the user groups/users that are listed in the User Lists that you select. Then select the User Lists by selecting their check boxes. You can still specify exceptions (via User Lists) in the **Exception** tab.

3.2.2.3.3 Exception Tab

The **Exception** tab enables you to specify exceptions to the users that satisfy the user criteria that you specified in the **Apply To** tab.

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

This tab displays the complete list of site-defined User Lists (which are defined via the **Users | User Lists** menu option. For more information, see User Lists), and enables you to select any number of those lists.

To specify exceptions to the users who satisfy the user criteria specified in the **Apply To** tab, select the appropriate User Lists by selecting their check boxes.

3.2.2.4 Condition Details for HTTPS Policy Rules

HTTPS Policy Rules contain one or more conditions. When clicking a Condition, the Condition details are displayed in the right pane.

Some items in Condition lists for Security, HTTPS, or Logging policies are displayed as links, in blue underlined text. Clicking a link opens another page for the item that displays the parameters of the condition. For example, clicking the **Web Pages** link for the **File Extensions** condition displays the out-of-the-box list of suspicious file extensions. Condition parameters can also display as links to additional information.

Out-of-the-box lists are not editable and the Edit button on such pages is disabled. To change the parameters of an *editable* condition, click the **Edit** button and make the changes you require. For example, you could add or delete one or more file extensions in the File Extension Cache Bypass List.

While in this drill-down mode, the SWG menu and navigation tree are disabled. To return to the Condition list, click the **Back** button or follow the path navigation at the top of the page.

HTTPS Policy Rules Condition Details Screen

Field	Description
Condition Name	Displays name of Condition. If you are defining a new condition, choose the required condition from the drop down list.
Applies To	You can select which options are to be included or excluded. In other words, you can either choose to apply this rule to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select/Deselect All	Choose to select/deselect all the items in the Condition
The items will display differently according to the Condition you have chosen.	

Predefined HTTPS Policies and their Rules/Conditions cannot be edited. Policies and their Rules/Conditions added by the administrator have the option to be changed using the **Edit | Save/Cancel** options. Each HTTPS rule may include multiple conditions - all of which must be met in order for the rule to be fired.

The following Conditions are available for selection within the HTTPS rules:

- Certificate Validation Errors refers to various types of errors that can arise when checking the validity of certificates for secured content.

- Location enables the administrator to block (or allow) content based on the location of the scanning server.

- URL Lists refers to predefined and configurable lists of URL addresses.

3.2.2.4.1 Certificate Validation Errors

This condition refers to various types of errors that can arise when checking the validity of certificates for secured content.

The Certificate Validation errors can be viewed and customized via HTTPS Certificate Validation.

3.2.2.4.2 Location

This condition enables the administrator to block (or allow) content based on the location of the scanning server.

Certificate Validation Errors Screen – Location Options

Option	Description
Cloud	The scanning server is located in the Internet cloud.
Local	The scanning server is located in the enterprise.

Policies

92

3.2.2.4.3 URL Lists

This condition refers to predefined and configurable lists of URL addresses.

The administrator can create new lists in the Lists tab which will appear as part of the condition. These lists can be viewed and modified via URL Lists.

3.2.3 Logging Policy

A Logging Policy is a set of rules that deals with the logging of transaction data and determines which actions are recorded for analysis. The only action resulting from a logging rule is to log the transaction. The Logging Policy can implement logging at different levels, depending on your requirements. Logging Rules decide both what is logged (blocked, allowed, all) and where the information is sent (to logs, archives, reports, and so on). As with Security rules, any action taken will be according to the rule of highest priority that matches the terms of the Rule.

> If any transaction is not matched specifically in the rules, it is allowed. Meaning, the SWG default behavior is **Allow**.

This section contains the following topics:

• Logging Policies Tree

• Logging Policy Details

• Logging Rule Details

• Conditions for Logging Policy Rules

3.2.3.1 Logging Policies Tree

The Logging Policies tree holds all the current Logging Policies within that definition, as well as, the rules that make up these Policies and the conditions that make up the rules.

This provides easy navigation through each Policy – displaying the components of that Policy at a glance.

Policies, rules, and conditions can be added or deleted by right-clicking the relevant node. Trustwave's default Logging Policies cannot be modified or deleted. However, they can be duplicated to create new customizable policies.

Trustwave provides four default Logging Policies:

- Archive All Protective Actions (RUSafe mode only)

- Log All Protective Actions

- Log All Protective Actions and Web pages

- Logging everything except Image files

Logging Rules Tree Policies

Rule Name	Description	Target
Log All Coached Transactions	Logs all HTTP transactions that have been defined as coach in the Security Policy.	Send to log Send to report
Log All Blocked Transactions	Logs all HTTP transactions that have been defined as block in the Security Policy.	Send to log Send to report
Log all User Approval Transactions	Logs all HTTPS transactions that have been defined as User Approval in the HTTPS Policy.	Send to log Send to report
Log all Block HTTPS Transactions	Logs all HTTPS transactions that have been defined as block in the HTTPS Policy.	Send to log Send to report
Log all Web pages (relevant for Log All Protective Actions and Web pages policy only)	Logs all Web pages that have passed through the system (both HTTP and HTTPS)	Send to log
Log everything except Image files (relevant for Logging everything except Image files policy only)	Logs all content passing through the system except for Image files (both HTTP and HTTPS)	Send to log
Log All Coached Transactions	Logs all HTTP transactions that have been defined as coach in the Security Policy.	Send to log Send to report

You may, for example, want to log all blocked transactions together with all transactions where Web pages were viewed, in order to analyze URL categories accessed by your users. Another example is that you may want to log all HTTP Web pages only. In this case, you would duplicate the Log All Protective Actions policy and amend the rules by choosing to select everything except the HTTPS Protocol.

When defining the Logging Rule, the conditions selected must match those of the Security Policy rule in order for the relevant transactions to appear in the Log View.

3.2.3.2 Logging Policy Details

Click a Logging Policy to display the Policy details in the right pane.

The Policy Details screen contains the following information with the option to make changes using the **Edit | Save/Cancel** options.

Logging Policy Details Screen Fields

Field	Description
Policy Name	Name of the specific policy
Description	Contains a description of the policy.
User Groups / Users	Policies can be assigned to different User Groups and Users. This section displays which Users have this particular Policy assigned to them. For more information on assigning Policies to Users, see Users/User Groups.

3.2.3.3 Logging Rule Details

Clicking any Logging rule displays the Rule Details screen in the right pane.

The Logging Rules Details screen contains the following three tabs, and several fields that are independent of the tabs:

- General Tab

- Apply To Tab

- Exception Tab

The following fields describe the fields that appear above, and are independent of, the tabs in HTTPS Policy rules:

Logging Rules Details Screen Common Fields

Field	Description
Rule Name	Specify a name for the Logging rule. Mandatory.
Description	Specify a description of the rule (optional).
Enable Rule	Select this check box to enable the rule (followed by Commit). When cleared, the rule is disabled.

3.2.3.3.1 General Tab

<div align="center">Logging Rules Details Screen – General Tab Fields</div>

Field	Description
Send To:	Select to which locations the logging information should be sent by selecting the appropriate check boxes:
Weblog	Sends information to the Trustwave log database, which can be seen via the Log View.
Archive	Sends log information in files to an external remote location. This must be selected to ensure that there is relevant information to archive.
Report	Sends information to the Trustwave reports database. This must be selected prior to running Reports to ensure that there is relevant information to display results.
Syslog	Sends information to one or two UNIX Syslog facilities which log data.

3.2.3.3.2 Apply To Tab

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

The **Apply To** tab enables you to specify to which users the rule will be applied. This tab displays a preset number of choices, each with a radio button (you can select only one). One of the choices however, displays the complete list of site-defined User Lists (which are defined via the **Users | User Lists** menu option. For more information, see User Lists), and enables you to select any number of those lists.

The following table describes the fields of the Apply To tab:

<div align="center">Logging Rules Details Screen – Apply To Tab Fields</div>

Field	Description
All Users	Select this radio button to apply the rule to all users (default). **Note**: You can still specify exceptions (via User Lists) in the **Exception** tab.
All Recognized Users	Select this radio button to apply the rule to all identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
All Unrecognized Users	Select this radio button to apply the rule to all non-identified users. You can still specify exceptions (via User Lists) in the **Exception** tab.
Select User Lists	Select this radio button to apply the rule to the user groups/users that are listed in the User Lists that you select. Then select the User Lists by selecting their check boxes. You can still specify exceptions (via User Lists) in the **Exception** tab.

3.2.3.3.3 Exception Tab

This tab appears in and works the same for **Security**, **HTTPS**, and **Logging** policy rules.

The **Exception** tab enables you to specify exception to the users that satisfy the user criteria that you specified in the **Apply To** tab. This tab displays the complete list of site-defined User Lists (which are defined via the **Users | User Lists** menu option. For more information, see User Lists), and enables you to select any number of those lists.

To specify exceptions to the users who satisfy the user criteria specified in the **Apply To** tab, select the appropriate User Lists by selecting their check boxes.

3.2.3.4 Conditions for Logging Policy Rules

Click a Condition to display the Condition details in the right pane.

Some items in Condition lists for Security, HTTPS, or Logging policies are displayed as links, in blue underlined text. Clicking a link opens another page for the item that displays the parameters of the condition. For example, clicking the **Web Pages** link for the **File Extensions** condition displays the out-of-the-box list of suspicious file extensions. Condition parameters can also display as links to additional information.

Out-of-the-box lists are not editable and the Edit button on such pages is disabled. To change the parameters of an *editable* condition, click the **Edit** button and make the changes you require. For example, you could add or delete one or more file extensions in the File Extension Cache Bypass List.

While in this drill-down mode, the SWG menu and navigation tree are disabled. To return to the Condition list, click the **Back** button or follow the path navigation at the top of the page.

The Condition Details screen displays the following information with the option to make changes using the **Edit | Save/Cancel** options.

<div align="center">Logging Policy Rule Conditions Screen Fields</div>

Field	Description
Condition Name	Displays name of Condition. If you are defining a new condition, choose the required condition from the drop down list.
Applies To	You can select which options are to be included or excluded. In other words, you can either choose to apply this rule to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select/Deselect All	Choose to select/deselect all the items in the Condition.
The bottom of the screen will display differently according to the Condition you have chosen.	

The following Conditions are available for selection within the Logging Policy rules:

> The following links (except Rule Action) point to descriptions under Condition Details for Security Policy Rules. The Rule Action link points to a description in this section.

- Active Content List

- Archive Errors

- Behavior Profile (Binary)

- Malware Entrapment Profile

- Content Size

- Digital Signature

- Direction

- File Extensions

- Header Fields

- IM

- Location

- Parent Archive Type

- Protocol

- Spoofed Content

- Static Content List

- Time Frame

- True Content Type

- URL Filtering (Trustwave)

- URL Lists

- Rule Action

3.2.3.5 Rule Action

This condition enables you the option of logging transactions when a specific end user action is carried out:

- Allow

- Block

- Block HTTPS

- Bypass

- Coach

- Inspect Content

- User Approval

Rule Action is only available for Logging Rules.

> **Warning:** If you want to log all end-user actions, do not include the Rule Action condition in your Logging Policy Rule.

> If you want to log more than one end-user action (but not all of them), you must add a separate rule for each action you need to the Logging Policy.

3.2.4 Default Policy Settings

In the **Default Policy Settings** screen you can define options relating to the Security, HTTPS and Logging Policies.

Enable Emergency Policy – Setting Emergency Policies here assigns them to all Users and overrides any other Security Policies individually set per User or per User Group.

- From the **Emergency Policy** drop down list, select the policy to be used as an emergency policy.

- From the **Emergency HTTPS Policy** drop down list, select the policy to be used as an emergency HTTPS policy.

Default Policy Values – The default Security, Logging and HTTPS policies are set here and will automatically be assigned to users in the system if no other Policies have been assigned to them in the Users tab. They will also be assigned automatically to unknown users.

- From the **Master Policy** drop down list, select one of the policies to be used as the Security policy by default. The empty option is the default value provided by the system. For more information, see Master Security Policy — An additional Security Policy level.

- From the **Security Policy** drop down list, select one of the policies to be used as the Security policy by default. The **Trustwave Default Security Policy** is the default value provided by the system.

- From the **Logging Policy** drop down list, select one of the policies to be used as the Logging policy by default. The **Log All Protective Actions** policy is the default value provided by the system.

- From the **HTTPS Policy** drop down list, select one of the policies to be used as the HTTPS policy by default. The **Trustwave Default HTTPS Policy** is the default value provided by the system.

> The policies you define here will be the values referred to in User Groups and LDAP Groups.

3.2.4.1 Master Security Policy — An additional Security Policy level

You can implement an additional level of Security policy, if there is a need. This level is called **Master Security Policy**.

Master Security Policy can provide an extra level of protection by allowing Super Administrators to force general administrators to use a specific security policy in addition to the security policy the administrator can assign to its users.

Once the Super Administrator assigns a master policy to an Administrator, all the users managed by this Administrator will be forced to use this policy in addition to the normal security policy defined.

Note that Master Security Policy is not a policy per se, but rather a Security Policy assignment. Just as you can assign any Security policy as the policy of the site and/or a particular User Group, so you can assign any Security Policy as the Master Security Policy of the site and/or a specific administrator.

- Usage of the Master Security Policy level is optional, and unless there is a good reason for implementing it, it is recommended that you do not. (By default, no policy assignment is made for Master Security Policy.)
- The Master Policy and the Security Policy for a user can be the same. There is a chance however, that a minimal amount of system degradation could occur.
- You can configure the Master Policy in X-ray mode (in which case, the policy is logged but no action is taken).

Log events triggered by the Master Policy as opposed to those triggered by the normal security policy, are indicated as such in the **Transaction Details** area of the Management Console Web Logs screen.

Master Policy Name and **Master Rule Name** must be selected in the Web Logs Profile Settings pane **General** tab to display their corresponding columns in the **Transaction Details** area.

In the case of customer license expiration or an emergency, the Master Policy will be the default Master Policy.

3.3 Device Policies

This section contains the following topics:

- Caching Policy
- Device Logging Policy
- Identification Policy
- Upstream Proxy Policy
- ICAP Request and Response Modification Policies

3.3.1 Caching Policy

The SWG Appliance can be used as a caching device. This means that the content is stored in the appliance for future use – thereby speeding up performance time.

Trustwave provides a single predefined Caching Policy, **Trustwave Default Caching Policy**, which contains two rules:

- **Bypass caching by URL**, which has a condition, **URL Lists**.

- **Bypass caching by File Extension**, which has a condition, **File Extensions**.

The Caching policy is a global policy that applies to all users who browse using the system. By default, when caching is enabled, all content is cached (no check boxes in the URL Lists and File Extension Lists are selected).

You cannot edit the pre-supplied Caching policy, but you can duplicate it and edit the duplicate.

Caching policy consists of both an Action and a Condition and are configured by system administrators.

- **Action:** The administrator can set the Action to bypass caching according to specific URL or file extension lists, ensuring that specific, non-cacheable URLs or specific file extensions are not cached. System administrators can also cache only specific sites or file extensions.

- **Condition:** Once an action is set, the administrator can select the criteria to which the rule will or will not match. The condition can be a specific URL list, multiple URL lists, or all lists excluding selected URL lists. Administrators can also select file extensions that Trustwave SWG caches or bypasses.

To bypass a specific type of traffic, edit the appropriate list (and select the appropriate check boxes).

This section contains the following topics:

- Caching Policy Details

- Caching Policy Rule Details

- Caching Policy Rule Condition Details

3.3.1.1 Caching Policy Details

Click any Cache Policy to display the **Details** screen in the right pane.

The Caching Policy Details screen contains the following information with the option to make changes using the **Edit | Save/Cancel** options:

Caching Policy Details Screen

Field	Description
Policy Name	Name of the specific policy
Description	Contains a description of the policy.

3.3.1.2 Caching Policy Rule Details

For non-predefined Rules, click **Edit** in the right pane to edit the fields on this screen.

Caching Policy Rule Details Screen Fields

Field	Description
Rule Name	Defines the name of the Caching rule.
Description	This provides a place for you to write a description of the rule.
Enable Rule	When selected, the rule is enabled. When cleared the rule is disabled.
Action: Cache	The Web content is cached.
Action: Bypass Cache	The Web content is not cached.

3.3.1.3 Caching Policy Rule Condition Details

To add a condition to a caching policy rule, right-click the rule in the Policies tree and click **Add Condition**. The **Condition Details** screen appears in the right pane. To edit an existing condition, click **Edit** in this pane.

Caching Policy Rule Condition Details Screen Fields

Field	Description
Condition Name	Displays name of Condition. If you are defining a new condition, choose the required condition from the drop down list. The following options are available: • File Extensions • Location • URL Lists
Applies To	You can select which options are to be included or excluded. In other words, you can either choose to apply this rule to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select /Deselect All	Choose to select/deselect all the items in the Condition.
The items will display differently according to the Condition you have chosen.	

3.3.2 Device Logging Policy

Device Logging Policies log the transactions carried out by the Identification and Upstream Proxy Policies.

This section contains the following topics:

- Device Logging Policies Tree

- Device Logging Policy Details

- Device Logging Rule Details

- Device Logging Policy Rule Conditions

3.3.2.1 Device Logging Policies Tree

The Device Logging Policies tree holds all the current Device Logging Policies within that definition—as well as the rules that make up these Policies—and the conditions that make up the rules. This provides easy navigation through each Policy – displaying the components of that Policy at a glance.

Policies, rules, and conditions can be added or deleted by right-clicking the relevant node. Trustwave's default Device Logging Policy cannot be modified or deleted. However, it can be duplicated to create new customizable policies.

Trustwave provides a predefined Device Logging Policy:

- **Device Logging Policy**: This Policy contains one rule designed to log all authentication attempts that failed.

3.3.2.2 Device Logging Policy Details

Clicking any Device Logging Policy displays the **Policy Details** on the right pane.

Device Logging Policy Details Screen Fields

Field	Description
Policy Name	Name of the specific policy.
Description	Contains a description of the policy.

3.3.2.3 Device Logging Rule Details

Clicking any Device Logging rule displays the Rule Details on the right pane.

Device Logging Rule Details Screen Fields

Field	Description
Rule Name	Defines the name of the logging rule.
Description	This provides a place for you to write a description of the rule. Trustwave provides pre-defined rule descriptions.

Device Logging Rule Details Screen Fields

Field	Description
Enable Rule	When selected, the rule is enabled. When cleared, the rule is disabled.
Send To:	
Archive	Sends log information in files to an external remote location. This must be selected to ensure that there is relevant information to archive.
Log	Sends information to the Trustwave log database, which can be seen via the Log View.
Report	Sends information to the Trustwave reports database. This must be selected prior to running Reports to ensure that there is relevant information to display results.
Syslog	Sends information to one or two UNIX Syslog facilities which log data.

3.3.2.4 Device Logging Policy Rule Conditions

Each rule may include multiple conditions, all of which must be met in order for the rule to be fired.

The following Conditions are available for selection within the Device Logging Policy rules:

- Authentication Cluster

- Authentication Domain

- Authentication Methods

- Authentication Protocols

- Authentication Status

- Header Fields

- IP Range

- Location

- Destination Port Range

- Pre Authenticated Headers

- URL Lists

> When defining the Device Logging Rule, the conditions selected must match those of the Identification Policy rule in order for the relevant transactions to appear in the Log View.

3.3.2.4.1 Authentication Cluster

This condition applies to the clusters as used in the parameters for **Authenticate** or **Get User Credentials** actions in Identification Rule Details.

3.3.2.4.2 Authentication Domain

This condition applies to the realm name against which authentication is performed, as used in the parameters for **Authenticate** or **Get User Credentials** actions in Identification Rule Details.

> Prior to using the Authentication Domain condition you must first define the Domains used at your site.

For more information, see Realm.

3.3.2.5 Authentication Methods

This condition details the four authentication methods defined in the **Action** field in Identification Rule Details. This condition can be used to include or exclude the authentication methods for logging purposes.

Device Logging Policy Rule Conditions – Authentication Method Options

Option	Description
Authenticate	Trustwave SWG communicates with the client to get USERID information and uses an external Authentication Site to validate this information.
Get user credentials	Trustwave SWG gets user identification via NTLM or another such method.
Identify by headers	Identifies the end-user according to the Header (HTTP).
Identify by source IP	Identifies the end-user by source IP.

3.3.2.5.1 Authentication Protocols

This condition logs the protocols used for authentication (Basic, NTLM or Negotiate).

3.3.2.5.2 Authentication Status

This condition logs the failed status of authentication attempts.

3.3.2.5.3 Header Fields

This logging rule condition covers the Header Fields as detailed in Header Fields.

3.3.2.5.4 IP Range

This logging rule condition covers the IP ranges as detailed in IP Range.

3.3.2.5.5 Location

This condition is used to distinguish a client application based on the location of the scanning server.

Device Logging Policy Rule Conditions – Location Options

Option	Description
Cloud	The scanning server is located in the Internet cloud.
Local	The scanning server is located in the enterprise.

3.3.2.5.6 Destination Port Range

This logging rule condition covers the Destination Port ranges as detailed in Destination Port Range.

3.3.2.5.7 Pre Authenticated Headers

This logging rule condition applies to the Pre Authenticated headers as used in the **Identify by headers** action in Identification Rule Details.

3.3.2.5.8 URL Lists

This logging rule condition covers the URL Lists as detailed in URL Lists.

3.3.3 Identification Policy

Identification Policies carry out the classification of an end-user to determine whether they should browse through the system. The Identification Policy also enables the system to enforce the proper Security Policy for the end-user. The Rules are based on both the type of Authentication or Identification that Trustwave SWG will use as well as using Conditions of Header Fields, IP Ranges, Port Ranges and URLs.

This section contains the following topics:

- Identification Policies Tree

- Identification Policy Details

- Identification Rule Details

- Identification Policy Rules Condition Details

3.3.3.1 Identification Policies Tree

The Identification Policies tree holds all the current Identification Policies within that definition, as well as the rules that make up these policies and the conditions that make up the rules.

This provides easy navigation through each Policy – displaying the components of that Policy at a glance.

Policies, rules, and conditions can be added, duplicated or deleted by right-clicking the relevant node. Trustwave's default Identification Policies cannot be modified or deleted. However, they can be duplicated to create new customizable policies.

Trustwave provides several predefined Identification Policies:

- **Authentication**: This Policy contains the Identify and Authenticate Users rule whose purpose is to authenticate end-users using an Authentication Device. The rule in this policy is disabled by default. To activate it, configure an Authentication Site via **Users | Realm**.

- **Default Cloud Scanners Read Headers Policy**: This policy contains the following rules:

  - Identify Branch Office Users by Headers rule whose purpose is to identify the users based on the HTTP headers that have been pre authenticated.

  - Always Identify Users by Headers whose purpose is to identify the end-users based on pre-defined Cloud Scanner HTTP headers.

- **Get User Credentials**: This policy contains the **Get User Credentials to Identify Users** rule whose purpose is to obtain USERID information using the NTLM protocol and the default cluster of Authentication Devices IF the end-user is NOT in the defined IP Range and Header Field lists.

- **Read Headers**: This policy contains the Always Identify Users by Headers rule whose purpose is to identify the users based on the HTTP headers that have been pre authenticated.

- **Source IP Only:** This Policy contains the Always Identify Users by Source IP rule whose purpose is to identify the user by Source IP. This is the default identification action.

3.3.3.2 Identification Policy Details

Clicking any Identification Policy displays the Policy Details screen in the right pane.

The Policy Details screen contains the following information with the option to make changes using the **Edit | Save/Cancel** options.

Identification Policy Details Screen Fields

Field	Description
Policy Name	Name of the specific policy.
Authenticated By	Device making the authentication.
Description	Contains a description of the policy.

3.3.3.3 Identification Rule Details

Clicking an Identification rule displays the Rule Details screen in the right pane.

The Identification Rule Details screen contains the following information with the option to make changes using the **Edit | Save/Cancel** options.

Identification Rule details Screen Fields

Field	Description
Rule Name	Defines the name of the Identification rule.
Description	Contains a description of the rule.
Enable Rule	When selected, the rule is enabled. When cleared, the rule is disabled.
Action	**Authenticate:** SWG communicates with the client to get USERID information and uses an external Authentication Site to validate this information. In order to do so, various parameters must be defined.
	Get User Credentials: SWG gets User Identification via NTLM or another method.
	Identify by Headers: Used when a downstream device (proxy) provides user information by forwarding device specific HTTP headers within the request.
	Identify by Source IP: Identifies the end-user by source IP. This is the default method of identification.
	Depending on the action taken the following options appear.
Authentication Protocols	Determines the type of protocol (Basic, NTLM or Negotiate).
Authentication Site	Depending on the selected **Action** this drop down list is displayed, which includes the customer Authentication Sites as defined in LDAP and/or Realm.
Pre-Authenticated Headers	Depending on the selected **Action** this drop down list is displayed, which includes all headers which have been pre authenticated as defined in Pre-Authenticated Headers.

3.3.3.4 Identification Policy Rules Condition Details

Click a Condition to display the Condition details in the right pane.

Identification Policy Rules Condition Details Screen Fields

Field	Description
Condition Name	This displays the condition name. When creating new conditions, choose the required condition from the drop down list. This selection determines which items are display in the check box list in the middle of the window.
Applies To	Indicate whether the checked items that follow indicate criteria to be "applied" or "exception" criteria (that is, apply any criteria except the checked items).
Select/Deselect All	To simplify selection of check boxes, you can check/clear this check box to select/clear all items in the check box list (and then adjust as needed).
The bottom pane displays different items according to the condition you have chosen.	

The following conditions are available for selection within the Identification rules:

- Destination Port Range

- Header Fields

- IP Range

- Location

- URL Lists

3.3.3.4.1 Destination Port Range

This condition is used to distinguish a client application connecting to Trustwave SWG by its target destination port.

The default rule enables the administrator to exclude a list of Port ranges. Destination Port Range can be edited via Destination Port Range.

3.3.3.4.2 Header Fields

This condition is used to distinguish a client application connecting to Trustwave SWG by the User Agent or any other HTTP header name and value.

The Header Fields list can be modified via Header Fields.

Identification Policy Rules Condition Details Screen – Header Field Options

Option	Description
Content-Disposition Executable	Defines malicious exes detected as spoofed executables.
Exclude by Headers	Provides a list for customers to add headers which identify applications (such as IM). In the default rule provided, these identification headers are excluded from identification.
Firefox 1.x, 2.x	Defines specific browser versions of Firefox.
Media Players	Defines Media Players header fields.
Netscape 7.x	Defines browser version of Netscape version 7.
Older and Unsafe Browsers	Defines a list of browsers based on older versions and those that are considered unsafe.
Partial Downloading	Refers to partial downloads of Internet content.
SSL	Defines SSL header fields. Pinpointing specific SSL headers enables the administrator to build specific rules regarding SSL content.
Trojans	Defines header fields suspected of being created by a Trojan Horse.

3.3.3.4.3 IP Range

This condition is used by the administrator to define IP address ranges that end-users may be using in order to effectively identify or authenticate them. In the default rule provided, these IP ranges are excluded from identification methods.

This list can be edited via IP Range.

3.3.3.4.4 Location

This condition is used to distinguish a client application connection by the location of the scanning server.

Identification Policy Rules Condition Details Screen – Location Options

Option	Description
Cloud	The scanning server is located in the Internet cloud.
Local	The scanning server is located in the enterprise.

3.3.3.4.5 URL Lists

This condition refers to predefined and configurable lists of URLs.

The administrator can create new lists to identify client connections to SWG by the URL they target. These lists can be viewed and modified via URL Lists.

3.3.4 Upstream Proxy Policy

The Upstream Proxy Policy screen enables administrators to configure upstream proxy settings for traffic scanned by the SWG system. To allow for more thorough configurations, multiple Upstream Proxy policies can be defined, although the default Upstream Proxy is (**Direct**). This enables direct access to the Internet in every situation. As such, the default component is not editable.

Upstream Proxy Policies are built as follows:

- Policies are compiled from rules

- Rules are based on Conditions

A Policy may be assigned to one user or user group that passes through a specific device.

> To ensure that needed options are available, rules and conditions must be configured prior to adding a policy. For more information, see Upstream Proxy.

The right-click menu or sidebar option in the Upstream Proxy Policies tree enables you to **Add a Policy**.

Once a new policy is created, you can add rules, or delete/duplicate policy.

Upstream Proxy Policy Screen Fields

Field Name	Description
Client IP Header	Header information for user identifiers supplied by an upstream proxy.
User Name Header	Specifies the User Name in the Header Field.
Protocol	
Protocol – IP Address – Port – Active	For each protocol – HTTP, HTTPS, FTP, click **Active** and add the required IP address. To use the same proxy for all protocols, select **Use for all protocols**.

3.3.5 ICAP Request and Response Modification Policies

ICAP Policy comprises ICAP Request Modification and ICAP Response Modification policies. These policies define the ICAP Service Groups from which SWG requests ICAP Services, and defines behavior in case of an error.

> You cannot edit the pre-supplied Request Modification and Response Modification policies (**Trustwave Default ICAP REQMOD Policy** and **Trustwave Default ICAP RESPMOD Policy**). However, you can duplicate the policy and edit the duplicate. You can also create an ICAP policy from scratch.

This section contains the following topics:

- ICAP Request Modification Policy Tree

- ICAP Response Modification Policy Tree

- ICAP REQMOD Policy Details

- ICAP RESPMOD Policy Details

- ICAP Policy Rule Details

- ICAP Rule Condition Details

3.3.5.1 ICAP Request Modification Policy Tree

The ICAP Request Modification Policy tree contains a single, pre-supplied ICAP Policy, **Trustwave Default ICAP REQMOD Policy**, as well as the single rule that the policy contains. This rule contains no conditions.

You cannot edit a pre-supplied policy, but you can duplicate it and edit the duplicate - and you can create an ICAP Policy from scratch.

> Before you can save a rule in an ICAP Policy, you must ensure that the ICAP Service Group that will be associated with the rule has already been created (you can use the group before it has been committed). For instructions, see ICAP Service Groups.

To duplicate an ICAP Policy, right-click the policy node and choose **Duplicate Policy**.

3.3.5.2 ICAP Response Modification Policy Tree

The ICAP Response Modification Policy tree contains a single, pre-supplied ICAP Policy, **Trustwave Default ICAP RESPMOD Policy**, as well as the single rule that the policy contains. This rule contains no conditions.

You cannot edit a pre-supplied policy, but you can duplicate it and edit the duplicate - and you can create an ICAP Policy from scratch.

> Before you can save a rule in an ICAP Policy, you must ensure that the ICAP Service Group that will be associated with the rule has already been created (you can use the group before it has been committed). For instructions, see ICAP Service Groups.

To duplicate an ICAP Policy, right-click the policy node and choose **Duplicate Policy**.

3.3.5.3 ICAP REQMOD Policy Details

Clicking the pre-supplied, or user-defined, ICAP Policy node displays the **Policy Details** in the right pane.

ICAP Policy Details Screen Fields

Field	Description
Policy Name	Name of the policy (mandatory).
Description	Description of the policy (optional).

3.3.5.4 ICAP RESPMOD Policy Details

Clicking the pre-supplied, or user-defined, ICAP Policy node displays the **Policy Details** in the right pane.

ICAP Policy Details Screen Fields

Field	Description
Policy Name	Name of the policy (mandatory).
Description	Description of the policy (optional).

3.3.5.5 ICAP Policy Rule Details

The ICAP Policy rule lets you define from which ICAP Service Group the ICAP Services can be requested, and how to proceed in case of an error response.

Clicking this rule node, or the node of a user-defined ICAP rule, displays the Rule Details screen in the right pane.

To edit a rule in a user-defined ICAP policy, click **Edit**. To save the changes, click **Save**. To commit the

changes, click ![icon] **Commit Changes** in the toolbar.

ICAP Policy Rule Details Screen Fields

Field	Description
Rule Name	Name of the ICAP rule (mandatory).
Description	Optional description of the rule.
Enable Rule	Select this check box to enable the rule. (When cleared, the rule is disabled.)
ICAP Service Group	ICAP Service Group from which the ICAP Services should be requested. For information regarding the definition of ICAP Service Groups, see ICAP Service Groups.

Field	Description
In Case of Error	What to do in case of error. Possible actions: • **Bypass ICAP service processing** — In case of TCP and ICAP failure, continue as usual. • **Discontinue client request** — In case of any ICAP conversation failure, fail the HTTP transaction.

3.3.5.6 ICAP Rule Condition Details

To add a condition to an ICAP rule, right-click the rule and choose **Add Condition**. The rule's Condition Details window is displayed in the right pane.

To edit an existing condition, select the condition. Then click **Edit** in the Condition Details window.

To save the changes, click **Save**. To commit the changes, click ⟱ **Commit Changes** in the toolbar.

ICAP Rule Condition Details Screen Fields

Field	Description
Condition Name	Choose the appropriate condition from the drop down list (mandatory).
Applies To	Choose whether the rule should apply to everything selected below or to apply this rule to everything EXCEPT for the items selected below.
Select/Deselect All	Choose to select/clear all the items in the condition.
The bottom pane displays different items according to the condition you have chosen.	

The following Conditions are available for selection within the ICAP Policy rules:

> The following links (except IP Range) point to descriptions under Condition Details for Security Policy Rules. The IP Range link points to a description in this section.

• Content Size

• HTTP Method

• Header Fields

• IP Range

• Protocol

• Time Frame

• URL Filtering (Trustwave)

- URL Lists

In addition, the following are available only for the Trustwave Default ICAP RESPMOD Policy:

- True Content Type

- File Extensions

3.3.5.7 IP Range

This condition is used by the administrator to define IP address ranges that end-users may be using in order to effectively identify or authenticate them. In the default rule provided, these IP ranges are excluded from identification methods.

This list can be edited via IP Range.

3.4 Condition Elements

Many Policy Rule Conditions have configurable values and can be tweaked to fine-tune the Policies to match your organization's needs.

This section contains the following:

- General Information

- The configurable Condition Elements listed in the following table. (The table provides links to the Condition Elements and identifies the policy types in whose rules the conditions can appear.)

Configurable Condition Elements

Condition Element	Added conditions appear in Condition checklists of the same Condition Type (Names), in rules for the following Policy Types
Active Content List	Security, Logging
Application Control	Security, Logging
Archives	
Binary Behavior	Security, Logging. **Note:** The condition is also called **Behavior Profile (Binary)** in certain locations.
Content Size	Security, Logging
Data Leakage Prevention	Security, Logging
Destination Port Range	Identification, Device Logging
File Extensions	Security, Logging, Caching
Header Fields	Security, Logging, Identification, Device Logging, Upstream Proxy
HTTPS Certificate Validation	HTTPS
ICAP Service Groups	ICAP Request Modification, ICAP Response Modification
IP Range	Identification, Device Logging, Upstream Proxy
Pre-Authenticated Headers	Device Logging
Time Frame	Security, Logging
Upstream Proxy	Device Logging. **Note:** The added Upstream Proxy value also appears in the rule **Action** selection list of the **Upstream Proxy** Policy.
URL Lists	Security, Logging, HTTPS, Caching, Identification, Device Logging, Upstream Proxy

3.4.1 General Information

SWG comes with a large number of predefined conditions, many of which are used in predefined rules. Most conditions consist of checklists where you select the items that should be used (or not used) as the conditions in determining if the rule should be applied. (Often, an item in a checklist is itself a checklist)

In many cases, you can add condition checklists (via **Policies | Condition Elements**). Once committed, these checklists become available for selection when their conditions are added to relevant policy rules.

Configurable Condition Elements identifies the Condition types for which you can add additional checklists, and the policies in which these conditions can be relevant. The **Condition Type** value in the table applies to both of the following:

- Menu selection for adding the new condition checklist (**Policies | Condition Elements | *Condition Type***)

- **Condition Name** value which, when selected in a rule's condition, will result in the added checklist being displayed in the condition's checklists.

This section contains the following topics:

- Options in the Condition Elements Tree

- Accessing Used In Data

3.4.1.1 Options in the Condition Elements Tree

Condition Elements Tree Actions

Action	Description
Add Component	Available from top level folder only. Enables you to create a new Condition Component.
Delete Component	Available from specific Component. Enables you to delete a Component.
Duplicate Component	Only available from Trustwave pre-defined profiles. Enables you to duplicate a Component and then select required options.

For each Condition Element, additional options provide for further functionality. Access these options either through the right-click menu or the sidebar.

Condition options are dependent upon the specific condition component.

They include:

Action	Description
✕ **Delete List**	Available from specific URL list Component. Deletes the list
Import to List	Available from specific Component.
	Enables importing many URL addresses into a list. For more information, see Searching all URL Lists for Specific URLs.
Export to File	Available from specific Component.
	Enables exporting the URL addresses within a list to a file which can then be edited, printed, imported, and so on.
Delete all Items	Available from specific Component. Deletes all the URL addresses in the list on the right screen.
Used In	Available for all Components. Enables the administrator to see in which policies and rules this particular condition was used. For more information, see Accessing Used In Data.

3.4.1.2 Accessing Used In Data

The **Used In** option enables the administrator to determine, for any condition item, in what rules and policies the condition is used.

To access the Used In data:

1. Navigate in the Management Console to **Policies | Condition Elements** – and select the specific condition component. For example: **Policies | Condition Elements | Data Leakage Prevention.**

2. Right-click the component or click the icon in the furthest left pane and select **Used In**.

   The **Used In** screen appears. Rules may contain numerous components and policies may contain various rules.

3. To view the policies in which this item is used and the rules accorded to the policy, click 📋 on a specific record and select either **Navigate to Policy page** or **Navigate to Rule page.**

   The selected screen will open for viewing.

4. To return to the Used In screen, navigate through **Policies | Condition Elements** to the specific Component.

3.4.2 Active Content List

The system identifies Java Applets, ActiveX and executable files when they enter the system, and then creates a signature for each file. These signatures are stored for caching purposes in the system. A list of these items, the **Auto-Generated** list, is generated automatically.

This list cannot be used in a rule but items from this list may be moved to the following two lists (or indeed any new list that you create by right-clicking the **Add List** menu option) in order to create exceptions as rule conditions:

- **Allowed** – you can move **trusted** items from the Auto-generated list to the Allowed list.

- **Blocked** – you can move **questionable** objects from the Auto-generated list to the Blocked list.

Click ✚ on any piece of active content to display further information.

Active Content List conditions are available for rules in the following Policy types: Security, Logging.

The following topics are relevant to the Active Content List.

- Accessing Used In Data.

- Adding a New Active Content List

- Moving Between Active Content Lists

- Auto-Generated List Settings

For information on options, see Options in the Condition Elements Tree.

3.4.2.1 Adding a New Active Content List

Creating a new Active Content List enables you to move items from other lists, including the Auto-Generated list, to a newly created one. The right pane window therefore, supplies only a Name field. After a new list has been added, refer to Moving Between Active Content Lists to populate it with items.

For example:

1. Right-click the top level Active Content List in the left tree pane or the ✚ icon to **Add List**.

2. Give the new list a name such as "Custom List". Click **OK**.

3.4.2.2 Moving Between Active Content Lists

Trustwave has provided an Allowed and Blocked list to which you can move Active Content items.

To move an entry from one Active Content list to another:

1. Select a component from the Active Content tree, for example, **Auto-generated list**.

2. Click **Edit** to enable changes.

3. Use the check box to select all the entries you want to move.

4. In the **To** drop down list, choose the list you want to move the entries to, for example, the **Blocked** list.

5. Click **Save** to apply changes. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

> Moving these objects into new lists or changing their status from Blocked or Allowed, will impact on your Security Policy – if these lists are selected in the Rule Conditions

3.4.2.3 Auto-Generated List Settings

Auto-Generated list is automatically generated with Java Applets, ActiveX and executable files that enter the system.

Active Content List Screen – Auto-generated List Setting Fields

Field	Description
List Name	Displays the list name: **Auto-generated**.
Find All	Enter a search term in this field.
Plus Icon	Expands entry to show more detail.
Search	Click **Go** after entering a search term in the **Find All** field to return a list matching your search term.
Clear	Clears the items found in the Search and restores the Auto-generated list.
Previous/Next	Enables you to move through the pages of entries in the List.
Check box	Check this if you want to select one or all entries to move to another list.
To	Select which list to move the selected entries to. Click **Save** to move the entries.
Delete after x days	Defines the number of days after which the active content in this list will be deleted.
Maximum number of entries	Defines the maximum number of profiles that will be left in the List after daily cleanup (midnight) – after which the list will fill up again.

3.4.3 Application Control

Business use of Web applications presents a number of security, compliance, and productivity challenges. Trustwave assists enterprises to mitigate these issues by providing granular control of common social media applications. SWG Application Control is supported for Facebook, LinkedIn, Google +, Twitter, and YouTube.

Administrators can define which specific activities to block for which groups of users, or even for which individual users.

A built-in set of Application Control Profiles is defined. The profile set can be easily adjusted to the organization's own definition.

For more information, see Application Control.

Application Control provides the following benefits:

- Visibility and control over applications

- Reduction in the risk of exposure of sensitive data

- Reduction in the vectors that can be utilized for attacks, and optimization of security scans by limiting allowed protocols and applications

- Optimization of bandwidth usage and improved productivity by limiting non-relevant application usage

3.4.4 Archives

An archive file is a file that contains other files. That is, it is a bundle of files packaged together. Groups of files that belong together are archived because it's easier to move one bundled file from one place to another than it is to transfer many individual files, one at a time.

In the Archives tabs, you can configure the number of files bundled together - the number of archives within archives and the size of the extracted file. Archives include: Zip Archive, GZip Archive, RAR Archive, CAB Archive, BZ2 Archive and TAR Archive.

Archives Engine Screen Fields

Field Name	Description	Defaults (bytes)	Allowed Values (bytes)
Archive Depth	Configures the maximum depth level of nested archives.	5	1- 64000
Maximum Entries in Container	Configures the maximum number of entries allowed per archive. If the number of entries exceeds this amount, the container will not be scanned or forwarded.	2000	1- 4500000000
Maximum Extracted Content Size	Determines the size of the maximum extracted content.	1073741820	1- 4000000000

3.4.5 Binary Behavior

The condition is called Behavior Profile (Binary) in certain locations.

Trustwave's binary behavior engine is based on checking security behaviors and profiles that are a subset of all available behaviors.

The behaviors are examined through the inspection of the binary's exposed mechanisms that define its required interfaces in the system, and which can be detected and filtered by the groups defined below. See Tabs in the Binary Profile Behavior Window.

By applying the organizational security policy and translating it into the behaviors defined in the binary behavior profile, adequate protection and implementation of the security policy can be achieved.

The behavior groups are created by Security experts from Trustwave, and fed into the Binary Behavior Profile, enabling the identification of malicious active content that violates the standard organizational security policy.

Binary Behavior conditions are available for rules in the following Policy types: Security, Logging.

3.4.5.1 Tabs in the Binary Profile Behavior Window

Trustwave provides a Default Binary Profile Behavior, which displays the following tabs:

- Automatic Execution and Termination Tab

- File Access Tab

- Registry Access Tab

- Network Access Tab

- Minor Risk Operations Tab

- Disclosure of Information Tab

- Java Runtime Tab

- Change Settings Tab

- System Settings Tab

- General Tab

- Other Running Applications Tab

For information on options, see Options in the Condition Elements Tree.

3.4.5.1.1 Automatic Execution and Termination Tab

The following Automatic Execution options are considered unsafe when performed by **ActiveX and Executables**.

Binary Profile Behavior Screen – Automatic Execution and Termination Tab Options

Automatic Execution	Description
Create Process	Potential misuse of function which is used to create system processes.
Dynamic Link Library Invocation Functions	Access to external DLL files in order to gain additional functionality by ActiveX.
Terminate Process	The binary file contains a reference to process termination operation.
Unresolved Library Access	An attempt to access a library of functions that cannot be resolved directly.

The following Automatic Execution options are considered unsafe when performed by **Java Applets**.

Binary Profile Behavior Screen – Automatic Execution and Termination Tab Unsafe Options

Automatic Execution	Description
Access Other Applications	Accessing applications outside the context of the applet is considered a security violation. Applets are usually self-contained and do not require access to other applications.
Create Process	Potential misuse of function, which is used to create system processes
Load Class	Potential misuse of function which is used to load/locate external Java program
Load Library	Potential misuse of function which is used to load library (external library which contains program codes)
Remote Method Invocation	An attempt to call a method on a remote object accessible over the network (internal or external)
System Commands	The binary file contains a reference to system commands (execute, schedule processes, and so on)
Terminate Process	The binary file contains a reference to process termination operation

3.4.5.1.2 File Access Tab

The following File Access options are considered unsafe when performed by **ActiveX and Executables**.

Binary Profile Behavior Screen – File Access Tab Options

File Access	Description
File Delete	Potential misuse of local privileged functions for file/directory removal
File Read	Potential misuse of local privileged functions for file read, data read
File Write	Potential misuse of local privileged functions which write data to a file (audio, text or binary types)

The following File Access options are considered unsafe when performed by **Java Applets**:

Binary Profile Behavior Screen – File Access Tab Unsafe Options

File Access	Description
File Create	Potential misuse of local privileged functions as File Create/File Copy.
File Write	Potential misuse of local privileged functions which write data to a file (audio, text or binary types).
File Delete	Potential misuse of local privileged functions for file/directory remove.
File Read	Potential misuse of local privileged functions for file read, data read.
File Query	Potential misuse of local privileged functions for file read, open file, querying files parameters, and so on.
File Rename	Potential misuse of local privileged functions for file rename.

3.4.5.1.3 Registry Access Tab

The following Registry Access options are considered unsafe when performed both by **Java Applets** and **ActiveX and Executables**:

Binary Profile Behavior Screen – Registry Access Tab Options

Registry Access	Description
Registry Delete	Potential misuse of local privileged functions for deleting registry key/value
Registry Read	Potential misuse of local privileged functions for reading registry key/value
Registry Write	Potential misuse of local privileged functions for writing/changing registry key/value

3.4.5.1.4 Network Access Tab

The following Network Access options are considered unsafe when performed by **ActiveX and Executables**:

Binary Profile Behavior Screen – Network Access Tab Options

Network Access	Description
Bluetooth Networking	Potential misuse of local privileged functions such as sending an authentication request to a remote Bluetooth device or retrieving information on a remote Bluetooth device
DNS Functions	Potential misuse of local privileged functions that use DNS Client API, such as DNS query, record compare, and so on.
Network Connect	Potential misuse of local privileged functions in order to connect to other network elements such as functions that use HTTP client API to send requests through HTTP protocol to other HTTP servers, and so on.
Network Listen	Potential misuse of local privileged functions calls in order to access network services (e.g. listen for incoming connection)
Network Receive	Potential Misuse of local privileged functions calls in order to access network services (e.g. retrieving content/data from other resources such as retrieving file from FTP server)
Network Send	Potential misuse of local privileged functions calls in order to access network services (e.g. send network commands)

The following Network Access options are considered unsafe when performed by **Java Applets**.

Binary Profile Behavior Screen – Network Access Tab Unsafe Options

Network Access	Description
Network Receive	Suspected network behavior such as open socket, receiving data packets.
Network Resolve	Suspected network behavior such as communicating with DNS server, getting host information, and so on.
Network Send	Suspected network behavior such as open socket, sending data packets.
Open Socket	Suspected network behavior such as open socket for communication (for data packet transfer).

3.4.5.1.5 Minor Risk Operations Tab

The following Network Access options are considered unsafe when performed by **ActiveX and Executables**:

Binary Profile Behavior Screen – Minor Risk Tab Options

Minor Risk Operations	Description
Potentially Dangerous Memory Management Functions	Changes the way that an application uses the system memory may result in a crash or the disclosure of sensitive data.
Potentially Dangerous Process-Debugging Functions	Process debugging functions may be used to reveal information from the system and alter the execution logic of the debugged applications.

The following Minor Risk Operations options are considered unsafe when performed by **Java Applets**:

Binary Profile Behavior Screen – Minor Risk Tab Unsafe Options

Minor Risk Operations	Description
CORBA Connection	An attempt to create or manage a CORBA connection (Common Object Request Broker Architecture). This may utilize functionality that is provided remotely by an external object.
Memory Write	An attempt to write data to a mapped memory segment.
Database Access	Functionality related to database access activity.
Print Access	Indicated access to printing functionality within the application.
Exit Browser	Terminates the browser session.
Use Reflection	Provides functionality to query existing applications and objects by examining them and gathering functionality information.

3.4.5.1.6 Disclosure of Information Tab

The following Disclosure of Information options are considered unsafe when performed by **Java Applets**:

Binary Profile Behavior Screen – Disclosure of Information Tab Unsafe Options

Disclosure of Information	Description
Access Clipboard	Potential misuse of local privileged functions such as reading computer clipboard and revealing sensitive information.
Access Cookies	Potential misuse of local privileged functions such as reading Internet cookies which might allow a remote user to access bank accounts/Web-based email, and so on.
Enumerate Printer Connections	Potential misuse of local privileged functions such as mapping or removing printer connections.

Binary Profile Behavior Screen – Disclosure of Information Tab Unsafe Options

Disclosure of Information	Description
Get User Information	Potential misuse of local privileged functions such as getting specific user information (user name, system name, and so on).
Keystrokes	Potential misuse of local privileged functions such as logging of keystrokes which might reveal user's password.

3.4.5.1.7 Java Runtime Tab

The following Java Runtime options are considered unsafe when performed by **Java Applets** since by doing so an attacker may eliminate security restrictions:

Binary Profile Behavior Screen – Java Runtime Tab Unsafe Options

Java Runtime	Description
Set Class Loader	Potential misuse of function in order to locate, run Java program.
Set Properties	Potential misuse of function which might change the current working environment.
Set Security Manager	Potential misuse of function in order to set system's security.

3.4.5.1.8 Change Settings Tab

The following Change Settings options are considered unsafe when performed by **ActiveX and Executables**:

Binary Profile Behavior Screen – Change Settings Tab Unsafe Options

Change Settings	Description
Change Network Systems	Potential misuse of local privileged functions calls in order to change network settings (e.g. using HTTP server API functions).
Change System Settings	Potential misuse of local privileged functions in order to change system settings (e.g. shell commands, network programming).

3.4.5.1.9 System Settings Tab

The following System Settings options are considered unsafe when performed by **Java Applets**:

Binary Profile Behavior Screen – System Settings Tab Unsafe Options

System Settings	Description
Change Printer Connections	Attempt to change printer connections which may lead to disclosure of data

3.4.5.1.10 General Tab

The following General options are considered unsafe when performed by **ActiveX and Executables**:

Binary Profile Behavior Screen – General Tab Unsafe Options

Database Access	Description
Database Access	Potential misuse of local privileged functions which allow access to a database.
Exit Windows	Potential misuse of local privileged functions which perform system shutdown, lock work stations, and so on.

3.4.5.1.11 Other Running Applications Tab

The following Other Running Applications options are considered unsafe when performed by **ActiveX and Executables**:

Binary Profile Behavior Screen – Other Running Applications Tab Unsafe Options

Other Running Applications	Description
Code Injection into Running Process	Potential misuse of local privileged functions which allow, for example, the creation of a thread that runs in the virtual address space of another process.
Sending Messages to other Applications	Potential misuse of local privileged functions which allow the sending of messages to a specific system process/procedure on a local machine, and so on.

The **Higher Sensitivity Binary Behavior Profile** contains the same Profile information. However, in this screen all the options are checked.

3.4.6 Content Size

Content size refers to the size (in KB) of the content being scanned. These content size values can be selected as a Condition to be included in your Policy Rules thereby limiting very large files from entering or leaving your organization. The predefined content sizes cannot be modified. However, new Content Size lists can be created.

> For containers, the content size refers to the size of the files once taken out of the containers – so while the actual container might be smaller than the size you defined, it could still be blocked.

Content Size conditions are available for rules in the following Policy types: Security, Logging.

The following topic is relevant to Content Size.

- Generating Content Size

For information on options, see Options in the Condition Elements Tree.

3.4.6.1 Generating Content Size

To generate Content Size:

1. Right-click the top-level heading **Content Size** and select **Add Component**.

2. Enter an appropriate Content Size name.

3. Enter the required Content Size (in KB).

4. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

5. If you need to modify this component in the future, select **Edit** and make your changes.

3.4.7 Data Leakage Prevention

Data Leakage Prevention (DLP) is a content processor through which Secure Web Gateway scans information stored within varying types of documents (such as customer records, financial information, and intellectual property), and prevents it from leaving the company network should it violate specific company compliance.

The main purpose of DLP is to protect such information, but DLP capabilities can also assist companies in demonstrating regulatory compliance (such as HIPAA, and CISP).

To handle DLP, SWG can scan HTTP, HTTPS and the FTP protocols for textual parts of documents. The document is split into multiple parts such as: Document body, Document metadata (like Microsoft Word document properties such as Author), Comments, and Headers/Footers.

SWG also uses the TextCensor engine, which dynamically classifies web pages and files based on their content. The engine is used to enhance the DLP capabilities of the system, and as a complementary solution to the URL filtering engine.

> Trustwave provides Data Leakage prevention and monitoring capabilities for Web protocols only. Email or other protocols will not be handled unless specifically mentioned.
>
> Under FTP, only incoming content is scanned.

Supported file types include:

*   Microsoft Office

    *   MS Word 2003 and 2007 (binary), 2007 (XML)

    *   MS Excel 2003 (binary) and 2007 (XML)

    *   RTF

*   Adobe PDF

Data Leakage Prevention is provided via several Default SWG Scripts. These scripts incorporate multi-language built conditions used in DLP rules, in X-ray mode, within policies. Each script includes a cumulative Trigger Threshold which defines how often one or more of the specified terms can occur before a Block action is triggered.

The default scripts cannot be edited. You can, however, create and define additional scripts, using the DLP script builder. The script builder lets you create a textual representation of the type of information that is not allowed to leave the organization's network.

To define the details of a Data Leakage Prevention (DLP) script, see Creating/Editing a Data Leakage Prevention Script.

Data Leakage Prevention scripts are available for rules in the following Policy types: Security, Logging.

3.4.7.1 Default SWG Scripts

SWG provides several default DLP scripts, pre-set to identify potentially harmful data. Secure Web Gateway provides a default list of words, combinations of words, terms, and numbers, for which to scan.

- **CVs and Resumes:** Scans for work-search related information identified by specific terms such as "curriculum vitae" and "work experience".

- **Confidential Data Leakage:** Scans for confidential data identified by specific terms such as "internal use only" and "confidential".

- **Multiple Credit Card Numbers:** Scans for credit card-related information identified by specific terms such as "CCard".

- **Sensitive Data:** Scans for confidential credit card and US social security data identified by specific terms such as "CCard" and "US-SSN"

To define the details of a Data Leakage Prevention (DLP) script, see Creating/Editing a Data Leakage Prevention Script.

3.4.7.2 Creating/Editing a Data Leakage Prevention Script

To create or edit a Data Leakage Prevention script:

1. Navigate to **Policies | Condition Elements | Data Leakage Prevention**.

2. Do either of the following:

   - To create a new script: Right-click the **Data Leakage Prevention** node and select **Add Script**. Then enter the **Script Name** and **Trigger Threshold**.

   - To edit an existing script, select the node in the tree and click **Edit**. If required, change the **Script Name** and **Trigger Threshold**.

3. Define the details of the Script. For instructions, see Defining Script Expression Details.

4. When the script definition is complete, click **Save**.

5. To commit the changes, click **Commit Changes** in the toolbar.

The new condition can be associated with any appropriate rule.

3.4.7.3 Defining Script Expression Details

The Script Expression Editor provides a large field where you can manually enter the desired text. It also provides icons for adding symbols (such as wildcards), operators (such as And/Or), and parentheses, at the current cursor location.

In the expression definition window, do the following:

1. Navigate to **Policies | Condition Elements | Data Leakage Prevention**.

2. Right-click the script in the tree and select **Add Expression**.

3. Click **Edit**.

4. Enter a descriptive **Name** for the expression.

5. Enter an **Expression Score** for this expression. Scores are accumulated for each expression matched within the relevant script and will trigger the policy rule when they reach the **Trigger Threshold** for the script. See Creating/Editing a Data Leakage Prevention Script.

6. Define how the Expression Score is accumulated by selecting the relevant radio button.

   - Add the score every time the expression matches: For this option there is no maximum to the number of times the score is added

   - Add the score for the first *n* matches only: For this option there is a defined limit to the number of times the score is added

7. Define the expression syntax in the large field by typing in or pasting text, and using the options provided. A large cross or checkmark indicates whether the condition syntax is acceptable.

   - Operators: Icons are provided for adding the Operators **AND**, **OR**, **NOT**, and **( )**

   - Functions:

     • **Followed By** and **Preceded By** - Where an expression is followed or preceded by 4 or fewer instances of another expression. The default value of 4 is configurable.

     • **Instances** - Where the number of occurrences is fewer or equal to a defined number

     • **Near** - Where a defined instance is located a set distance from another defined instance

     • **Case Sensitive** - Where the instance must match the case of the defined word(s)

   - Wildcards:

     • **Letter** and **Digit** - Any single letter or digit

     • Number - Any number made up of one or more digits

     • - Zero or more letters or digit characters

     • - Any single letter or digit

- Specials:

  - **CCARD** - Any series of digits that look like credit card numbers

  - **US-SSN** - Any series of digits that look like US Social Security numbers

> When copying text from another source, remove all formatting by pasting the text into Notepad or a similar plain text application first, and then re-copy it from the text application to the SWG screen.

8. When the script definition is complete, click **Save**.

3.4.8 Destination Port Range

You can use Destination Port Range to define (specify and label) one or more port ranges for use in Identification Policy rules.

The rules will apply to client applications whose target destination ports are in the range.

> Persistent connections enable the client to connect to various targets via the same proxy connection. This means that the first request may target a different server port than the following requests.

After you commit the Destination Port Ranges that you have defined, they will be listed in any **Destination Port Range** conditions that appear in an Identification Policy rules. You can then select them for allowing or blocking.

Destination Port Range conditions are available for rules in the following Policy types: Identification, Device Logging.

The following topic is relevant to Destination Port Range.

- Defining Destination Port Ranges

For information on options, see Options in the Condition Elements Tree.

3.4.8.1 Defining Destination Port Ranges

To define a Destination Port Range:

1. Right-click the top-level heading **Destination Port Range** and select **Add Component**.

2. Enter an appropriate **Destination Port Range** name.

3. In the Destination Port Range section, click ✚ to add a new row.

4. Enter a Port number in the **From/To** range (for example, 443 to 450).

5. Repeat as many times as necessary. You can delete entries by clicking 📒 on the same row as the entry and selecting **Delete Port Range**.

6. Click **Save** to apply changes. To commit the changes, click 🗸 **Commit Changes** in the toolbar.

7. If you need to modify this range in the future, select **Edit** and make your changes.

3.4.9 File Extensions

Each node in the File Extension tree identifies a predefined list of file extensions, organized by topic for convenience and ease of use. They can be used as rule conditions in your security policy. Each node is actually a list of other file extensions, organized by topic. They are presented as predefined lists for convenience, and they can be used as rule conditions in your security policy.

Also included in the tree is the Multiple File Extensions list. This refers to files that have more than one extension, and the last extension allows the Operating System to run the file (for example, **file.txt.exe**).

With the exception of the Multiple File Extensions list, which can be edited, you cannot add or delete extensions from the existing File Extensions provided by Trustwave. You can, however, create new File Extension lists.

File Extension conditions are available for rules in the following Policy types: Security, Logging, Caching. The following topics are relevant to File Extensions.

*   Creating a File Extension List

*   Editing the Multiple File Extensions List

For information on options, see Options in the Condition Elements Tree.

3.4.9.1 Creating a File Extension List

To create a new File Extension List:

1. Right-click the top-level heading and select **Add Component**.

2. Enter an appropriate **File Extension** name.

3. In the File Extensions section, click ![plus icon] to add a new row.

4. Enter the relevant File Extension.

5. Repeat as many times as necessary. You can delete entries by clicking ![icon] on the same row as the entry and selecting **Delete Extension**.

6. Click **Save** to apply changes. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

7. If you need to modify this list in the future, select **Edit** and make your changes.

3.4.9.2 Editing the Multiple File Extensions List

To edit the Multiple File Extensions List:

1. Select the **Multiple File Extension List** in the tree.

2. In the main window, click **Edit**.

3. To add a File Extension, click ![plus], and in the new row enter the File Extension.

4. To delete an entry, click ![icon] on the same row as the entry and select **Delete Extension**.

5. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

3.4.10 Header Fields

Headers are metadata allowing the customer to customize rules based on these header fields. For example, you can create a rule that blocks requests from specific user-agents. The headers can be either request or response headers.

The Header Fields tree comes with a number of predefined Header Fields provided by Trustwave. With the exception of **Exclude By Headers**, which can be edited, you cannot add or delete any of them.

You can, however, add and define new Header Fields.

Header Fields conditions are available for rules in the following Policy types: Security, Logging, Identification, Device Logging, Upstream Proxy.

The following topic is relevant to Header Fields.

- Defining Header Fields

For information on options, see Options in the Condition Elements Tree.

3.4.10.1 Defining Header Fields

To define a Header Field:

1. Do either of the following:

   - To edit **Exclude by Headers**: Select the **Exclude by Headers** node in the Header Field tree. Then, in the main window, click **Edit**.

   - To add a new Header Field item: Right-click the root (**Header Fields**) node, and choose **Add Component**. Then enter an appropriate **Header Field** name.

2. In the Header Fields section, click ![plus] to add a new row.

3. Enter a Header Name, Condition, and Header Value as required.

   ![info icon] The Header Field value uses various parameters for Regular Expression or Equals to. For example, ".*?Trustwave" searches for the shortest string before the word Trustwave.

4. Repeat as many times as necessary. You can delete entries by clicking ![icon] on the same row as the entry and selecting **Delete Header**.

5. Click **Save** to apply changes. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

6. If you need to modify this component in the future, click **Edit** and make your changes.

3.4.11 HTTPS Certificate Validation

Certificate validation includes certificate integrity checks, expiration checks, revocation and matching. Secure Web Gateway ensures that corporate policies regarding certificates are enforced, while removing the decision from the user's hands by automatically validating each certificate and making sure that the chain goes back to the trusted authority. Policies regarding certificates are enforced by checking individual certificate names, date, trusted authority chain and revocation lists.

A list of trusted certificate authorities is supplied with the system and used for digital signature analysis and for HTTPS certificate validation. Digital certificate lists are updated via Trustwave security updates. These lists include the required trusted certificate authorities as well as the Certificate Revocation Lists.

Trustwave includes one predefined **Default Certificate Validation Profile**. Administrators cannot modify or delete this default profile. However, using the HTTPS Certificate Validation right-click menu or sidebar options, they can duplicate or add HTTPS Certificate Validation Profiles which can then be customized.

HTTPS Certificate Validation conditions are available for rules in the following Policy types: HTTPS.

To create an HTTPS Certificate Validation Profile:

1. Right-click the **Profiles** node in the HTTPS Certification Validation tree, and then select **Add Component**.

2. Enter a name for the profile.

3. In the displayed definition tree, select the relevant items in each tab. The following are links to tab descriptions.

   - Invalid Certificate Structure

   - Certificate Cannot be Trusted

   - Certificate is Not Currently Valid

   - Certificate Revoked

   - Host Cannot be Trusted

   - Bad Certificate Usage

4. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

5. If you need to modify this component in the future, click **Edit** and make your changes.

HTTPS Certificate Validation profiles contain the following tabs for defining certificate error events.

For information on options, see Options in the Condition Elements Tree.

3.4.11.1 Invalid Certificate Structure

HTTPS Certificate Validation Screen – Invalid Certificate Structure Tab Options

Invalid Certificate Structure	Description
Cannot decode issuer public key	The certificate signature could not be decrypted (meaningful for RSA keys).
Certificate signature cannot be decrypted	The public key in the certificate SubjectPublicKeyInfo could not be read.

3.4.11.2 Certificate Cannot be Trusted

HTTPS Certificate Validation Screen – Certificate Cannot be Trusted Tab Options

Certificate Cannot be Trusted	Description
Authority and issuer serial number mismatch	Authority and issuer serial number mismatch. The current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate.
Authority and subject key identifier mismatch	The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate.
Certificate chain too long	The certificate chain length is greater than the supplied maximum depth.
Certificate is self signed	The certificate is self signed and the same certificate cannot be found in the list of trusted certificates.
Certificate not trusted	The root CA is not marked as trusted for the specified purpose.
Certificate rejected	The root CA is marked to reject the specified purpose.
Certificate signature failure	The signature of the certificate is invalid.
Invalid CA certificate	Either the CA is not valid or it may not be used to sign the tested certificate for HTTPS communication.
Issuer certificate could not be found	This occurs if the issuer certificate of an untrusted certificate cannot be found.
Key usage does not include certificate signing	The current candidate issuer certificate was rejected because it may not sign other certificates (keyUsage).

HTTPS Certificate Validation Screen – Certificate Cannot be Trusted Tab Options

Certificate Cannot be Trusted	Description
Root certificate could not be found locally	The certificate chain could be built up using the untrusted certificates but the root could not be found locally.
Subject issuer mismatch	The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate.
Unable to get local issuer certificate	The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.
Unable to verify the first certificate	Unable to verify the first certificate – signatures could not be verified because the chain contains only one certificate and it is not self signed.

3.4.11.3 Certificate is Not Currently Valid

The following table describes the options:

HTTPS Certificate Validation Screen – Certificate is not Currently Valid Tab Options

Certificate is Not Currently Valid	Description
Certificate is not yet valid	The notBefore date is after the current time.
Certificate has expired	The notAfter date is before the current time.
Format error in certificate notAfter field	The certificate notAfter field contains an invalid time.
Format error in certificate notBefore field	The certificate notBefore field contains an invalid time.

3.4.11.4 Certificate Revoked

The following table describes the options:

HTTPS Certificate Validation Screen – Certificate Revoked Tab Options

Certificate Revoked	Description
Certificate revoked	The certificate has been revoked.
CRL has expired	Certificate has expired. The notAfter date is before the current time.

HTTPS Certificate Validation Screen – Certificate Revoked Tab Options

Certificate Revoked	Description
CRL is not yet valid	Certificate is not yet valid. The notBefore date is after the current time.
CRL signature failure	The signature of the certificate is invalid.
Format error in CRL lastUpdate field	The CRL lastUpdate field contains an invalid time.
Format error in CRL nextUpdate field	The CRL nextUpdate field contains an invalid time.
Unable to decrypt CRL signature	The actual signature value could not be determined (rather than it not matching the expected value).
Unable to get certificate CRL	The CRL of a certificate could not be found.

3.4.11.5 Host Cannot be Trusted

The following table describes the options:

HTTPS Certificate Validation Screen – Host Cannot be Trusted Tab Options

Host Cannot be Trusted	Description
Cannot verify hostname	The host name is unavailable and therefore cannot be verified against the certificate.
Host name does not match certificate name	The host name mismatches the one mentioned in the certificate.

3.4.11.6 Bad Certificate Usage

HTTPS Certificate Validation Screen – Bad Certificate Usage Tab Options

Bad Certificate Usage	Description
Unsupported certificate purpose	The supplied certificate cannot be used for the specified purpose.
Path length constraint exceeded	The basicConstraints pathlength parameter has been exceeded.

3.4.12 ICAP Service Groups

To enable SWG to act as an ICAP Client, you must configure the ICAP Services that it can receive. These services, however, must be clustered into ICAP Service Groups. Therefore, before configuring an ICAP Service, you must define the group to which it will belong.

For SWG to act as an ICAP Client (and receive ICAP Services), you must also configure:

- ICAP Client Module (via **Administration | System Settings | SWG Devices**), and

- ICAP Request and Response Modification Policies (via **Policies | Device Policies**). However, before you can configure an ICAP Policy, you must configure the ICAP Service Group that will be associated with the policy.

This section contains the following topics:

- Basic ICAP Service Group/Service Operations

- Fields in the ICAP Service Group Window

- Used-In Window

- ICAP Service Window

3.4.12.1 Basic ICAP Service Group/Service Operations

- To add an ICAP Service Group, right-click the **ICAP Service Groups** (root) node, and choose **Add Group**. The main window for defining the group is displayed. For a description of the fields in the window, see Fields in the ICAP Service Group Window.

- To edit an existing group, select the group node, and in the main window click **Edit**.

After creating/editing a group, click **Save**. To commit the changes, click ⬇ **Commit Changes** in the toolbar.

You do NOT have to commit the ICAP Service Group before using it in an ICAP policy rule.

- To delete an ICAP Service Group, right-click the group and choose **Delete Group**.

- To display the list of ICAP Policy rules in which a group is used, right-click the group and choose **Used In**. For more information, see Used-In Window.

- To add an ICAP Service to an ICAP Service Group, right-click the group node and choose **Add Service**. The Service Definition window is displayed. For information on defining the service in the window, see ICAP Service Window.

- To edit an ICAP Service, select the ICAP Service node, and in the main window click **Edit**.

After creating/editing an ICAP Service, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

- To delete an ICAP Service, right-click the Service and choose **Delete Service**.

3.4.12.2 Fields in the ICAP Service Group Window

The ICAP Service Group window contains the following tabs:

- General Tab

- Advanced Tab

3.4.12.2.1 General Tab

The **General** tab of the ICAP Service Group is used to define basic parameters of the group.

ICAP Service Group Screen – General Tab Fields

Field	Description
Name	Specify a name for the ICAP Services Group (mandatory).
Method	Mode in which the ICAP protocol works:
	• **REQMOD** — Request mode. This mode processes the Client request to a distant server while it is being sent to the Internet (that is, before it reaches the Internet). An example of a service in this mode is a DLP (Data Leakage Prevention) scan.
	• **RESPMOD** — Response mode. This mode processes the response from a distant server before it reaches the Client. An example of a service in this mode is an Anti-Virus scan.
Load Balancing Algorithm	Type of algorithm that should be used for distributing the load. Currently, only one algorithm is supported.
	• **Round Robin** — Distributes the load between servers sequentially in a circular pattern.
Health Check URL	URL to which the SWG scanner sends health check requests through the ICAP Service to ensure that the ICAP Service server is alive (up and running). **Note**: These requests are sent at the interval defined in the **Keepalive Services** tab in the ICAP Client module.

ICAP Service Group Screen – General Tab Fields

Field	Description
Expected Return Code	Return code expected from the Health Check URL. If this return code is received, it indicates that the ICAP Service is alive.

3.4.12.2.2 Advanced Tab

The **Advanced** tab of the ICAP Service Group is used to define timeouts.

ICAP Service Group Screen – Advanced Tab Fields

Field	Description
Connection Timeout	Maximum number of seconds to wait for a health check connection to be established. Default: 60.
I/O Timeout	Maximum number of seconds to wait for completion of a health check transmission. Default: 30.

3.4.12.3 Used-In Window

The Used-In window displays the list of ICAP policy rules in which an ICAP Service Group is used (that is, the rules where the check box for the ICAP Service Group is selected).

To display the Used-In window for a User List, right-click the list in the tree and choose **Used In**.

From the Used-In window, you can navigate the policy or rule definition page of a rule that uses the ICAP Service Group, by clicking the for the detail line and choosing the appropriate option.

After viewing the rules in which the group is used, perform any other action to close the Used In display (for example, select the ICAP Service Group node to re-display the group details).

The fields in the Used-In window are not editable.

Used-In Screen Fields and Buttons

Field/Button	Description
Name	Name of the ICAP Service Group. This name appears in the title bar of the window.
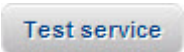
Used-In Screen Fields and Buttons

Field/Button	Description
Used In table	List of Policies/Rules in which the list is used. The table includes the following elements:
(icon)	To navigate to the definition of the policy or rule listed in the detail line, click this icon and choose **Navigate to Policy Page** or **Navigate to Rule Page**. This will take you to the Policy or Rule definition screen.
Policy Name	Policy that contains the rule that uses the ICAP Service Group.
Rule Name	Rule that uses the ICAP Service Group.

3.4.12.4 ICAP Service Window

To add ICAP Service to an ICAP Service Group, right-click the group and choose **Add Service**. The ICAP Service definition window is displayed.

ICAP Service Window Screen Fields and Buttons

Fields/Buttons	Description
Name	Name of the service. Mandatory.
Enable ICAP Service check box	Select this check box to enable use of this external ICAP Service.
URL	URL of the ICAP Service and Server, in the following segments:
icap:// first entry field	Address of the server hosting the ICAP service.
: second entry field	Port on which the ICAP Service is listening.
/third entry field	URL of the ICAP Service on the hosting server.
Scanner area	Lets you identify the scanner through which Discovery should be performed, and initiate Discovery. This area also contains the fields where the discovery results are displayed. For more information, see Performing Discovery.
Scanner	In the device-IP drop down, select the device IP of the SWG Scanner through which Discovery will be performed.
Max Connections	Maximum number of simultaneous connections to the Service.
Support Preview check box	Indicates if the ICAP Service supports Preview.
Preview Window	Size (in bytes) of the request Preview portion. Default: 4096
Test service	Click this button to perform Discovery of the ICAP Service's Connection Options through the selected Scanner.

Performing Discovery

SWG uses Discovery to discover the Connection Options (*maximum connections*, *preview support*, and *preview size*) of an ICAP Service. These Connection Options impact the connection of the ICAP Client to the ICAP Service.

The Policy Server, however, does not connect directly to the ICAP Service (unless the Policy Server is an All-in-One machine). Instead, the Policy Server goes through the Scanning Server for detection (Discovery) purposes. Since ICAP services and SWG scanners might not all reside in the same subnet, the Policy Server cannot know which Scanning server to choose.

To eliminate such problems, SWG lets the user choose the proper Scanning Server and perform Discovery through that server.

The user does this in the ICAP Service definition window. The Scanning area of this window contains a field for selecting the Scanning Server device IP, a button for initiating discovery, and fields for holding the values returned by the discovery.

The values returned by discovery replace the current values, and if the returned values are different than the ones they replace, the field is marked with a green asterisk.

You can return the defaults by pressing the **Cancel** button, and you can override the returned values with your own.

> The ICAP client and ICAP Discovery can even work through a scanner that is /not/ enabled as an ICAP client. This means that you can perform discovery through a scanner before defining the Scanner's ICAP Client module, and use the results to determine if you want the scanner to be an ICAP client.

3.4.13 IP Range

You can use **IP Range** to define (specify and label) one or more IP ranges for use in Identification Policy rules.

The rules will apply to end-users whose IP are in the range.

After you commit the IP Ranges that you have defined, they will be listed in any **IP Range** conditions that appear in an Identification Policy rules. You can then select them for allowing or blocking.

SWG comes with the following pre-supplied IP Range definitions: **Exclude by IP** and **Branch Offices IPs**. The Administrator can edit their details (though not their names), and add/modify their own IP ranges as required.

IP Range conditions are available for rules in the following Policy types: Identification, Device Logging, Upstream Proxy.

* For more information, see Defining IP Ranges.

* For information on options, see Options in the Condition Elements Tree.

3.4.13.1 Defining IP Ranges

To define an IP Range:

1. Do either of the following:

    - To edit **Exclude by IP** or **Branch Offices IPs**: Select the node in the IP Range tree. Then, in the main window, click **Edit**.

    - To add a new IP Range component: Right-click the root (**IP Range**) node, and choose **Add Component**. Then enter an appropriate **IP Range** name.

2. In the IP Range section, click ⊕ to add a new row.

3. Fill in the **From** and **To** values.

4. Repeat as many times as necessary. You can delete entries by clicking 📋 on the same row as the item and selecting **Delete IP Range**.

5. Click **Save** to apply changes. To commit the changes, click 🗸 **Commit Changes** in the toolbar.

6. If you need to modify this range in the future, select **Edit** and make your changes.

3.4.14 Pre-Authenticated Headers

Pre Authenticated Headers include headers whose header data has been previously authenticated by a downstream proxy agent. These are available for inclusion in the Identification Policy Rules.

Pre Authenticated Header conditions are available for rules in the following Policy types: Device Logging.

- For more information, see Generating a Pre Authenticated Header.

- For information on options, see Options in the Condition Elements Tree.

3.4.14.1 Generating a Pre Authenticated Header

To generate a Pre Authenticated Header:

1. Right-click the **Pre Authenticated Header** (root) node and select **Add Component**.

2. Enter an appropriate **Pre Authenticated Header** name.

3. Fill in the following Forwarded User Credentials:

Pre-Authenticated Header Forward User Credentials Fields

Field Name	Description
Pre-Authenticated Header IP Address	Enter an IP address; for example **X-Client-IP**.
Pre-Authenticated Domain/User	Choose one of the following Domain/User types:

Pre-Authenticated Header Forward User Credentials Fields

Field Name	Description
Basic …	If the **Basic Authenticated header from downstream proxy** radio button is selected, the proxy will use the basic authentication header per transaction and not per connection.
Custom	Custom header; for example, **X-Authenticated-User**.

4. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

5. If you need to modify this component in the future, select **Edit** and make your changes.

3.4.15 Time Frame

The predefined time frames provided with the system can be modified to suit local times and customs. New Time Frames can also be added. This condition enables the administrator to modify organizational demands and needs according to varying times of the week, thereby increasing system efficiency and productivity.

Time Frames are available for inclusion in Security and HTTPS Policy Rules.

Using the Time Frame right-click menu or sidebar options, you can add and delete Time Frames.

Time Frame conditions are available for rules in the following Policy types: Security, Logging.

For more information, see Adding a New Time Frame.

For information on options, see Options in the Condition Elements Tree.

3.4.15.1 Adding a New Time Frame

To add a new Time Frame:

1. Right-click the **Time Frame** (root) node, and select **Add Component**.

2. Enter an appropriate Time Frame name.

3. In the Time Frames section, click to add a new row.

4. Enter Name, From Day, From Time and To Day, To Time values as required.

5. Repeat as many times as necessary. You can delete entries by clicking on the same row as the entry and selecting **Delete Time Frame**.

6. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

7. If you need to modify this list in the future, click **Edit** and make your changes.

3.4.16 Upstream Proxy

After traffic is scanned by the SWG system, it can be sent either to a router, based on routing table information, or to an upstream proxy, where the request is sent in proxy format.

Before configuring any Upstream Policy, the upstream proxy connections must be configured. This is done in the Upstream Proxy screen under Condition Elements.

Upstream Proxy definitions are available for rules in the following Policy types: Device Logging.

> **Direct** is the default Upstream Proxy component and is therefore not editable.
>
> Defined Upstream Proxies are available as rule **Actions** in Upstream Proxy policy rules.

For information options, see Options in the Condition Elements Tree.

3.4.16.1 Adding Upstream Proxy Connections

To add an Upstream Proxy and configure its connections:

1. In the Upstream Proxy tree, right-click the **Upstream Proxy** (root) node and select **Add Component**.

2. In the Name field, specify a name for the Upstream Proxy.

3. Fill in the following details:

Adding Upstream Proxy Connection Fields

Field Name	Description
Client IP Header	Header information for user identifiers supplied by an upstream proxy.
User Name Header	Specifies the User Name in the Header Field.
For HTTP, HTTPS, FTP over HTTP Protocols:	
Host	Host Name.
Port	Port Number.
Active	Select the check box if the settings for the protocol should be active.
Use for all protocols	Select this check box to use the same proxy for all protocols.
Enable caching per whole proxy definition	Select (or clear) this check box if caching should be activated globally (or on a per upstream proxy basis).

4. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

5. If you need to modify this list in the future, click **Edit** and make your changes.

3.4.17 URL Lists

URL Lists provide a large number of lists, almost all of which are editable (the only pre-supplied list that is not editable is **Trustwave Recommended White List**). You can also create your own lists.

URL lists play a large part in Security Policy. Many of the predefined URL lists are white lists (allowed), black lists (blocked), or bypass lists.

URL List conditions are available for rules in the following Policy types: Security, Logging, HTTPS, Caching, Identification, Device Logging, Upstream Proxy.

> The Bypassed Context Scanning List can be edited here but is not included in Rule Conditions. You can edit this list to decide which embedded objects do NOT need to be scanned in their full context. This is automatically used as part of the scanning process

The following topics are relevant to URL Lists.

* Creating a URL List

* Editing URL List Contents

* Searching all URL Lists for Specific URLs

* Regular Expressions

For information on options, see Options in the Condition Elements Tree.

3.4.17.1 Creating a URL List

To create a URL List:

1. Right-click the URL Lists (root) node and select **Add List**.

2. Enter an appropriate URL List name.

> To include the entire domain, a slash (/) and an asterisk (*) must be added.

3. Fill in the details of the list. For instructions, see Editing URL List Contents.

4. Click **Save** to apply changes. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

5. If you need to modify this list in the future, click **Edit** and make your changes.

3.4.17.2 Editing URL List Contents

The URL List definition screen contains two tabs:

* **URLs** — For listing the URLs that belong in the list.

* **Regular Expressions** — For defining expressions for URL categorization using Regex (Regular Expressions used to describe or match a set of strings according to certain syntax rules).

When adding URLs to a list, you can use either of the following methods:

- Manually add the URLs in the URL tab.

- Import a list of URLs into the URL List.

To manually edit a URL List:

1. If the definition screen for the list is not currently displayed, select the list in the **URL Lists** tree.

2. Click **Edit** if you are not in Edit mode.

   At any time, you can perform a search for specific items in the a tab by entering the desired value in the **Find All** field, and clicking **Search**. To clear the results, click **Clear**.

3. To edit the list of URLs, do the following in the **URLs** tab:

   a. To add a URL: Click ➕. Then enter the URL and optionally a description. Repeat as necessary.

   b. To delete a URL entry: Click 📋 on the row of the entry. Then select **Delete URL**.

4. To edit Regular Expressions, do the following in the **Regular Expressions** tab:

   a. To add a Regular Expression: Click ➕. Then enter the Regular Expression and optionally a description. For information on expression syntax, see Regular Expressions. Repeat as necessary.

   b. To delete a Regular Expression entry: Click 📋 on the row of the entry. Then select **Delete Regular Expression**.

5. Click **Save** to apply changes. To commit the changes, click ⚡ **Commit Changes** in the toolbar.

To import listed URLs from xml or txt files:

1. If the list to be imported does not yet exist, create it as follows:

   a. Do either of the following:

   Write a text file of URLs, with each URL starting on a new line

   or

   Write an xml file with each node representing a URL

   b. Save the file to a known location. (Alternatively, **export** an existing list of URLs to a known location and edit the list.)

2. If the URL List into which you want to import does not yet exist, create it. For instructions, see Creating a URL List.

3. In the URL List tree, right-click the URL List into which you want to import the file contents and select **Import to List**.

4. Click **Browse** and navigate to your saved file. Next, click **Open** on the Windows dialog box.

5. Click **Import,** located on the bottom of the screen. The contents of the file – that is, the URL addresses, appear in the pane.

6. Click **Save** to apply changes. To commit the changes, click **Commit Changes** in the toolbar.

7. The second option involves adding individual URLs (without protocols) to the list.

3.4.17.3 Searching all URL Lists for Specific URLs

To search all URL Lists for specific URLs:

1. Right-click the **URL Lists** (root) node in the tree, and select **Find URL**.

2. In the **Find URL** field of the **URL Lists** screen, enter an appropriate **URL.** This field requires only a partial URL.

3. Click **Search**.

The results of the find (the particular URL List in which the URL was found, and the actual URL) are listed in the area below.

3.4.17.4 Regular Expressions

The URL list also allows the use of Regex (Regular Expressions used to describe or match a set of strings according to certain syntax rules) to support regular expressions usage for URL categorization. The regular expression may be defined for each category as well for the URL List, with the ability to define several regular expressions for each category. As with all Regular Expressions, specific syntax rules vary depending on the specific library used.

Supported Regular Expression Syntax used in the Trustwave SWG URL Lists:

Supported Regular Expression Syntax used in the Trustwave SWG URL Lists

Sequence	Meaning
\a	Alert (bell)
\b	Backspace
\e	ESC character, x1B
\n	Newline
\r	Carriage return
\f	Form feed, x0C
\v	Horizontal tab, x09
\t	Vertical tab, x0B
\octal	Character specified by a three-digit octal code

Supported Regular Expression Syntax used in the Trustwave SWG URL Lists

Sequence	Meaning
\xhex	Character specified by a hexadecimal code
\cchar	Named control character
"..."	All characters taken as literals between double quotes, except escape sequences

Character and Class-like Constraints:

Character and Class-like Constraints

Sequence	Meaning
[...]	A single character listed or contained within a listed range
[^...]	A single character not listed and not contained within a listed range
.	Any character
\d	Digit character ([0-9])
\D	Non-digit character ([^0-9])
\s	Whitespace character ([\t\n\r\f\v])
\S	Non-whitespace character ([^ \t\n\r\f\v])
\w	Word character ([a-zA-Z0-9_])
\W	Non-word character ([^a-zA-Z0-9_])

Alternation and Repetition:

Alternation and Repetition

Sequence	Meaning
...|...	Try subpatterns in alternation.
*	Match 0 or more times (greedy)
+	Match 1 or more times (greedy)
?	Match 0 or 1 times (greedy)
{n}	Match **exactly** n times
{n,}	Match at least n times (greedy)
{n,m}	Match at least n times but no more than m times (greedy)
*?	Match 0 or more times (abstemious)
+?	Match 1 or more times (abstemious)

Alternation and Repetition

Sequence	Meaning
??	Match 0 or 1 times (abstemious)
{*n*,}?	Match at least *n* times (abstemious)
{*n,m*}?	Match at least *n* times but no more than *m* times (abstemious)
{*MACRO*}	Include the Regex *MACRO* in the current regex
^	Start of string or after a new line

3.4.17.5 True Content Type

The administrator can choose to edit True Content Type lists.

These lists are based on existing True Content Type profiles and cannot be edited via **Policies | Condition Elements**.

True Content Type

Component Name	Description
True Content Type White List	Any True Content Type that you check in this list will be allowed through but will be scanned for viruses.
True Content Type Black List	Any True Content Type that you check in this list will be blocked from entering the organization.

3.4.17.6 URL Categorization

The administrator can choose to block URL Categories.

These lists are based on existing URL Filtering categories and cannot be edited via **Policies | Condition Elements**.

URL Categorization

Component Name	Description
URL Category Black List	Any category that you check in this list will be blocked from entering the organization. This is in addition to the pre-selected categories in the URL Filtering condition.

3.5 End User Messages

The End User Message option (**Policies | End User messages**) has the following sub-options:

- Block/Warn Messages — Lets you edit messages sent to end-users from Security and HTTPS Rules.

- Message Template — Lets you redesign the message template used for displaying block and warn messages.

3.5.1 Block/Warn Messages

The Block/Warn messages are sent to end-users if the URL site which they are attempting to access has either been blocked by SWG or has been designated as a site requiring user approval or coaching action (user approval and coaching messages are referred to collectively as Warn Messages).

These messages are chosen for each Block/Coach/User Approval rule in the Security/HTTPS Policies as required.

The messages include Place Holders which are replaced with real values when displayed to the end-user.

> For a full list of the pre-defined Block/Warn Messages that will appear in the Page Blocked/Coach/User Approval messages and their corresponding Security Rule (where applicable), see Appendix B: End User Messages.

To create a new Block/Warn message:

1. Select **Policies | End User Messages | Block/Warn Messages**.

2. Right-click the **Block/Warn Messages** (root) node and select **Add Message**.

3. Type in the **Message Name**. This field is mandatory.

4. In the **Message** section, enter the required message text.

5. Use the **Place-Holders** drop down menu to provide the end-user with more information. For example, select **Client IP**, **Malware Entrapment Profile Names**, and **Domain**. Be sure to click **Add** between each. For more information, see Block/Warn Message Details.

6. Click **Save**.

   The new message can now be selected from the Rule Details screen, in the End-User Message drop down list.

7. If you are ready to distribute and implement the changes in your system devices, click ⬇ **Commit Changes** in the toolbar. To modify this message in the future, click **Edit** and make your changes.

The end result of this message page is either a **Coach**/**User Approval** (Warning) message or a **Page Blocked** message sent to the end-user.

3.5.1.1 Block/Warn Message Details

Each message is composed of a mixture of free text and placeholders, which can be moved around to create your own unique message.

When copying text from another source, remove all formatting by pasting the text into Notepad or a similar plain text application first, and then re-copy it from the text application to the SWG screen.

Warn message Details – Place Holders

Place Holder	Description
Binary Behavior Profile Names	Description of the potentially dangerous binary content operation.
Binary Profile List	Active Content List name that appears in a Trustwave or customer defined black list.
Binary VAD	Description of Binary exploit.
Client IP	Client IP address.
Container Type	Type of container holding the content of this transaction.
Container Violation	Container condition, such as password protection, or deep nesting of archives.
Content Type Name	Name of the Content Type.
Digital Signature Violation	Type of violation of digital signature.
Direction	Direction (Incoming or Outgoing) of the transaction.
Domain	End-user NTLM domain name.
File Extension	File extension of the content.
File Name	File name as extracted from URL. Note that not all URLs contain file names (i.e. this placeholder may appear blank).
File size	Size of the file (bytes). Currently, the file size appears without the unit after it. Add the word "bytes" to make it clear to the end-user.
Header Fields	Header Field names associated with the transaction.
HTTPS Certificate Validation Mismatch	Defined Certificate Validation errors.
HTTPS Policy Name	Name of HTTPS Policy enforced on the transaction (as shown in **Management Console | Policies**).
Identification Policy Name	Name of Identification Policy enforced on the transaction (as shown in **Management Console | Policies**).

Place Holder	Description
Instant Messaging	IM method.
Logging Policy Name	Name of Logging Policy enforced on the transaction (as shown in **Management Console | Policies**).
McAfee/Sophos/ Kaspersky Virus Name	Name of the virus as identified by one of the AV Scanning Engines.
Policy Name	Policy name currently set to the User or User Group initiating the transaction.
Script Behavior Profile Names	Description of the potentially dangerous script content operation.
Site domain	Domain name of the site that was blocked or coached.
Site URL	URL name.
Size Category	Content Size.
Spoofing Type	Type of spoofed content.
Spyware Description	Description of the spyware as identified by Trustwave Spyware database.
Spyware name	Name of the Spyware as identified by Trustwave Spyware database.
Static Content List	Content found in the Malicious Objects List.
Time Frame	Time Frame for the defined transaction.
Transaction ID	Unique transaction ID which can be matched in the Management Console log view.
Transaction time	Time that the transaction was carried out.
URL List Name	URL List name that appears in a Trustwave or customer defined list.
User Name	End-user NTLM name.
The following Place Holders deal with formatting issues:	
Bold End	Delineates the end of bold format for a word or phrase.
Bold Start	Delineates the start of bold format for a word or phrase.
New Line	Delineates a new line in the error message.

3.5.2 Message Template

The **Message Template** option (**Policies | End User Messages | Message Template**) enables you to redesign message templates. You do this by making the appropriate selections and then clicking the appropriate buttons, This inserts the chosen elements into the template.

> **Warning**: It is recommended that you do not change message templates. Editing the Block/Warn pages may result in security vulnerabilities.
>
> If you do make changes, make them carefully and preview them before applying them. Also do not use non-Trustwave form elements or Java Script commands.

To redesign a message template:

1. Select **Policies** | **End User Messages** | **Message Template**.

2. In the main window, click **Edit**.

3. In the Rule Action drop down list, select the type of template that you want to edit.

4. In the template development box, design the template by doing any of the following (ensure that you position the cursor in the desired location before performing the action):

    •   To add text, type it in.

    •   To add a variable representing notification text, select **Notification** in the drop down list next to the **Add** button, and click **Add**.

    •   To add an **OK** button, select **Redirect Button** in the drop down list next to the **Add** button, and click **Add**.

    •   To add a **Back** button, select **Back Button** in the drop down list next to the **Add** button, and click **Add**.

5. Preview your design by clicking the **Preview** button. The Preview is displayed in a different window. Close it when you are done with the preview.

6. To see the HTML version of your design, click **Switch to HTML View**. You can then toggle back.

7. If you are certain that you want to save the changes, click **Save**. Otherwise, click **Cancel**.

8. If you are ready to distribute and implement the changes in your system devices, click **Commit Changes** in the toolbar.

4 Logs and Reports

Logs are available for system monitoring and for administrator monitoring.

Reports enable you to analyze system activity and performance based on data stored in the Reports database. The Reports screen provides predefined Reports divided into meaningful categories only on data from those users that you are responsible for (as defined in Administrator Permissions). New reports cannot be created in the SWG Management Console. However, existing reports may be duplicated. Schedule Reports provides you with the flexibility to decide when you want a Report to be generated, where you want it to be sent and in what format. Reports can be scheduled according to time, output and format, and Reports previously created by the Schedule Report Target option can also be viewed.

The Logs and Reports menu provides access to several methods of monitoring your system:

- **Logs**

  The Log Server logs all transactions, according to the configuration settings that you define. There are three types of logs:

  - **Web Logs** — Records Web-surfing transactions of users in your network, according to your logging policy.

  - **System Logs** — Records events that have taken place in the system, for example, updates that have been installed, a module that is not responding and so on.

  - **Audit Logs** — Records all changes made or actions taken from the Management Console, including tracking the creation of and changes to, policies, as well as system configuration.

  The Views window consists of two panes:

  - Views tree — Lists the currently-defined Views for that type of log.

  - View definition main window — Displays the selection options for the log and the log table.

    Clicking 🔲 **View Settings** on the left of the Web Logs, System Logs, or Audit Logs windows displays two tabs (**General** and **Filter**) where the View parameters of the log type are defined.

  Each log type comes with pre-defined Views. A View defines which log data columns to display, and filtering specifications for each log entry. When working with logs, you can choose which View to apply to the log, define additional Views, and set other log display criteria. For more information, see Changing a Log View.

- **Reporting Tool**

  The **Reporting Tool** comes with a number of predefined reports (that is, report definitions) that enable enterprises to analyze the activity and performance of the SWG system based on data stored in the Reports database. Reports are generally categorized according to the type of data they provide.

  You can also define the connection method and location to which all reports are exported.

- **Dashboard**

  For more information, see **Dashboard**.

4.1 Changing a Log View

You can change a log view according to your management needs.

1. Click ![icon] **View Settings** on the left of the window, or right-click the log in the tree and select **View Settings**. Then click the **Edit** button.

2. In the **General** tab:

   a. Select the check boxes of the columns you want in the displayed table. Deselect the check boxes of the data you do not require.

   b. Set the refresh interval and number of entries required.

3. In the **Filter** tab, select the conditions for retrieval of the log records.

4. Click **Save**.

5. In the displayed log table, drag and drop column headers to change their order according to your viewing preferences.

6. To adjust the width of a column to fully view the contents or the header name, double-click the column header.

Logs and Reports Sub-Menu Options

Menu Options Under the Logs and Reports Main Menu

Main Option Sub Option	Description/Purpose
Web Logs	Displays the list of Web Log entries, in the Web Logs screen. This window lets you specify selection criteria which will impact which Web Log entries are displayed. It also provides a number of control buttons. For more information, see Web Logs.
System Logs	Displays the list of System Log entries, in the System Logs screen. This window lets you specify selection criteria which will impact which System Log entries are displayed. It also provides a number of control buttons. For more information, see System Logs.
Audit Logs	Displays the list of Audit Log entries, in the Audit Logs screen. This window lets you specify selection criteria which will impact which Audit Log entries are displayed. It also provides a number of control buttons. For more information, see Audit Logs.

Menu Options Under the Logs and Reports Main Menu

Main Option Sub Option	Description/Purpose
Reporting Tool	Provides access to the menu options of the Reporting feature:
Reports	Displays the window for selecting, editing, viewing and running reports. This window consists of two panes: **Reports tree** — Lists available reports, broken down by category. The tree also contains a Favorites folder where you can add shortcuts to your favorite reports. In this tree, you choose which actions (run, schedule, history, and so on) are to be performed on a particular report. **Main reports window** — The currently-defined views for that type of report. **View definition main window** — Contains three tabs (**General**, **Columns**, and **Filters**) which determine the type of information displayed in the report. For more information, see Reports.
Exported Reports Location	Enables you to define the location to which reports will be exported, and to test the connection to that location. For more information, see Exported Reports Location.

4.2 Web Logs

The Web Logs window displays user Web surfing transactions.

The super administrator sees a Web View with logs belonging to all other administrators in the Trustwave SWG. System administrators see those Logs belonging to User groups assigned to them or according to their specific permissions.

The logs show user transactions that have been blocked, allowed or coached, according to the Logging Policy assigned to the administrator.

To change a log view according to your management needs, see Changing a Log View.

This section describes the following:

• Selection Fields in the Web Logs Window

• Data Fields in the Web Logs Window

• Data Handling in the Web Logs Window

• Action Buttons in the Web Logs Window

• Transaction Entry Details Window

4.2.1 Selection Fields in the Web Logs Window

Selection fields in the Web Logs window enable you to determine what Web Log data is displayed.

After specifying a search parameter, you must click Apply to perform the search.

Web Logs Window – Selection Fields

Field	Description
Admin Group	Enables you to view Web logs by administrator group, or for all administrator groups. The field provides a drop down list of administrator groups whose Web logs you have permission to view. For more information, see Administrators.
Time Frame	Enables you to view Web transactions whose dates fall within a specific time frame, such as **Today**, **Last 7 Days**, or **All**. Select the time frame from the drop down list.
	If you select **Date Range** from the list, you can choose exact start and end dates and times.
Find By	Enables you to search for a transaction by selecting a search parameter such as Transaction ID or URL Category from the drop down list.
	• You can further refine the results by entering a filter in the field next to the **Find By** box. A drop down list is provided for some search parameters.
	• To remove the filter on an entered search parameter, click **Reset Field** ☒ .

4.2.2 Data Fields in the Web Logs Window

The Default column in the following table indicates in which predefined views (if any) the data item appears as a default. The Default column uses the following numbers to indicate which view(s):

1 - Default view

2 - Approved Coached view

3 - Blocked Transaction view

Data Fields in the Web Log

Data Field	Description	Default
Transaction id	Unique ID of the transaction	
Action	**Allow**/**Block**/**Coach**/**Nothing**, and several other options.	1,3
URL	Transaction URL	1, 2, 3
Transaction Time	Time the transaction took place.	1, 2, 3,
Block Reason	Reason the transaction was blocked. This is the reason that appeared in the browser during the block. **Note:** This message can be configured.	1
User Name	User name as recognized by the scanning engine.	
anti-virus (Sophos, McAfee, or Kaspersky)	**Note:** Only the licensed Anti-virus' field will appear. The field will also display the Anti-virus item that blocked (or coached) the transaction, if the Anti-Virus engine was involved.	1, 2, 3
URL Category	**Note:** Only one field will appear, depending on the customer license. This field will also display the category that blocked (or coached) the transaction, if the URL Category engine was involved.	1, 2, 3
Dynamically Categorized	Displays **Yes** if the URL was identified using TextCensor in cases where the URL Categorization engine fails to classify it.	
Authenticated Domain / Authenticated User name	These fields will be filled only if the transaction was identified by Authentication (e.g. LDAP, Realm).	
Client IP	IP of the client that used the proxy (displayed only if the transaction was identified by IP).	1, 2, 3
Site	Site of the transaction (part of the URL).	

Data Fields in the Web Log

Data Field	Description	Default
Scanning Server IP	Scanning server that scanned the transaction.	
Security Policy Name	Name of the security policy that was used for scanning the transaction.	
Security Rule Name	Name of the security rule that was used for scanning the transaction.	
HTML Repair	(Y/N). Displays **Yes** if the HTML was repaired before rendering it in the browser.	
HTTPS Policy Name	Name of the HTTPS policy that was used for scanning the transaction.	
Master Policy Name	Name of the Master policy that was used for scanning the transaction.	
Identification Policy Name	Name of the Identification policy that was used for scanning the transaction.	
HTTPS Rule Name	Name of the HTTPS rule that was used for scanning the transaction.	
Identification Rule Name	Name of the Identification rule that was used for scanning the transaction.	
Destination IP	The IP of the requested URL.	
XRAY mode	Y/N according to the XRAY mode.	
Cache Hit	Indicates if the cache was used.	
Active Content List	Will includes the list that blocked (or coached) the transaction, if the ACL engine was involved.	
Behavior Profile (Binary)	Will include the item that blocked (or coached) the transaction, if this engine was involved.	1, 2, 3
Malware Entrapment Profile	Will include the item that blocked (or coached) the transaction, if this engine was involved.	1, 2, 3
Coach Page	Displays a page indicating to the user that the requested page is restricted.	
Coach Bypass	Displays the action to be taken after an attempt to view a restricted page.	2
Parent Archive Type	Will include the item that blocked (or coached) the transaction, if this engine was involved.	
True Content Type	Will include the item that blocked (or coached) the transaction, if this engine was involved.	

Data Fields in the Web Log

Data Field	Description	Default
Extension	Will include the item that blocked (or coached) the transaction, if File Extension engine was involved.	
File Name	Displays the File Name if the URL includes file name.	
Header Fields	Will include the item that blocked (or coached) the transaction, if the Header Fields engine was involved.	
IM/P2P Protocol	Refers to the Instant Messaging (IM) and Peer-to-Peer File Sharing (P2P) protocols.	
Master Rule Name	Name of the Master rule that was used for scanning the transaction.	
Identification Status	(Usually displays **Succeeded**.)	
Upstream Proxy Status	(Usually displays **Succeeded**.)	
Protocol	HTTP/FTP/HTTPS	1, 2, 3
ICAP Policy Name	Name of the ICAP REQMOD or RESPMOD policy that was used for scanning the transaction	
ICAP Rule Name	Name of the ICAP REQMOD or RESPMOD rule that was used for scanning the transaction	
ICAP Rule Status	REQMOD or RESPMOD: (Usually displays **Succeeded**.)	
ICAP Service	Which ICAP REQMOD or RESPMOD Service handled this transaction.	
ICAP Block Reason	Reason the ICAP Service blocked the transaction.	

4.2.3 Data Handling in the Web Logs Window

Clicking the ▶️ icon next to a Web Log transaction in the Web Logs window enables you to choose any of several actions to perform on that item.

You can also double-click an item to view the item's **Details**.

Web Logs Window – Transaction Detail Options

Option	Description
Details	Displays additional Transaction Entry details in the same window. For more information, see Transaction Entry Details Window.
Open in a new window	Displays additional Transaction Entry details in a new window. For more information, see Transaction Entry Details Window.
Add to URL list	Adds the URL to the required URL list, thus allowing it to be blocked/allowed in the Security Policy.
Export to CSV **Export to XML**	Displays the log entry as a csv or xml type file. You can right-click the file and then save or print the file as required.

4.2.4 Action Buttons in the Web Logs Window

Web Logs Window Action Buttons

Button	Description
Next/Previous	Lets you page forward and backward through the list of transactions.
Log Cleanup	(In the Header row) Deletes all Web log entries in the table. **Warning: Log cleanup cannot be stopped once it is initiated, and the process is irreversible.**

4.2.5 Transaction Entry Details Window

The Transaction Entry Details window displays additional information about a Web Log transaction entry.

To display this window, click the ▶️ icon next to a transaction in the Web Logs window, and choose either **Details** or **Open in a new window**:

- if you choose **Details**, the details are displayed in the current window.

- If you choose **Open in a new window**, the details are displayed in a new window.

The Transaction Entry Details window contains a Transaction Entry tree and a main window:

- The Transaction Entry tree contains:

    - a main node, called **Details**.

    - where relevant, two lower nodes, called **Request** and **Response**.

- The display in the main window depends on the selection in the tree:

    - When **Details** is selected in the tree, the main window is called the **Details** pane, and it contains numerous tabs, each displaying information about the transaction.

    - When **Request** or **Response** is displayed, the main window displays the appropriate Request or Response information.

If you opened the Transaction Entry Details window in the same window (instead of in a new window), clicking **Back** re-displays the Web Logs view.

The following sections describe the fields in the tabs of the **Details** pane (and **Request** and **Response** panes) of the Transaction Entry Details window.

- Details Pane: Transaction Tab

- Details Pane: User Tab

- Details Pane: Policy Enforcement Tab

- Details Pane: Content Tab

- Details Pane: Scanning Server Tab

Details Pane: Transaction Tab

Transaction Entry Details Window – Details Pane – Transaction Tab Fields

Field	Description
Transaction ID	The Unique ID identifies the specific transaction as displayed in the End User Message and is useful when following up a blocked transaction for the end user. It is advisable to have the Transaction ID displaying at all times. However, even if you choose not to display this column heading, you can still search for it in the Logs.
Transaction Time	Time and date that the transaction took place.
URL	URL to which the user browsed. Click this URL to add it to the required URL List.
Referer	Value of HTTP header "Referer" if present in the current transaction.
Destination IP Address	IP of the server that is supposed to respond to the requested URL.
Protocol	Protocol that was used by the end-user.

To copy the URL to the clipboard, click the ▣ icon next to the URL value, and choose **Copy to clipboard**. If you are prompted for confirmation, confirm the request.

To add the URL to the a URL list:

1. Click the ▣ icon next to the URL value, and choose **Add to URL list**.

2. In the **Add to URL List** window that is displayed, select the URL List in the drop down list and click **OK**.

Details Pane: User Tab

Where available, click the displayed button or link for more details.

Transaction Entry Details Window – Details Pane – User Tab Fields

Field	Description
Trustwave SWG User Name	Name of the user defined in the Users tab who requested the transaction.
Client IP Address	IP address of the end-user.
Authenticated User Name	User Name as provided by NTLM or basic authentication.
Authenticated Domain	User Domain as provided by NTLM or basic authentication.

Details Pane: Policy Enforcement Tab

Where available, click the displayed button or link for more details.

Transaction Entry Details Window – Details Pane – Policy Enforcement Tab Fields

Field	Description
Action	Rule Action (Block, Allow, Coach or Block HTTPS, Bypass, Inspect or User Approval).
X-Ray Mode	Defines whether the transaction was processed in X-Ray mode. If X-Ray mode is enabled, the log view shows what would have happened to the transaction had the rule/policy been active.
Master Policy Name	Name of the master policy used to process the transaction.
Security Policy Name	Name of the Security Policy used to process the transaction.
HTTPS Policy Name	Name of the HTTPS Policy used to process the transaction.
Identification Policy Name	Name of the Identification Policy used to process the transaction.
Upstream Proxy Policy Name	Name of the Upstream Proxy Policy used to process the transaction.
ICAP Policy Name	Name of the ICAP REQMOD or RESPMOD Policy used to process the transaction.
Block Reason	Message sent to the end-user explaining the reason the content was blocked.
Master Rule Name	Name of the master rule used to process the transaction.
Security Rule Name	Name of the Security rule used to process the transaction.

Transaction Entry Details Window – Details Pane – Policy Enforcement Tab Fields

Field	Description
Security Rule Description	Text that appears in the Rule Description field.
HTTPS Rule Name	Name of the HTTPS rule used to process the transaction.
Identification Rule Name	Name of the Identification rule used to process the transaction.
Identification Status	If identification succeeded.
Upstream Proxy Rule Name	Name of the Upstream Proxy rule used to process the transaction.
Upstream Proxy Status	If the connection to the Upstream Proxy was a success or failure.
ICAP Rule Name	Name of the ICAP REQMOD or RESPMOD rule used to process the transaction.
ICAP Rule Status	If the ICAP REQMOD or RESPMOD rule processing was a success or failure.

Details Pane: Content Tab

Where available, click the displayed button or link for more details.

Transaction Entry Details Window – Details Pane – Content Tab Fields

Field	Description
File Name	Name of the file specified in the requested URL.
Behavior Profile (Binary)	Behavior profile (binary) that matched the content in the transaction.
True Content Type	True Content Type that matched the content in the transaction.
Malware Entrapment	List of actions that could be considered malicious or suspicious when executed by Web pages, VB Script files, Java Script files or other relevant files.
Parent Archive Type	Parent Archive Type that matched the content in the transaction.
Active Content List Found	Active Content List that matched the content in this transaction.
File Extension	File extension (including Multiple Extension) that matched the content in this transaction.
Header Field	Header Field that matched the content in this transaction.
URL Category	URL Category that matched the content in this transaction

Transaction Entry Details Window – Details Pane – Content Tab Fields

Field	Description
Advanced Binary Scanning	Description of Binary exploit.
Anti-Virus (Sophos) Scan Result	Virus detected by the Sophos Anti-Virus engine.
Anti-Virus (McAfee) Scan Result	Virus detected by the Mcafee Anti-Virus engine.
Anti-Virus (Kaspersky) Scan Result	Virus detected by the Kaspersky Anti-Virus engine.
Cache Hits	Lists how many times the cache was used instead of the original site.

Details Pane: Scanning Server Tab

Transaction Entry Details Window – Details Pane – Scanning Server Tab Fields

Field	Description
Scanning Server IP	IP address of the Scanning Server that scanned this transaction.
Scanning Server Type	Type of Scanning Server that scanned this transaction. (Cloud or other)

Transaction Entry: Request and Response Phases

For each transaction, the content is scanned on both the request and/or the response phase depending on the nature of the content and the nature of the rule that it triggered.

The information displayed in these panes depends on the nature of the transaction and is useful in determining why the transaction was blocked.

4.3 System Logs

The System Logs window displays information relevant to the components of the Trustwave Secure Web Gateway Appliance.

To change a log view according to your management needs, see Changing a Log View.

This section describes the following:

- Data Fields in the System Logs Window

- Action Buttons in the System Logs Window

- Selection Fields in the System Logs Window

4.3.1 Data Fields in the System Logs Window

<div align="center">System Log Data Fields</div>

Data Field	Description
The following data fields are displayed by default:	
Log ID	ID of the transaction.
Time	Time of the system log
Device IP	Device in the SWG configuration where the system log was generated
Severity	Severity of the system log
Message	System log message
The following Syslog data fields are available but are not displayed by default (To change the display, click the **View Settings** icon on the left, or right-click the log in the tree and select **View Settings**):	
Sender	Component that sent the system log
Module	Module that generated the system log

4.3.2 Action Buttons in the System Logs Window

<div align="center">System Logs Window Action Buttons</div>

Button	Description
Next/Previous	Lets you page forward and backward through the list of transactions.

4.3.3 Selection Fields in the System Logs Window

Selection fields in the System Logs window allow you to determine what System Log data is displayed in the window.

<div align="center">System Logs Window – Selection Fields</div>

Field	Description
Find Log ID	Enables you to search for a transaction by specifying its unique Log ID. • After specifying the Log ID, you must click **Apply** to perform the search. • To undo filtering on the Log ID, click **Reset Field** ❌ .

4.4 Audit Logs

The Audit Logs window enables you to keep track of all administrator changes to the SWG Management Console. The Audit logs all changes made or actions taken from the Management Console, including tracking the creation of and changes to policies, as well as system configuration.

To change a log view according to your management needs, see Changing a Log View.

This section describes the following:

• Selection Fields in the Audit Logs Window

• Data Fields in the Audit Logs Window

• Action Buttons in the Audit Logs Window

4.4.1 Selection Fields in the Audit Logs Window

Selection fields in the Audit Logs window allow you to determine what Audit Log data is displayed in the window.

<div align="center">Audit Logs Window – Selection Fields</div>

Field	Description
Find Log ID	Enables you to search for a transaction by specifying its unique Log ID. • After specifying the Log ID, you must click **Apply** to perform the search. • To undo filtering on the Log ID, click **Reset Field** ❌ .

4.4.2 Data Fields in the Audit Logs Window

Audit Logs Window – Data Fields

Data Field	Description
The following data fields are displayed by default:	
Log ID	ID of the transaction.
Time	Time of the Audit operation.
Message	Audit message.
Notes	Audit Notes. (These are the notes that are added during the **Commit** operation.)
Admin Id	Admin name that made the operation of this audit.
Severity	Severity of the system log.
The following data fields are available but are not displayed by default (To change the display, click the **View Settings** icon on the left, or right-click the log in the tree and select **View Settings**):	
Module	Module that generated the Audit.
Device IP	Device in the SWG configuration where the Audit was generated.
Client IP	Admin IP.

4.4.3 Action Buttons in the Audit Logs Window

The **Next** and **Previous** buttons let you page forward and backward through the list of transactions.

4.5 Reporting Tool

This menu option contains the following sub-menu options:

• Reports

• Exported Reports Location

4.5.1 Reports

The Trustwave Reporting Tool comes with a number of predefined reports (that is, report definitions) that enable enterprises to analyze the activity and performance of the SWG system based on data stored in the Reports database.

The Reports are generally categorized according to the type of data they provide (for example, Anti-Virus reports, Productivity reports).

The data that actually appears in a report generally depends on number of factors:

- permissions of the Administrator under whom the report is being run (for example, the report can only include data pertaining to those users for which the administrator has access permission)

- filtering criteria applied to during the report run

Reports are defined, run, and managed in the Reports window, which is accessed by selecting **Logs and Reports | Reporting Tool | Reports**.

The Reports window contains two panes:

- **Tree Pane** — Lists all available reports, by category (for a description of the categories, see Reports Categories in the Tree Pane). This pane also contains a **Favorites** folder for adding shortcuts for selected reports. And it includes icons for quick performance of report management functions.

- **Main Pane** — Generally displays the definition of the report selected in the tree. It can also display other contents, depending on the particular action you perform.

A report definition contains:

- several identifying parameters (name and description)

- the list of data columns to be included in the report

- filters to be applied to the report and optional scheduling criteria

You can define schedules that determine when a report will be run, and you can manually run a report at any time you wish.

> Before a report can be generated with data, the **Send to: Report** check box in **Policies | User Policies | Logging | Rule: Logging Action** must be selected (which enables log data to be sent to the Reports database).

In addition to running and viewing reports, you can perform a number of other report actions. For example, you can duplicate reports and modify the duplicate definitions, and you can store and access a report's history.

4.5.1.1 Tabs, Fields, and Buttons in the Report Definition (Main) Pane

When clicking on any report (in any category), the following tabs are displayed:

- General Tab

- Columns Tab

- Filters Tab

General Tab

The General tab contains any or all of the following fields. Click **Edit** to activate the screen:

Report Definition Main Pane – General Tab Fields

Field/Button	Description
Name	Predefined Name of Report.
Description	Provides a predefined detailed description for the Report.
Report Type (where relevant)	Select the type of report, such as pie chart, bar chart, and so on.
View As	This is the output of the Report. In the drop down list, you can choose between HTML, PDF, Excel and CSV.

Columns Tab

The Columns tab contains the columns/fields which are displayed in the final report. Column options available are dependent on the report selected.

For example, in the **Blocked Web Sites** report, the column options include: Bandwidth, Security Rule Name, Site, Transaction time, and URL Category.

In the **Infected Machines** report, the column options include: Authenticated User, Transaction time, URL, and User Name.

Filters Tab

The Filters tab contains fields used for selecting the conditions in the log records retrieval.

Click **Edit** to enable filter editing. Click **Save** when you are done.

Report Definition Main Pane – Filters Tab Fields and Buttons

Field Name/Button	Description
Field	Drop down menu of the fields available with which to run the filter, per specific report. For example, Traffic Analysis By Hour includes fields such as Client IP, URL Category, and Content Type.
Operator and Value	Offers the values used in configuring the filter. For example, if **Transaction Time** is selected from the **Field** drop down menu, the time frame for which this report is to run has the following two enable options: **From:** date and time in hh:mm:ss format. **Last:** X number of days
	Clicking this icon displays options for adding or deleting filters.

Report Definition Main Pane – Filters Tab Fields and Buttons

Field Name/Button	Description
✗	Clicking this icon deletes a filter row (displayed in Simple mode only).
Switch to Simple mode	When defining multiple filters, you can work in **Simple Mode** or **Advanced Mode**. **Simple Mode** (default) is useful when multiple filters all have an AND relationship (or, of course, if you define only a single filter). This mode: • allows only AND relational operators; it does not allow OR operators. • does not display parentheses columns for defining complex relationships. • displays a ✗ icon to the left of the Filter definition. **Note:** If a filter definition contains brackets or an "OR" operator, this button is disabled.
Switch to Advanced mode	When defining multiple filters, you can work in **Simple Mode** or **Advanced Mode**. **Advanced Mode** is useful when multiple filters have at least one OR relationship. This mode: • allows specification of AND and OR operators. • display parentheses columns for defining complex relationships. • displays a ✗ icon to the left of the filter definition.

4.5.1.2 Reports Categories in the Tree Pane

The only right-click option that can be performed on a Category folder is **Delete**. This option is intended only for use with duplicates made of original Trustwave Reports. Original Trustwave reports provided with the system cannot be deleted.

Reports are categorized according to the type of data they provide. For example, Productivity, Compliance, Web Security, and Anti-virus. The following table provides a brief description of each Report category. (See Appendix A: Appendix A: Reports for a more detailed listing of all Reports.)

Report Categories

Category	Description
Anti-Virus	Generates reports detailing the top viruses blocked by SWG.
Compliance	Generates reports detailing the organization's compliance with various regulatory requirements, based on reports such as potential disclosure of sensitive information, browsing to Websites that could expose the company to legal liability, and so on.

Report Categories

Category	Description
Instant Messaging and P2P	Generates reports detailing the use of Instant Messaging and P2P communication within the organization.
IT Operation	Generates reports providing an overview of the network activity, that allow to detect infected machines and network characteristics and bottlenecks.
Productivity	Generates reports detailing the employees browsing habits, with targeted reports for special Website categories – such as legal liability related, job search, and so on.
Web Security	Generates reports detailing the security threats blocked by the various security engines of SWG.

4.5.1.3 Actions Performed in the Report Window Tree Pane

Important: In addition to the action options listed below, you can also backup and restore the Reports database (via **Administration | Reports DB Backup**). For more information, see Reports DB Backup.

The following table provides a brief description of actions that can be performed for any report. These actions can be performed by either:

• selecting the report in the tree pane and clicking the icon.

• right-clicking the report in the tree pane and choosing the option.

Where useful, detailed descriptions are provided after the table.

Report Window – Tree Pane – Available Actions

Icon	Action	Description
🔍	**Run Report**	Use this option to manually run a report at any time. This option displays the Report definition in the Report window, but the window contains modifications relevant to running a report, including an option to run the report in the background. For more information, see Run Report Option.
📄	**Duplicate Report**	Creates a copy of a report definition, which you can then modify (for example, column and filter values) and save with a new name.

Report Window – Tree Pane – Available Actions

Icon	Action	Description
	Add New Schedule	Opens the New Schedule window, which enables you to create a schedule for a single run or recurring runs of the report. This window also enables you to define the Report target, columns that will appear in the report, and filtering criteria for the report.
		Once defined, the schedule is listed in the tree pane as a node under the report.
		You can define multiple schedules for any report. Existing schedule definitions can be edited as needed.
		For more information, see New Schedule/Existing Report Schedule Window.
	Restore Defaults	Restores default settings in the default screen. Duplicated reports will be restored to defaults of the original report.
	History	Displays a report's history. This option can be applied to either of the following:
		• Report — When activated against a report, the history window lists all report runs from all schedules, and all manual background runs of the report.
		• Report schedule — When activated against a report's schedule, the history window lists only those report runs generated by that schedule.
		You can view or delete reports listed in the history display.
		For more information, see History Display.
	Add to Favorites	Lists the report (and its schedules) in the Favorites folder (in addition to its being listed in its regular location). This option is intended to provide easy access to frequently used reports, so that you do not have to scroll through the entire tree.
		The Favorites folder itself has no right-click options, but you can apply the same options/actions to listings in the Favorites folder that you can apply to the regular listings. (You can also delete a listing from the Favorites folder without deleting it from its regular location, by right-clicking the listing and choosing **Remove From Favorites**.)
	Delete Report	You can use this option to delete duplicates of original Trustwave Reports. (Original Trustwave reports cannot be deleted.)

4.5.1.3.1 Run Report Option

The Run Report option is used to run reports on demand (as opposed to on a schedule).

Choosing the **Run Report** option displays the Report definition in the main Report window. The tabs of the report definition (**General**, **Columns**, **Filters**) contain their default values. You can modify the defaults for the report run (the changes will affect only the current run).

The Report window also displays several important modifications:

- A **Run in Background** check box is added to the **General** tab. Selecting this check box both enables the report to run in the background, and ensures that the report run is stored in the History repository. The check box is accompanied by an **Instance Name** field, which enables you to assign a name to this report run instance for easy identification.

  Note the following:

  - If a report is run in the background, the report run will be listed in the History screen, which you can access by right-clicking the report in the tree and choosing **History**. From there, you can request to view the report. For more information, see History Display.

  - If you do not run the report in the background, the report is displayed in a new window. The results are not saved.

- The Report window displays a ✔ Run Report button, which you can click to run the report after you are done modifying the definition.

4.5.1.3.2 New Schedule/Existing Report Schedule Window

You can create and modify run schedules for a report. These schedules can be for a single report run or recurring report runs. When defining these schedules, you can also define a target for the report run, the columns that should appear in the report run, and filtering criteria for the report run.

You create new report schedules in the New Schedule window, which you open by right-clicking the report name in the tree and choosing the **Add New Schedule** option (or by clicking the 🗐 icon).

Once you define and save the schedule, it is listed in the Reports tree as a node under the report.

You can then display the schedule definition in the existing report schedule window by selecting the schedule node in the tree. To edit the definition, click **Edit** in the main window.

Whether you are creating a new schedule, or editing an existing schedule, the process of defining the schedule remains the same:

- The schedule must be assigned an identifying name (in the **Schedule Name** field).

- The **Enable Scheduling** check box at the top of the screen must be selected.

- The schedule itself must be defined, and the other parameters of the report schedule definition should be filled in.

  The window provides the following four tabs for this purpose:

  - Report Schedule Tab — For defining the report schedule (described in greater detail below)

  - Report Target Tab — For defining the report output target (described in greater detail below)

  - Columns tab — For defining the columns that will appear in the report (for more information, see the Columns Tab description provided for report definitions)

  - Report Parameters tab — For defining filtering criteria (for more information, see the Filters Tab description provided for report definitions)

Report Schedule Tab

You must define a schedule for the report. You can define a schedule for a single run and/or recurring runs, in any combination, as needed. Note the following:

- **Once** — Select this check box for a single run, at the date and time you specify.

- For recurrent runs, select the **Daily**, **Weekly**, and/or **Monthly** check boxes, and specify the accompanying criteria.

- Hours must fall in the range of 0 (or 00) — 23.

- Minutes must fall in the range of 0 (or 00) — 59.

Report Target Tab

The **Report Target** tab enables you to send reports to one or more targets. You do this by selecting the appropriate target check boxes and adding the Email Address of the intended recipient.

Report Schedule Window – Report Target Tab

Field	Description
Enable Available Reports	Select this check box if the report should be stored on the appliance and appear in the **History** screen (for more information, see History Display). **Note:** The space limitation for locally saved reports is 1 GB; older reports will be erased once this limit is reached.
Export Report	Select this check box if the report should exported. If selected, the network destination must be defined in the Exported Reports Location window (accessed via **Logs and Reports | Reporting Tool | Exported Reports Location**).
Email to	Sends the report to the specified email address(es). Click the ➕ icon to add additional email addresses. **Important:** The icon is inactive, and emails cannot be sent, until Mail Server configuration (**Administration | System Settings | Mail Server**) is complete.

4.5.1.3.3 History Display

The following type of report runs are saved in the History repository:

- Scheduled report runs for which you selected the **Enable Available Reports** check box in the Report Target tab of the schedule; for more information, see New Schedule/Existing Report Schedule Window).

- Manual report runs that are run in background (for more information, see Run Report Option).

You view the list of a report's runs in the History display, which you open by applying the **History** option (right-click or icon). The display provides the following information for each listed run: **Name**, **Recurrence**, **Status**, **Date**, **Time**, **Format**.

You can apply the **History** option either directly to the report, or to a schedule belonging to the report, and this choice determines which runs are included in the History display:

• **Report** — When the **History** option is activated against a report, the History display lists all report runs from all schedules, and all manual background runs of the report.

• **Report schedule** — When the **History** option is activated against a report's schedule, the History display lists only those report runs generated by that schedule.

To view (or delete) reports listed in the History display, click the ▥ icon for the report run, and choose **Show Report** (or **Delete Row**). When you view a report, it is opened in a separate window.

> The History display opens in your current window (that is, the window that normally displays the report definition or schedule definition). Therefore, to re-display the definition, re-select the report or schedule in the tree.

4.5.2 Exported Reports Location

When defining a schedule for a report, you can indicate that the report should be exported (the **Report Target** tab contains an **Export Report** check box).

However, if you enable the export of scheduled reports, you must define the following parameters: **Connection Method**, **Report Location**, **User to connect with**, and **Password**.

You define these parameters in the Exported Reports Location window, which you access via **Logs and Reports | Reporting Tool | Exported Reports Location**.

You can choose any of the following **Connection Method** values:

• **FTP** — Connect using regular File Transfer Protocol.

• **FTP Passive** — Connect using File Transfer Protocol (there is a firewall located between the Policy Server and the remote FTP site).

• **Samba** — Connect using Server Message Block (SMB) communication protocol.

• **SFTP** — Connect using Secure File Transfer Protocol.

Note that the connection method you choose determines the format of the **Report Location**, **User to connect with** and **Password** value. The following table describes the formats according to connection method.

Export Reports Location – Connection Methods

Connection Method	User Name and Password Format
FTP, FTP Passive, or **SFTP**	**Report Location** format is: • For **FTP** or **FTP Passive**: `<server_ip_address>`**/dir** (for example, 10.194.5.104/Sarah_FTP) • For **SFTP**: `<server_ip_address>` (for example, 10.194.5.104/). **User to connect with** is the user name used when connecting to the Report Location. **Password** should be the password used by the above user.
Samba	**Report Location** must include the server IP address and directory for your selected location, in the following format: **//**`<server_ip_address>`**/dir**, (for example, `//192.168.1.10/backup`.) **User to connect with** must include the workgroup name and the user name used when connecting to the Report Location, in the following format: workgroup/user, for example, marketing/nicole. **Password** should be the password used by the above user.

You can click the **Test** button to check the parameters that you defined.

4.6 Dashboard

Select this sub-menu option to display to open the Dashboard (in a separate window). For information on the Dashboard, see Dashboard.

5 Administration

The Administration menu contains various sub-menus that enable you to configure system components and manage global settings.

The Administration Menu contains the following options:

- Administrators — Enables a Super Administrator to create administrators and administrator groups, and assign permissions for the various configuration options within the Management Console.

- System Settings — Enables you to configure SWG Devices, Scanning Options, Scanning Engines, Digital Certificates and Administrative Settings

- Cloud (Hybrid Deployment) — Enables you to configure Trustwave's Mobile Security Client settings that pertain to Policy Server configuration and GUI management.

- Policy Server DB Backup — Enables you to roll back the system to a previous stable state. Comprises Backup and Restore functions.

- Reports DB Backup — Enables an Administrator to either backup or restore data from the Reports database.

- Export/Import — Enables you to export Policies, HTTPS Policies, Identification Policies and Identification Logging Policies—as well as their conditions—from one Policy Server and import them into another.

- Updates and Upgrades — Enables you to configure and upload various updates for both security and software releases onto your Appliance.

- Alerts — Enables you to monitor the main modules and components of the system and notifies you of system events, application events or update events (via email or SNMP).

- System Information — Enables you to view the status of the system with respect to license and module information.

- Change Password — Allows an Administrator to change their password.

5.1 Administrators

SWG supports multiple administrators and administrator groups. All Administrator groups are characterized by the permissions that they are granted to access different items (for example, Alert Settings, or Block and Warn messages). All administrators are automatically assigned the permissions of the group to which they belong.

To simplify the process of assigning permissions to Administrator Groups, SWG comes with a set of baseline Default Permissions for all items for which access permission can be granted. This set of Default permissions is pre-configured by Trustwave, and cannot be edited.

Whenever you add an Administrator Group, this set of default permissions is automatically assigned as defaults for the group. You then adjust the permission assignments for the group as needed.

When you add an Administrator to an Administrator Group, the group's permissions (as adjusted) are automatically assigned as the defaults for the Administrator. You then adjust the permission assignments for the administrator as needed.

SWG also comes with two predefined Super Administrators. A Super Administrator is authenticated locally in the system (even when RADIUS authentication is enabled), and has maximum allowable permissions. Any administrator belonging to the Super Administrators group is, by definition, a Super Administrator.

If you are connected to a RADIUS Server, that server authenticates all administrators (except Super Administrators). In this case, new administrators (that is, those not assigned to another group) are automatically placed in a group called the RADIUS Default Group.

If your site has implemented Master Policy usage, you can also assign a Master Policy to the Administrator Group.

The Administrators screen (accessed via **Administration | Administrators**) displays two panes:

- tree pane

- main window

The contents of the main window depends on your selection in the tree pane.

This section contains the following topics:

- Default Permissions

- RADIUS Default Group

- Super Administrators and Other Administrator Groups

- Administrators

- Access Permissions – Category View and Grid View

5.1.1 Default Permissions

You can display the Default Permissions window by selecting the **Default Permissions** node in the tree.

The window displays the baseline permission defaults for administrators. The defaults in this window are preconfigured by Trustwave for easy permissions assignment and cannot be edited (the **Edit**, **Save** and **Cancel** buttons are grayed out). These defaults are automatically assigned to any Administrator group that you create. You can then edit the permissions of the particular group.

The Default Permissions window contains two tabs — the **Permissions – Categories View** tab, and **Permissions – Grid View** tab. Both tabs display the same information, but in different formats, so you can choose to display the default permissions using either tab.

For more information about these tabs, and the fields in them, see Access Permissions – Category View and Grid View.

5.1.2 RADIUS Default Group

The RADIUS Default Group is relevant only if you are connected to a RADIUS Server (which simplifies the process of granting new administrators access to the system by using already-defined users).

The RADIUS Default Group is a predefined Administrator Group that handles the following special situations:

- New, undefined administrators will receive the policy assigned to the RADIUS Default Group. (After the new administrator logs in for the first time, an existing administrator can move the new administrator to another group. The new administrator will then inherit the policy that is assigned to that group.)

- If the administrator is authenticated but the RADIUS server has no parameter containing the administration group ID, the user will automatically be assigned to the RADIUS Default Group.

Important: It is recommended that the RADIUS Default Group be assigned **View Only** permissions, so that higher permissions are not granted to every administrator authenticated by the RADIUS server. If an administrator needs higher permissions, create the administrator in a different group and delete the administrator from the RADIUS Default group.

To display the RADIUS Default Group window, select the **RADIUS Default Group** node in the tree.

To edit the details of the RADIUS Default Group, click **Edit**. After editing, click **Save**. To commit the changes, click ⋎ **Commit Changes** in the toolbar.

The RADIUS Default Group window has three tabs.

- **General** tab — This tab contains a single field, called **Notes**. In this field, you can enter any relevant free text that you want.

- **Permissions** — **Categories View** tab, and **Permissions – Grid View** tab. For information on using these tabs, see Access Permissions – Category View and Grid View

To add an administrator to the RADIUS Default Group, right-click the **RADIUS Default Group** node and choose **Add Administrator**. For information on filling in the details in the Administrator window, see Administrators).

For information on RADIUS Servers and RADIUS Server authentication parameters, see RADIUS Authentication.

5.1.3 Super Administrators and Other Administrator Groups

All Administrator groups are characterized by the permissions that they are granted to access different items (for example, Alert Settings, or Block and Warn messages). All administrators are automatically assigned the permissions of the group to which they belong.

A Super Administrator is a special category of Administrator. Super Administrators are not limited by access permission constraints. They have update permissions on all objects within all classes, and can see all the Management Console options for all user groups. Only Super Administrators can create administrator groups and add administrators to administrator groups.

By definition, all administrators in the Super Administrators group are Super Administrators, and the Super Administrator group comes with two predefined administrators: **support** and **admin**. Additional Super Administrators can be defined.

To create additional Administrator Groups, right-click the **Default Permissions** node and choose **Add Administrators Group**.

To edit the details of the Super Administrators Group or other administrator group, click **Edit**. After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

The window of the Super Administrator Group and other Administrator groups contains three tabs.

- **General** — For information on the fields in this tab, see Fields in the General Tab of Administrator Groups.

- **Permissions** — **Categories View** tab, and **Permissions – Grid View** tab. For information on using these tabs, see Access Permissions – Category View and Grid View

5.1.3.1 Fields in the General Tab of Administrator Groups

Administrator Groups Window – General Tab Fields

Field	Description
Group Name	Specify a descriptive name for the Administrators Group (protected field for the Super Administrators Group).
Notes	Use this field to add a free text description about the group.
Password expiration after *x* days check box	Number of days after which the administrators in this group are forced to replace the password.
Enforce secure password check box	Select this check box to force specified passwords to satisfy at least 3 of the following criteria: • must contain at least one uppercase alphabetic character (A-Z), • must contain at least one lowercase alphabetic character (a-z) • must contain at least one numeric character (0-9) • must contain at least one of the following characters !@#$%^&*()
Require password change on first login check box	Select this check box to force new administrators in the group to change the password on first login.

5.1.4 Administrators

Administrators in a group are automatically assigned the group's permissions (as adjusted). You can then adjust permission assignments for the administrator as needed.

The **Super Administrators** Group contains two pre-defined Administrators: **support** and **admin**.

Only Super Administrators can add administrators to a group.

- To add an administrator, right-click the group node in the tree and choose **Add Administrator**. The main window then displays the fields for defining the administrator's details.

- To delete an administrator, right-click the administrator and choose **Delete Administrator**.

To edit an Administrator's details, click **Edit**. After editing, click **Save**. To commit the changes, click .

The window for defining an Administrator contains three tabs:

- **General** tab — For information on the fields in this tab, see Fields in the General Tab of Administrators.

- **Permissions – Categories View** tab, and **Permissions – Grid View** tab. For information on using these tabs, see Access Permissions – Category View and Grid View

5.1.4.1 Fields in the General Tab of Administrators

Administrator Window – General Tab Fields

Field	Description
Administrator Name	Specify a name for the Administrator (this field is protected for the pre-defined Administrators — **support** and **admin**).
Notes	You can use this field to add a description about the administrator.
Email	Administrator's email address.
Master Policy	Master Policy assigned to the administrator. **Note**: This is relevant only if your site used Master Policy, and in this case, it is recommended that you NOT change the Use Default Setting value unless you want the administrator to use a different Master Policy than the site default.
Password / Confirm Password	Specify and confirm the password to be assigned to the Administrator.

5.1.5 Access Permissions – Category View and Grid View

This section contains the following topics:

- Concepts

- Fields in the Permissions - Categories View Tab

- Fields in the Permissions – Grid View Tab

5.1.5.1 Concepts

The following basic set of access permissions can be assigned. **Update**, **View**, and **None**. (These permissions are self-explanatory and require no further explanation.)

Every item for which permissions can be granted falls into one of two levels, and permissions are defined at both levels:

- **Category** — This is a high level item that generally contains lower level items (for example, Policies).

- **Sub-category** — This is a low-level, specific item, generally a part belonging to a class of items (for example, a URL List).

A previously mentioned, the windows for defining the Administrator Group details and Administrator details have two tabs for defining permissions:

- **Permissions – Categories View**

- **Permissions – Grid View**

The same tabs also appear in the Default Permissions window, though they cannot be edited there.

> **Important**: The information contained in both of these view tabs is exactly the same. Only the format is different, to allow you to choose the format that is easier for you to use when defining permission settings. This is discussed in greater detail in Permissions Tabs — Comparison of Categories and Grid View

In these tabs, for each item (high or low level), there are two permission fields: One field displays the default permission for this item, and the other displays a drop down list for changing the permission value of the item.

There is, however, another field in these tabs — a field representing a "container." To understand the concept of a container, consider the following example.

Example

An administrator duplicates a policy and modifies the Active Content List in the condition. When assigning permissions for the Active Content List, the following issues arise:

- The members of the Administrator's group should have Update permissions for this Active Content List.

- Whether other Administrator Groups should be allowed to view the Active Content List should depend on the Group (for example, only one other, specific Administrator Group should be allowed view the Active Content List).

- The Active Content List in the original Trustwave policy should not be assigned Update permissions.

Clearly, setting a single, context-independent permission value for the Active Content list is inadequate. Containers provide the solution.

SWG provides three type of containers:

- **SWG** — Contains the relevant predefined Trustwave items. In general, these can only be viewed, not updated.

- **My Group** — Used for setting permissions (generally Update) for the Administrator Group that created the object.

- **Other** — Used for setting permissions for Administrator Groups other than the one that created the object.

This Concepts section contains the following topics:

- Permissions Tabs — Comparison of Categories and Grid View

- Choosing Which Permissions Tab to Use

5.1.5.1.1 Permissions Tabs — Comparison of Categories and Grid View

As mentioned, the following two tabs used for defining/adjusting permissions contain the same information.

- Permissions – Categories View

- Permissions – Grid View

Their format, and even their field naming is different, but the information is identical.

Figure 1 (the Categories view) and Figure 2 (the Grid view) illustrate the different tabs.

Notice that despite their format differences, both tabs show basically the same information:

- HTTPS policies

- The Trustwave container within which are the two pre-defined Trustwave HTTPS policies

- The beginning of the My Group container for HTTPS policies

- Permissions for those policies (default and assigned)

The Categories View tab contains the following fields: Category, Sub Category, Objects Created by/Default Permissions, Objects/Override (default)/(new permission).
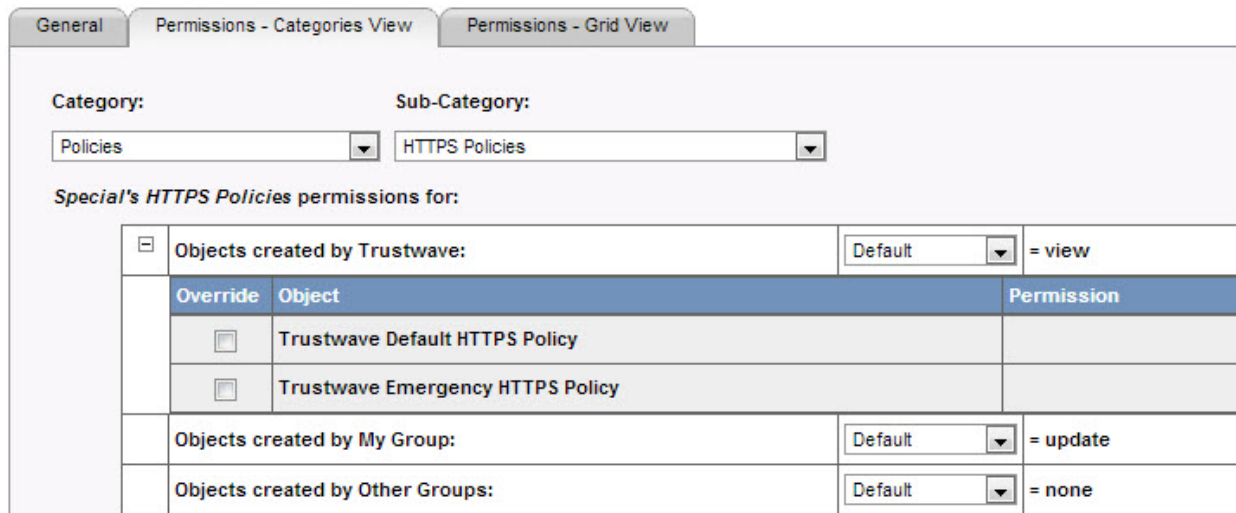
Figure 1: Permissions – Categories View

The Grid View tab contains the following fields: Classification, Owner, Object, Default (permissions), Access (permissions).

Figure 2: Permissions – Grid View tab

There is a direct correspondence to these fields.

> When working out the correspondence between these fields, you should ignore the Category field in the Categories view. The Category field has been added to the view only to make it easier to find the top level item that you want (in the Sub Category drop down list). The Category value (for example, Logs and Reports) cannot be assigned a permissions value.

The following table summarizes the relationship between the fields in the two views:

Corresponding Fields in the Permissions Categories and Grid Views

Field in Categories View	Field in Grid View	Additional information
Category	(None)	Purpose is to simplify search for definition.
Sub-Category	**Classification**	Top level in hierarchy.
Objects Created by:	**Owner**	Container type. When used, always consists of three types of containers (note that the wording for the containers labels varies slightly between the two views): • **SWG** — Contains objects that are pre-supplied by Trustwave. • **My Group** — Objects created by the Administrator's group. • **Other** — Used for assigning permissions to other administrator groups.
Object	**Object**	Lowest level in hierarchy. Used for assigning permissions for the object that override the permissions assigned to the type of object.

5.1.5.1.2 Choosing Which Permissions Tab to Use

As mentioned, you can use either tab, depending on which you find easier. The following paragraphs provide some information that might help you decide which tab to use.

Permissions – Categories View

The **Categories View** tab provides a relatively easy flow to display the objects you want to see. It displays a short list of high level categories (**Administration**, **Condition Elements**, **Logs and Reports**, **Policies**, **System Settings**, and **Users**) as a push-off point. You select a category, which then determines the contents of the Sub-Category drop down menu. Based on your sub-category selection, the list of Object types is displayed. You can expand an object type to display its objects.

Permissions – Grid View

The **Grid View** tab begins with a comprehensive list of Class items, in alphabetical order. You can expand any class item to reveal its lower level items. This view might be easier to use if you know exactly the name of the class item you are interested in, or if you do not know what category/subcategory to select in the Categories View screen.

5.1.5.2 Fields in the Permissions - Categories View Tab

Not all fields described in the table are displayed in the tab at all times. Which fields are displayed depends on the Category/SubCategory selection.

Fields in the Permissions – Categories View Tab

Field	Description
Category	Drop down list of categories to simplify the search for setting the definition.
Sub-Category	Top level in hierarchy of items.
***user*'s permission for *item* uses default (Currently *defaultpermission*) radio button**	Where: • ***user*** can be one of the following: **Default**, **RADIUS Default Group**, **Super Administrator**, **administrator** • ***item*** is the Sub-Category (or related) value • ***defaultpermission*** is the current default for the item Choose this radio button if the users should use the current default permission for this top level item.
***user*'s permission for *type* uses *permission*) radio button**	Where: • ***user*** can be one of the following: **Default**, **RADIUS Default Group**, **Super Administrator**, **administrator** • ***item*** is the Sub-Category (or related) value • ***permission*** is a drop down list from which you select a permission Choose this radio button (and select a permission) if the user should use a different permission than the default for this top level item.
***user*'s *item* permissions for:**	Where: • ***user*** can be one of the following: **Default**, **RADIUS Default Group**, **Super Administrator**, **administrator** • ***item*** is the Sub-Category (or related) value This message is displayed when the **Object Created by *xxx*** fields (described below) are displayed.
Objects Created by Trustwave:	For the particular item (sub-category), for objects pre-supplied by Trustwave, lists in the default permission and enables you to select a different default (in the accompanying fields described below).

Fields in the Permissions – Categories View Tab

Field	Description
permission drop down list	Use this field to select a different default for the Sub-category listed in parent **Objects created by ...** field. Valid values:
	Default — Use the default setting
	Update — Can make changes, create new objects, and so on.
	View — Can view classes/objects only
	None — Has no permissions to this object/class
= *permission*	Current (default) permission for the SubCategory. Valid values:
	Update — Can make changes, create new objects, and so on
	View — Can view classes/objects only
	None — Has no permissions to this object/class
expand/collapse icon	To override the defaults for specific objects in this SubCategory, expand the **Objects Created by ...** display to display a table of lower level objects in the SubCategory. In this table, you define the overrides.
Override check box	To override the default for the Object adjacent to this check box, select this check box.
Object	Object for which you will override (or not override) the default. The list of objects depends on the SubCategory, and which Objects By list.
Permission	Select the desired permission for the object (the drop down list is displayed for an object if you select its check box).
Objects Created by My Group:	Used for setting permissions (generally **Update**) for the Administrator Group that created the object, if defined. See the above descriptions of fields associated with **Objects Created by Trustwave:** (they work the same way).
Objects Created by Other Groups:	Used for setting permissions for Administrator Groups other than the one that created the object. See the above descriptions of fields associated with **Objects Created by Trustwave:** (they work the same way).

5.1.5.3 Fields in the Permissions – Grid View Tab

Fields in the Permissions – Grid View Tab

Field	Description
expand/collapse icon	Used to expand or collapse the list underneath.
Classification	Top level in hierarchy of items.
Owner	Type of "container" which holds the objects. The "container" type is determined by "who" created the objects. Valid values:
	SWG — This container is used for setting permissions for objects in the class that were pre-supplied by Trustwave.
	My Group — This container is used for setting permissions (generally **Update**) for the Administrator Group that created the objects in the class.
	Other — This container is used for setting permissions for Administrator Groups other than the one that created the object in the class.
Object	Object within a class
Default	Default Permissions which are granted when no other permissions have been defined. Valid values:
	Update — Can make changes, create new objects, and so on
	View — Can view classes/objects only
	None — Has no permissions to this object/class
Access	Sets the Access permission. Valid values:
	Default — Use the default setting
	Update — Can make changes, create new objects, and so on
	View — Can view classes/objects only
	None — Has no permissions to this object/class

5.2 System Settings

The **System Settings** menu enables you to configure the following:

- SWG Devices

- Scanning

- Mail Server

- Administrative Settings

- Digital Certificates

- License

- Debug Log

- GUI Log Level

5.2.1 SWG Devices

To display the SWG Devices tree (in the left pane), navigate to **Administration | System Settings | SWG Devices**. The main window displays details relevant to the node selected in the tree.

This section contains the following topics:

- Concepts

- Default Values

- Management Devices Group

- Default Devices Group and User-defined Device Groups

- Device IPs

- Log Server

- Policy Server

- Scanning Servers

- Access List

- High Availability

5.2.1.1 Concepts

This section contains the following topics:

- Devices and their Role as Servers

- Device Implementations

- Devices Tree and Device Groups

- Servers

Devices and their Role as Servers

The Devices tree lists the device IPs defined in the system. These devices are concerned with some combination of the following roles:

- Policy Server: An administration point for system configuration and security policy settings. The settings defined in the Policy Server are pushed to all Scanning Servers such that the system is always updated.

- Log Server: A short-term centralized repository for transactional information. The transactional information is generated by the Scanning Servers and queued in Log Relays, after which they are aggregated to the centralized repository. By default, the Log Server is installed together with the Policy Server.

- Scanning Servers: Scanning servers scan content and enforce the predefined policy for that content. **Note:** This document also interchangeably uses the term **Scanner** to refer to a Scanning Server. If you implement Trustwave's Mobile Security Client, a special instance of Scanner, called a **Cloud Scanner**, is utilized.

In addition, there is the Report Server which generates and distributes reports based on transactional information. By default, the Report Server is installed together with the Policy Server and does not have any configurable settings.

Device Implementations

For each device to function in the device role you assigned to it, you must define initial system settings for each device. For more information, see the *Secure Web Gateway Setup Guide*.

By default, SWG utilizes a single Policy Server, a single Log Server, and a single Scanning Server. Generally, the Policy Server and Log Server reside on the same device.

These default servers can be installed in either of the following configurations:

- **All-in-One** — The Policy Server, Log Server, and Scanning Server reside on the same device.

- **Policy Server** — The Policy Server and Log Server reside on the same device. The Scanning Server resides on a different device.

SWG supports High Availability implementation. To implement this feature, you add an additional device which will function as a failover Policy Server in the event that the active Policy Server fails. (SWG allows you to define only one active Policy Server, and if you implement High Availability, only one passive Policy Server to be used for fail over.)

> Implementation of High Availability requires that your primary (Active) Policy Server be on its own device, NOT on an All-In-one device.

You must implement at least one Scanning Server. In an All-in-One installation, that Scanner is on the same device as the Policy Server and Log Server; alternatively, it can be installed on a separate device.

Your site can deploy multiple local scanners, each on its own device. Multiple scanners are generally used with a load balancer to balance the workload.

Scanning Servers can be configured for local usage or Cloud usage. The Cloud Scanning Server performs the same actions as a local scanner, but is intended for cloud security. See Cloud (Hybrid Deployment) for more information.

Even if you do not add additional scanners, you must configure your local scanner.

Devices Tree and Device Groups

Device IPs are grouped under group nodes. The tree contains two predefined group nodes.

- **Management Devices Group node** — For a description, see Management Devices Group.

- **Default Devices Group** — For a description, see Default Devices Group and User-defined Device Groups.

You can define additional Device Groups.

The Devices tree also contains a **Default Values** node, under which are additional nodes for configuring default settings that can be applied to devices. For details, see Default Values.

Servers

Each device has its particular server(s) that play specific network roles.

The following types of Servers have nodes (located directly under *Device_IP* nodes).

- Log Server

- Policy Server

- Scanning Servers

5.2.1.2 Default Values

This section contains the following topics:

- Device General Settings

- Device Settings

The **Default Values** node (under the root **Devices** node) contains the following two subnodes that allow you to configure default values.

- **Device General Settings** — Contains a subnode for configuring default Access Lists. For more information, see Access List.

- **Device Settings** — Contains module subnodes for configuring default settings for scanners.

The **Default Values** node contains a single right-click option, **Reset all with default values**. This option enables you to reset the values for all access lists and all modules on all Scanning Servers with the default values defined in the Default configuration windows under the **Default Values** node.

5.2.1.2.1 Device General Settings

The **Device General Settings** node contains a single subnode: **Access List**. The Access List feature enables you to control access to specific IPs or IP ranges. For more information, see Access List.

5.2.1.2.2 Device Settings

Each Scanning Server node contains a number of module nodes for configuring settings relevant to the Scanning Server

The same set of module nodes appears beneath the **Device Settings** node (which is under the **Default Values** node). This set of nodes for configuring default settings for scanners.

Both sets of nodes are basically the same, and the displayed module window is basically the same in both locations. (One difference — the window for a scanner module displays its device IP; no device IP is displayed in window for the default module.)

It is recommended that you configure the default Device Settings first. Default Scanning Server settings are automatically applied to all Scanning Servers. You can then modify those default settings for specific scanners, as needed.

For a description of the module nodes under Device Settings (and Scanning Servers), as well as a description of their options, see Scanning Servers.

5.2.1.3 Management Devices Group

By default, the **Management Devices Group** contains a single device.

This device is used to hold the Policy Server and Log Server. Depending on the configuration, the device can also hold a Scanning Server.

The device is configured at time of installation and setup in either of the following configurations:

- **All-in-One device** — In this configuration, the device holds the Policy Server, the Log Server, and a Scanning Server.

- **Policy Server** — In this configuration, the device holds the Policy Server and Log Server, but Scanning Servers are installed on different devices in different groups.

(If you implement High Availability, the Management Devices Group will have one more device node, containing a passive Policy Server. For more information, see High Availability.)

The Management Devices Group window (accessed by selecting the **Management Devices Group** node) contains only one editable field:

- **Virtual IP** — This field is generally useful only if you implement High Availability. It enables you to specify a Virtual IP that will automatically resolve to your currently active Policy Server machine. If you define a virtual IP value, you can use this value for access regardless of whether SWG has failed over to the previously passive Policy Server machine.

You must click **Edit** before editing this field, and **Save** your changes when done. To commit the changes, click **Commit Changes** in the toolbar.

5.2.1.4 Default Devices Group and User-defined Device Groups

The **Default Devices Group** is a predefined group dedicated to holding Scanning Server devices. You can also define additional groups dedicated to scanning server devices.

If you do not have an **All-In-One** device, you must have at least one scanning server device defined either under the Default Devices Group or under a user-defined Devices group. You can add additional scanning servers to any of these groups according to your needs.

To add a user-defined device group for Scanning Servers, right-click the **Devices** (root) node, and select **Add Group**.

To **Edit** a device group's parameters, select the group node; then click **Edit** in the device group window.

To add a device for a Scanning Server, right-click the appropriate Device group and choose **Add Device**.

Device_IP nodes for the Scanning Server devices appear directly under the devices group to which they belong. For more information, see Device IPs and Scanning Servers.

After editing the device group, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

This section contains the following topics:

- Options of the Default and User-defined Device Groups

- Fields in the Default and User-defined Device Groups

- Move Devices Window

5.2.1.4.1 Options of the Default and User-defined Device Groups

The following table describes the options that are available in the tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option.

Default and User-defined Device Groups Options

Action	Description
Add Device	Adds a new device, for a Scanning Server.
Add Device by Range	Adds a new device, for a Scanning Server, in a specified IP Range.
Move Devices	Lets you move devices from one scanning server device group to another. Fore more information, see Move Devices Window
Delete Group	Deletes a scanner-type device group.

5.2.1.4.2 Fields in the Default and User-defined Device Groups

The Default Device Group and User Defined Device Groups contain two tabs and several fields above the tabs.

Default and User-defined Device Groups Fields Tabs and Fields

Field/Tab	Description
Groups Name	Name of the Scanning Server Group. Mandatory. Cannot be changed for the **Default Devices Group**.
Description	Free text optional description.
Commit Scheduling tab	Used for defining schedules for when configuration changes to the devices in this group should be applied (in addition to when you click the ![button] button). Click the radio button of the desired schedule type, and fill in any required parameters. **Note:** The specified times follow the Policy Server time, not the local client time.
Immediately upon commit	Commits the changes only when you click the **Commit** button (default).
In ...	For specifying a set interval of *#* of days, at a specific time (*hh:mm*).
On ...	For specifying specific days of the week at a specific time (*hh:mm*)
On day ...	For specifying a specific day of the month at a specific time (*hh:mm*)

Default and User-defined Device Groups Fields Tabs and Fields

Field/Tab	Description
Update Scheduling tab	Used for defining schedules for when security updates to devices in this group should be applied. Select the radio button of the desired schedule type, and fill in any required parameters.
	Note: The specified times follow Policy Server time, not local client time.
Immediately	Applies the updates as soon as they appear (default).
At ...	Specify the time (hh:mm) at which the updates should start. In the **Update Window** box, specify the maximum number of minutes after the specified start time that updating can still be started. (If that window of opportunity passes before updating begins, SWG will try to apply the updates on the next day at the specified time.)

5.2.1.4.3 Move Devices Window

The **Move Devices** window lets you move Scanning Server devices from one group to another. Display the window by right-clicking the node FROM WHICH you want to move the Servers (either the **Default Device Group** node or a **user-defined Devices group** node), and then selecting **Move Devices**.

The window displays a check box list of devices that currently reside under the clicked node. The window also contains a **To** selection field that lets you select the target device group.

5.2.1.5 Device IPs

Device IP nodes identify devices that are part of the SWG configuration.

They appear directly under the relevant Group nodes (**Management Default Group**, **Default Devices Group**, and any user-defined Device groups) in the Devices tree.

Directly under Device IP nodes are nodes that identify the particular Servers (network roles) that are implemented on that device (for information, see Servers.

To display a window for configuring device-related parameters, select the *device_IP* node. This window contains several tabs. It also contains fields that are outside the tabs.

To edit the field in the window, click **Edit**. Then **Save** the changes. To commit the changes, click
Commit Changes in the toolbar.

This section contains the following topics:

- Options of Device IP Nodes

- Fields in the Device IP Window

- Cloud Scanner Node Details

5.2.1.5.1 Options of Device IP Nodes

The following table describes the options that are available in the tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option.

<p style="text-align:center">Device IP Node Options</p>

Action	Description / Node Where Available
Delete Device	Deletes the device.
Set As Access List Default	Replaces the default Access List settings with the Access List settings belonging to the particular device (that is, it makes them the new defaults).
Apply Default Access List Values	Applies the default Access List settings to the Access List of the particular device.

5.2.1.5.2 Fields in the Device IP Window

This section contains the following topics

- Device IP Fields Above The Tabs

- Status Tab

- Access List Tab

- Advanced Tab — For Policy Server or All In One devices

5.2.1.5.3 Device IP Fields Above The Tabs

The following Device IP definition fields appear outside of the tabs of the Device IP window.

Device IP Window – Fields Outside the Tabs

Field	Description
Device IP	IP address of the current device. Mandatory
Private IP	Private IP address of the device.

Type	• The device in the **Management Devices Group** can be one of the following:
	
	  • Policy Server
	  • All in One
	• For devices in the **Default Devices Group** or a user-defined Devices group (Scanning Server devices), you can choose between the following:
	
	  • Scanning Server (for local scanners)
	  • Cloud Scanning Server

Description	Description of the device.

5.2.1.5.4 Status Tab

The **Status** tab provides status information on the device such as connection and activity status.

Device IP Status Window – Status Tab Fields

Field	Description
Version	The SWG version number
Sync Status	Indicates whether the Device is synchronized with the Policy Server.
Connection Status	Indicates if the device is available (**Active**).
Committing Status	Indicates whether the device is undergoing a **Preparing to Commit** status, **Committing Changes** status, or is Stable.
Last Connection Time	Indicates the last time this device was connected to the Policy Server.
Next Commit Time	Indicates the time of the next automatically scheduled Commit. This is for dedicated scanner devices only.
Device Role	Displays the roles which belong to the device.
Activity Status	Defines whether the Role is **Active**.

5.2.1.5.5 Access List Tab

The fields in the Access List Tab are the same as the fields in the Default Access List node. For information and instructions regarding Access Lists, see Access List.

5.2.1.5.6 Advanced Tab

The Device IP **Advanced** tab allows administrators to enable the Reverse DNS lookup option, to determine the domain name that is associated with a given IP address (using DNS). In doing so, the administrator may prevent users from bypassing URL filtering security measures.

Selecting this check box runs the reverse lookup prior to writing log entries, which results in log entries listing the URL name rather than the IP address.

Click **Edit** and select the **Enable Reverse DNS** check box.

Then **Save** the changes. To commit the changes, click **Commit Changes** in the toolbar.

5.2.1.5.7 Cloud Scanner Node Details

The following Device IP definition fields appear outside of the tabs of the Device IP window.

Device IP Window – Fields Outside the Tabs

Field	Description
Device IP	IP address of the current device. Mandatory
Private IP	Private IP address of the device.

Type	• The device in the **Management Devices Group** can be one of the following:
	  • Policy Server
	  • All in One
	• For devices in the **Default Devices Group** or a user-defined Devices group (Scanning Server devices), you can choose between the following:
	  • Scanning Server (for local scanners)
	  • Cloud Scanning Server

Description	Description of the device.

5.2.1.5.8 Cloud Scanner Node Status Tab

The **Status** tab provides status information on the device such as connection and activity status.

Device IP Status Window – Status Tab Fields

Field	Description
Version	The SWG version number
Sync Status	Indicates whether the Device is synchronized with the Policy Server.
Connection Status	Indicates if the device is available (**Active**).
Committing Status	Indicates whether the device is undergoing a **Preparing to Commit** status, **Committing Changes** status, or is Stable.

Device IP Status Window – Status Tab Fields

Field	Description
Last Connection Time	Indicates the last time this device was connected to the Policy Server.
Next Commit Time	Indicates the time of the next automatically scheduled Commit. This is for dedicated scanner devices only.
Device Role	Displays the roles which belong to the device.
Activity Status	Defines whether the Role is **Active**.

5.2.1.5.9 Cloud Scanner Node Access List Tab

The fields in the Access List Tab are the same as the fields in the Default Access List node. For information and instructions regarding Access Lists, see Access List.

5.2.1.6 Log Server

A lone Log Server always resides on the Policy Server machine. (The Log server node is located under the IP node of the machine that holds the Policy Server.)

The Log Server contains the following module:

- Log Properties

5.2.1.6.1 Log Properties

The **Log Properties** node is located under the **Log Server** node.

Log Relays resident on each device receive the following information types, which are then collected by the Log Server, and then routed to the appropriate locations:

- Scanning Server (Web) messages

- System Log messages

- Audit Messages

By default, the Log Server sends this information to the internal Logs and Reports databases. It also routes information to the Policy Server for viewing in the Log Viewer.

Depending on the Logging Policy definition, the Log Server can also:

- send Scanner logs, System logs and/or Audit information to a Syslog server.

- and/or send Scanner information to an Archive (zip) file.

Before information can be sent to the non-default, external files, you must specify the location of the files and configure several other parameters.

You perform this configuration in the Log Properties window, which you display by selecting the **Log Properties** node (under the Log Server node, which is under the default IP node under the Management Devices Group).

The Log Properties window contains the following tabs.

- Collect Logs From Tab

- Syslog Target Tab

- Syslog Fields Tab

- Log Archiving Tab

- Fields in the Log Archiving Tab

- Web Log Retention Tab

To edit the Log Properties window, click **Edit**. When done editing the tabs, click **Save**. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

Collect Logs From Tab

By default, the Log server collects the information from each scanner every few seconds and provides information to the Policy Server.

However, you can define specific collection times for each scanner. This can facilitate more efficient use of available bandwidth. It is also useful in a distributed system in which scanning devices are located in different time zones or are reachable via slow communication lines.

- This tab is relevant only if your site is using multiple Scanning Servers.

- Scheduling time frames only apply to Web log messages collected based on Logging Policy. Other types of logs are still retrieved every few seconds.

You can also deactivate specific Log Relays.

Log Properties Window – Collect Logs From Tab Fields

Field	Description
Schedule column: ⊞	Click to display the following scheduling definition parameters for the device listed in the **Device IP** field.
From Time / To Time	Time range during which the Log Server can collect logs from the Log Relay
✚	Click this icon to define another time range.
Active check box	When selected (default), the Log Relay on the device is activated. To deactivate the Log Relay, clear the check box.
Device IP	IP of the Scanning Server or which the Log Relay parameters are being defined (Protected field).
Secured	Select this check box if the messages sent by the Log Relay should be encrypted for security.

Syslog Target Tab

The **Syslog Targets** tab of the Log Properties screen lets you define which types of Log messages the Log Server should send to designated Syslog server facilities. The following types can be sent:

- **System Log Messages**

- **Scanner Messages** — The Log Server will send log information generated by those Log Rules that have the **Syslog** check box selected as a log destination.

- **Audit Messages** — The Log Server will send Audit messages (all changes made or actions taken from the Management Console).

A different Syslog format (and therefore a different Syslog) is needed for each of these message types.

The **Syslog Targets** tab contains a check box for activating this Syslog functionality. It also contains two tables:

- In the upper table, you configure a Syslog "Facility" for each type of message that should be sent to a Syslog, The Facility contains connection parameters (primary/secondary IPs and ports) for the Syslog.

- In the lower table, you identify which message type(s) should be sent to a Syslog, and which Facility contains the connection parameters for that Syslog.

<div align="center">Log Properties Window – Syslog Target Tab Fields</div>

Field Name	Description
Enable Log	To activate this Syslog functionality, ensure that this check box is selected.

Log Properties Window – Syslog Target Tab Fields

Field Name	Description
Upper table	
Facility	Label used to distinguish between the different classes of messages. When filling in the parameters, begin with Facility 1 and continue in sequence.
Facility Mode	Use the Facility Mode field to differentiate Trustwave logs from each other and from other platforms' logs on the remote Syslog server, by assigning (selecting) a different value for each facility. Select one facility mode from the drop down list which is operational for all message types.
Primary IP	Primary Syslog Server target address.
Primary Protocol	Primary traffic protocol: UDP or TCP
Primary Port	Primary port to which the Syslog messages will be sent.
Secondary IP	Secondary Syslog Server target address (optional).
Secondary Protocol	Secondary traffic protocol: UDP or TCP
Secondary Port	Secondary port to which the Syslog messages will be sent (optional).

Log Properties Window – Syslog Target Tab Fields

Field Name	Description
Lower table	Contains two columns: • **Message Type**, for checking which message types should be sent to a Syslog. • **Facility**, for selecting which Facility definition in the upper table contains the Syslog connection parameters for that message type.
Message Type	Select the check boxes of the message types to be sent to a Syslog.
Send System Log Messages	Select this check box if System Log messages should be sent to the Syslog server facility.
Send Scanner Messages	Select this check box if Weblog messages should be sent to the Syslog server facility.
Send Audit Messages	Select this check box if Audit messages should be sent to the Syslog server facility.
Facility	Select the Facility defined in the upper table that applies to the checked Message type.

Configure Trustwave ports to work with ArcSight ports accordingly.

Syslog Fields Tab

The **Syslog Fields** tab contains configuration options for scanner syslog messages. This tab enables you to select the transaction field names required for scanner messages, such as Client IP or User ID.

Log Properties Window – Syslog Fields Tab Fields

Field	Description
Syslog Format	Format that will be used to present information to the user: • **Legacy** — Empty fields will not be shown in Syslog messages. • **Standard** — Empty fields will be shown in Syslog messages • **ArcSight** — For sites using the external **ArcSight** server. **Note:** If you choose this option, you must configure the IP and Port fields in the **Syslog Targets** tab with the IP and Port of the **ArcSight** server.

Log Properties Window – Syslog Fields Tab Fields

Field	Description
Select/Deselect All	Select this check box to select or deselect the transaction fields required for scanning Syslog messages.
Name	Syslog transaction fields. Ensure that the fields that should be logged are checked.
Prefix	The prefix of the syslog transaction item when listed in the final syslog message. ArcSight prefixes are not editable.

This tab is relevant and mandatory only if you are sending Scanner messages to the Syslog.

Note also that the **Send To: Syslog** check box must be selected in the Logging Policy rules whose logging information is to be sent to Syslog. If a rule's **Syslog** check box is not selected, its logging information is not sent to Syslog.

Log Archiving Tab

You can send Web Log Information from the Scanner to an external Archive location and schedule when the archives should be sent. (**Note:** You must also ensure that the **Send To: Archive** check box in the relevant Logging Policy rules is selected, or the logging information of those rules will not be sent to Archive.)

The Log Archiving tab of the Log Properties window is used to define the archive location and scheduling.

The Log Archiving feature can send the information in either of two formats: Basic or Extended.

• **Extended** — Includes all available information on each logged transaction. Required when working with Trustwave Security Reporter.

In addition to the SWG Internal Reporting Tool, Trustwave offers comprehensive support for integration with the Security Reporter. The Security Reporter (SR) is an advanced external reporter that offers organizational, security, and productivity reports. The SR option allows for sending log archives to both the Security Reporter and to an external storage location for archival purposes.

• **Basic** — Includes only a subset of details on each logged transaction.

The information is sent in Gzip file format and is displayed with comma separated values. You can then import this information into an external database for viewing or running reports.

To send the log archives to an external storage location, you must select the Connection Method (the method to be used to connect to the required location). Your selected Connection Method impacts the **Archive Location**, **User to connect with**, and **Password** values that you can define.

After defining the Archive details, you can test them before saving the definition.

Fields in the Log Archiving Tab

The following table describes the fields in the Log Archiving tab.

Log Properties Window – Log Archiving Tab Fields

Field	Description
Enable Log check box	To activate this Archiving functionality, ensure that this check box is selected.
Log Archiving Location table	Define the details of the Archive files in this area.
✚	Select this icon to add the details of an Archive file.
Enable	Select the check box to enable archiving to this file.
Connection Method	Select the method that the Log Server should use to connect to the Archive location: • **FTP** — Connect using regular File Transfer Protocol. • **FTP Passive** — Connect using File Transfer Protocol (there is a firewall located between the Policy Server and the remote FTP site). • **Samba** — Connect using Server Message Block (SMB) communication protocol.
Archive Location User Name Password	The details for these fields depend on the selected Connection Method. For a description of these details, see Archive Location Format, User Name and Password.
Archive Format	Select the Archive Format: • **Extended** — Includes all available information on each logged transaction. Required when working with Trustwave Security Reporter. • **Basic** — Includes only a subset of details on each logged transaction. For more information, see Data Items Logged in Basic and Extended Formats.
Test location settings on next save check box	To have the Archive location tested when you save the definition, ensure this check box is selected; otherwise, ensure that the check box is cleared. If you test the archive location, an attempt is made to send a test file to the archive location. If the attempt fails, a message pops up. If the operation is successful, the message **Archiving Operation Succeeded** displays in the bar on the bottom left of the screen.
Archive Now button	Click this button after you click **Save**, to perform immediate archiving. The System log should indicate the results of the test.

Log Properties Window – Log Archiving Tab Fields

Field	Description
Log Archive Scheduling	Defines a time for automatic Archive. You can choose to send the data to the archive location either at a fixed time every day or at a specified interval, as required, using either of the following formats
Run Daily at *time*	Perform archiving at the specified time (in **hour: minute** format)
Run every # hours and # minutes	Perform archiving at the specified intervals (after every # hours and minutes)

Archive Location Format, User Name and Password

Archive Location, User Name, and Password Details

Connection Method	Archive Location Format, User Name and Password
FTP, FTP Passive, or SFTP	**Archive Location** format is: • For **FTP** or **FTP Passive**: <server_ip_address>**/dir** (for example, 10.194.5.104/Sarah_FTP) • For **SFTP**: <server_ip_address> (for example, 10.194.5.104/). **User to connect with** is the user name used when connecting to the Archive Location. **Password** should be the password used by the above user.
Samba	**Archive Location** must include the server IP address and directory for your selected location, in the following format: **//**<server_ip_address>**/dir**, (for example, //192.168.1.10/ archive.) **User to connect with** must include the workgroup name and the user name used when connecting to the Archive Location, in the following format: workgroup/user, for example, marketing/nicole. **Password** should be the password used by the above user.

Data Items Logged in Basic and Extended Formats

This table lists the data items that are logged in the Extended format, in the Basic format, and in both formats. The format in cases is `<field value="data_item"/>`

The data items listed in the **Basic Only** column actually correspond to data items in the **Extended Only** column. By contrast, the **Extended Only** column has items without corresponding values in the **Basic Only** column.

Data Items By Format

Common Data Fields	Extended Only	Basic Only
tran_time	user_id	name
tran_id	file_name	block_reason
client_ip	policy_id	policy_name
domain_user_name	identification_policy_id	transaction_size
user_domain	https_policy_id	rule_name
url	kaspersky_virus_name	rule_description
protocol	sophos_virus_name	action
scanning_server_ip	mcafee_virus_name	true_content_type
xray	transaction_size	url_category
	HTMLRepaired	vad
	activex_name	albb
	action_gid	
	admin_group	
	cache_hit	
	destination_ip	
	http_method	
	response_status	

Web Log Retention Tab

Transactions displayed in reports will be retained according to the defined number of weeks (above), not including the current week.

Fields in the Log Retention Tab

<div align="center">Log Retention Tab Fields</div>

Field	Description
Enable Log Retention check box	To activate use of the value defined in this tab, select this check box (otherwise the retention value will be ignored).
Retention period	Specify the number of weeks logs should be retained. **Note**: Logs might be deleted sooner if disk space limits are reached.

5.2.1.7 Policy Server

The Policy Server is an administration point for system configuration and security policy settings. The settings defined in the Policy Server are pushed to all Scanning Servers such that the system is always updated.

SWG always has one Policy Server (unless High Availability is implemented, in which case a second, passive Policy Server is added as a different device).

The node for this Policy Server always appears under the **IP** device node in the **Management Devices Group** node. It has no right-click commands and cannot be deleted or edited.

It does contain the following module subnodes:

- System Updates
- RADIUS Authentication
- Dashboard

5.2.1.7.1 System Updates

Normally, when you configure automatic update of Scanning Servers with the latest SWG updates, all Scanning Servers are updated at once.

However, the System Updates node lets you choose to update selected scanning servers with the latest Operating System update instead of sending the update to all the scanning servers at the same time. This ensures greater system stability and provides you greater control over the individual Scanning servers in your configuration.

This feature is also useful when updating the Policy Server operating system in a High Availability configuration. In this scenario, some scanning servers can be left untouched, so that if the Update fails, the Policy Server will still be able to control the selected Scanning Servers.

All scanning servers will continue to function normally and logs will be retrieved from all of them; however they will not receive security updates or configuration changes.

- Policy Servers are only able to configure and send security updates to Scanning Servers which have the same Trustwave Operating System. Any scanning server which has a different Trustwave Operating System update to the Active Policy Server will have their corresponding icon displayed in yellow.

- Scanning Server Trustwave Operating System Updates do not apply to Maintenance or Hot Fix releases.

To edit the System Updates screen:

1. Click **Edit**.

2. Select **Update selected Scanning Servers** and select the Scanning Servers in your configuration that should be updated. (Alternatively, **Select All**, and clear any Scanning Servers that should not be updated.

5.2.1.7.2 RADIUS Authentication

Trustwave Secure Gateway system allows multiple administrators to manage the system at once.

In addition to manually adding administrators to the system, you can connect to a RADIUS server for authentication using an external Users database.

Connecting to the RADIUS server simplifies the process for the system administrator to grant access to the system to new administrators by using already-defined users instead of defining new Trustwave administrators.

The RADIUS Authentication Screen (accessed by selecting the **RADIUS Authentication** node under the **Policy Server** node) lets you select the Authentication method and specify required parameters including RADIUS Server connection parameters.

You must click **Edit** before editing the fields in the screen, and click **Save** when you are done. To commit the changes, click **Commit Changes** in the toolbar.

To connect to the RADIUS Server, ensure that you select the Active check box in the screen. SWG will then connect you after you Save the edits and commit the changes.

To ensure that the process runs efficiently, it is highly recommended to use NTP synchronization.

Fields in the RADIUS Authentication Screen

RADIUS Authentication Screen Fields

Field Name	Description
Active	Selecting this check box activates RADIUS authentication mode.
Authentication Method	Defines which authentication method should be used while authenticating administrator credentials.
Primary / Secondary Authentication Host	Primary/Secondary server name or IP address.
Port	Defines the communication port between client and server.
Shared Secret	Pre-shared password phrase used to authenticate against the RADIUS server.
Retry Limit	Maximum number of attempts to authenticate.
Retry Interval	Defines the interval, in seconds, between attempts.

5.2.1.7.3 Dashboard

The Dashboard window (accessed by selecting the **Dashboard** node under the **Policy Server** node) displays a single field: The **Enable Dashboard** check box.

Selecting/clearing this check box enables/prevents display of the Dashboard Console (described in Dashboard).

Click **Edit** to activate the window. After selecting/clearing the Dashboard check box, click **Save**.

To confirm the results (i.e., to see if the Dashboard display is enabled or disabled), click on the toolbar.

5.2.1.8 Scanning Servers

The **Scanning Server** is responsible for analyzing and checking all content passing through the system in accordance with the Security Rules.

SWG lets you employ as many Scanning Servers as needed (one per device).

To add a device for a Scanning Server, right-click the appropriate Device group and choose **Add Device**.

Scanning Server nodes are always located under *<device_id>* nodes. Note the following:

- If an **All-in-One** device is configured, a Scanning Server resides on that device in the **Management Devices Group**.

- If you do not employ an All-in-One device, at least one Scanning Server must reside in either the **Default Devices Group** or in a user-defined Device group.

- All other Scanning Servers that you add can be placed in any combination of the Default Devices Group and/or user-defined Device groups.

No definition window is displayed when you select a Scanning Server node. Instead, underneath each Scanning Server node is a set of module subnodes, which display definition windows. (There are, however, options that you can perform on Scanning Server nodes.)

The same set of module subnodes appears below each **Scanning Serve**r node. Furthermore, the same module subnodes appear under the **Default Settings** node (which is located under the **Default Values** node).

Using the options, you can apply the default settings for a module to a module on a Scanning Server, and use the settings of a module on a Scanning Server to replace the default settings.

For On-premise Scanning Servers and Cloud Scanning Servers, different Scanning Server nodes are available. The following table describes the available Scanning Server nodes.

Scanning Server Nodes

On-premise Scanning Servers	Cloud Scanning Servers
General Module	General Module
Authentication Module	Authentication Module
Cache Module	Cache Module
FTP	HTTP Module
HTTP Module	HTTPS Module
HTTPS Module	ICAP Client Module
ICAP Service Module	
ICAP Client Module	
WCCP Module	

This section contains the following topics.

Each of the following topics, except the first topic, describes a module under the Scanning Server.

- Options Available on Scanning Server Nodes

- Options on Modules Under Scanning Servers/Default Settings

- General Module

- Authentication Module

- Cache Module

- FTP

- HTTP Module

- HTTPS Module

- ICAP Service Module

- ICAP Client Module

- WCCP Module

5.2.1.8.1 Options Available on Scanning Server Nodes

The following table describes the options that are available in the tree. Click an action icon on the left of the tree or right-click the tree node and select a menu option.

Scanning Server Options

Option	Description / Node Where Available
Restart Scanner	Restarts the Scanning Server.
Set As Default	Replaces the current default values for all modules in the Default Settings with the module values from the Scanning Server where the action was performed.
Apply Default Values	Applies the default values to the modules under the Scanning Server where the action is performed.

5.2.1.8.2 Options on Modules Under Scanning Servers/Default Settings

The following table describes the options that can be applied to individual module nodes under the **Default Settings** node or under **Scanning Server** nodes.

> For options that apply to all module nodes (rather than individual module nodes) under Scanning Servers, see Options Available on Scanning Server Nodes.
>
> (There are no options that apply to all module nodes (rather than individual module nodes) under Default Settings.)

Scanning Servers – Default Setting Options

Option	Description / Node Where Available
The following option is only available for each module listed the Device Settings node	
Reset all *module_name* modules with default values	Resets all modules of type *module-name* (which are located under Scanning Server nodes) with the default values defined for that module type under Device Settings.
The following options are available for each module listed under a Scanning Server node	
Set As Default	Replaces the current default values for the particular module type with the values of that module type taken from the Scanning Server where the action is performed.

Option	Description / Node Where Available
Apply Default Values	Applies the default values of the module type to the particular module under the Scanning Server where the action is performed.
The following option is only available for the Cache module, under both the Default Settings and a Scanning Server node	
Manage Cache Content	Enables deletion of a single URL and the flushing the cache.
The following options are only available for the HTTPS module, under both the Default Settings and a Scanning Server node	
Import Certificate	Enables Certificate import.
Generate Certificate	Generate a Certificate.
Export Certificate	Enables Certificate export.

5.2.1.8.3 General Module

The **General** module window lets you configure general settings for the device. It contains the following tabs:

- Device Policies Tab

- Downloads Tab

- Timeouts Tab

- Transparent Proxy Mode Tab

To edit the General Module window, click **Edit** in the right pane. After editing all (or any) tabs, click **Save**.

To commit the changes, click **Commit Changes** in the toolbar.

5.2.1.8.4 Device Policies Tab

In the **Device Policies** tab, you select the policies (of specific types) to be associated with this particular Scanning Server. The following table identifies, and provides links to detailed descriptions of, those policy types.

To change the assignment for a given policy type, select the desired policy from the drop down list.

General Module Window – Device Policies Tab Policy Types

Policy Type	Description
Identification Policy	Identification Policy defines whether and how the end-user will be identified or authenticated by the system.
Device Logging Policy	Device Logging Policy deals with the logging of transaction data for this specific Device IP.
Upstream Proxy Policy	Upstream Proxy Policy defines upstream proxy settings for traffic scanned by the SWG system.
ICAP Request and Response Modification Policies	ICAP Policies identify the ICAP Service Groups from which SWG can request ICAP Services, and defines behavior in case of an error.
Caching Policy	Caching policy defines when caching should be performed. Note: Caching Policy is relevant only if Caching is licensed (and enabled).

5.2.1.8.5 Downloads Tab

The **Downloads** tab lets you to configure the maximum scannable file size (in megabytes), for downloaded files, and for files uploaded via the proxy.

5.2.1.8.6 Timeouts Tab

The SWG system acts as a Proxy device which handles connections coming from the client to the server. This tab is used for setting the maximum time delays in communications between the client and server before it is judged a timeout:

It is highly recommended that you not modify the default timeout settings.

- **Client Side Timeout** — Maximum time delay (in seconds) between consecutive requests within the client-proxy connection.

- **Server Side Timeout** — Maximum time delay (in seconds) between consecutive content pieces received from server.

5.2.1.8.7 Transparent Proxy Mode Tab

When configuring Scanning Servers, you can enable the SWG appliance to work in Transparent Proxy mode. This is useful for checking content passing through specific FTP, HTTP and/or HTTPS ports.

In Transparent proxy mode, FTP, HTTP, and HTTPs requests can be transparently intercepted by the appliance and passed on to the server (Web or FTP).

When multiple scanning servers are used, a layer 4 load balancer appliance, or a WCCP enabled router or switch should redirect the Web and FTP traffic to the scanning servers using transparency.

Transparency in SWG works at the IP layer. Traffic must be routed to the SWG appliance in order for it to be scanned. For example, the SWG scanning server could be specified as the default gateway for client machines.

The Transparent Proxy Mode tab contains an Enable check box, and separate areas for FTP, HTTPS, and HTTP, where you can identify the port ranges (From and To ports) where Transparent Proxy should be implemented, Once enabled, traffic destined for the specified ports only are scanned; traffic on other ports will be passed through.

- Selecting the Enable Transparent Proxy check box sets (changes) the Authentication Retention Method (in the Authentication Module) to IP Caching, which authenticates only the first transaction from the IP address (and treats the remaining transactions from that address as already authenticated).

- If traffic exists on the network using non-standard port numbers, it is possible to add additional port numbers for scanning. For example, if there is HTTP traffic on Port 81, it is treated as HTTP and scanned by SWG.

General Module Window – Transparency Proxy Mode Policy Tab Fields

Field	Description
Enable Transparent Proxy Mode check box	Ensure that this check box is selected to enable requests to be intercepted in Transparent Proxy Mode.
Protocol sections	Fill in the fields in the following sections, as needed, to implement Transparent Proxy mode on requests received using that protocol: **FTP**, **HTTP**, and/or **HTTPS**
Fields and buttons in the areas	
➕	Click this button to add an IP Range definition line.
From IP	Lowest IP in the range.
To IP	Highest IP in the range.
📋	To delete an IP range, click this icon and choose **Delete Row**.
Extract Hostname from Certificate (HTTPS area only)	Select this check box to extract the hostname from the certificate. (If the hostname is needed for other purposes, such as URL categorization, this is the only way that the hostname can be determined in Transparent Proxy Mode.)

5.2.1.8.8 Authentication Module

The **Authentication** module window lets you configure Authentication settings for the device.

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

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

The window contains an Enable check box, and the following tabs:

- Configuration Tab

- Advanced Tab

To edit the tabs of the **Authentication** module window, click **Edit**, and then ensure that the **Enable**

Authentication check box is selected. After editing, click **Save**. To commit the changes, click
Commit Changes in the toolbar.

Before defining Authentication parameters for a Scanning Server, ensure that you:

- Created a Realm. For more information, see Realm.

- Defined/customized an Authentication-type Identification Policy. For more information, see Identification Policy.

Configuration Tab

The **Configuration** tab provides fields for selecting and configuring the **Authentication Retention method**. One of the methods allows authenticated user credentials to be cached, to reduce the number of authentication sessions.

The following table describes the fields of this tab, Choose the Authentication Retention method, and then fill in any necessary parameters.

Authentication Module – Authentication Tab Fields

Field	Description
No Retention	Select this method if the Scanning server should not retain authentication data but should instead request authentication for each call. **Note:** *This method is not a valid option if the Scanning Server is configured to work in* ***Transparent Proxy Mode***.
IP caching	Selected this method if, during the session, the Scanning server should only authenticate the first transaction from an IP address (and treat the remaining transactions from that address as already authenticated). In the **timeout** field, set how many seconds (1-600) the authentication data should be kept.
Cookie	Select this method if, during the session, the Scanning Server should perform authentication for different Web sites. Then do the following: • If the Cookie should be encrypted, select the **Use Encryption** check box (an encryption key will be auto-generated and used by the Scanning Server). • If the cookie should be retained for the duration of the **Timeout** interval, select the **Persistent** check box, and set the **Timeout** (in seconds). **Note:** This method is the default when the system is installed; it is also mandatory when the Scanning Server is working in Transparent Proxy Mode (for more information, see Transparent Proxy Mode Tab in the General Module).

Advanced Tab

The **Advanced** tab enables advanced configuration of the required authentication settings. The following table describes the fields in this tab:

Authentication Module – Advanced Tab Fields

Field		Description
Enable Challenge Token Reuse (NTLM Settings) check box		A client authenticating with a proxy is provided with a Challenge Token (a random token that must be generated each time the NTLM protocol is performed).
		To set NTLM Settings to enable token reuse: Select this check box, and then fill in the accompanying fields. (Note that this option decreases the system security level.)
	Random Challenge Token reuse number	Specify the number of times a Challenge Token can be reused before a new random token is generated. (The higher the value, the greater the savings in authentication time and proxy resources, but the weaker the security level.)
	Challenge Token Lifetime (in seconds)	Specify the maximum number of seconds a Challenge Token can be stored for reuse before it must be replaced.
Realm Connection to Authentication Servers		Fill in the following parameters to set the time-out and retry values for situations where the Realm does not respond to the Scanning Server requests for authentication.
	Connection Timeout	Set the time-out, in seconds, before the Scanning Server considers the Realm as not in service.
	Try Reconnect After	Set the time-out, in seconds, before the Scanning Server re-tries to connect to the Realm.
Transparent Authentication		If the Scanning Server is configured to work in Transparent Proxy mode, fill in the following parameters:
	Virtual Redirection Hostname	Specify the host name to which browsers in the system should be redirected. (Note that this host name does not have to be a real host name, but it must be resolvable by the DNS.)
		It is recommended to use only the host name and not a FQDN in order to prevent a user and password popup window.
	Virtual Redirection Port	Specify the TCP port number to be used for redirection.
Replace Domain With		Specify the domain that SWG should use to replace erroneously-specified "domains" (for example, if the user specified a computer name instead of a domain name).

Authentication Module – Advanced Tab Fields

Field	Description
Forward Upstream Proxy Authentication check box	Select this check box if an upstream proxy can and should authenticate users through the Secure Web Gateway system. In this case, Secure Web Gateway will not perform authentication, but will instead forward proxy authentication from the downstream client.

5.2.1.8.9 Cache Module

Caching stores downloaded content, thereby eliminating the need to reload identical content for each user's subsequent request.

Delivering content from a local cache accelerates content delivery to end-users. It also frees up the bandwidth that would be required to download multiple copies of the same object. As a result, the organization's applications run more efficiently.

Caching is done by evaluating HTTP headers to determine whether to store the Web content.

The **Cache** module window lets you enable caching, and set the maximum caching object size on the disk.

- Caching requires a separate license.
- Caching Policy is set per device, and applied to all users browsing through the device.
- To avoid situations where the secured content of one user is displayed to another user, HTTPS content is not cached.

To enable caching, ensure that the **Enable Cache** check box is selected. Then, in the **Maximum Object Size** field, set the maximum size of a single object that SWG caches.

For more information, see Flushing (Deleting) the Cache.

Flushing (Deleting) the Cache

Flushing the cache deletes the contents of the cache. The Flush Cache operation enables you to alternatively delete a single URL.

To flush the cache, right-click the **Cache** module node, and choose **Flush Cache**.

Important: Flushing the cache terminates all existing connections. Therefore, although you can flush the cache at any time, exercise caution before deciding to do so. You should NOT perform this operation as part of day-to-day maintenance.

5.2.1.8.10 FTP

The **FTP** module window lets you configure the File Transfer Protocol settings for the device. The window contains an Enable check box, and the following tabs:

- FTP Service Tab

- Upstream Proxy

- Allowed Server Ports

To edit the tabs of the **FTP** module window, click **Edit**, and then ensure that the **Enable FTP** check box is selected. After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

FTP Service Tab

FTP Module – FTP Service Tab Fields

Field	Description
Listening IP	IP address used by the FTP proxy. If this field is empty and the machine has multiple IP addresses, the FTP proxy listens on all IP addresses (interfaces).
Listening Port	Ports used by the FTP proxy.

Conversation Conversion

Select one of the radio button options:

- **Convert all Active conversations to Passive**: If set, all outgoing connections from the proxy will be converted to passive FTP, regardless of the type of connection coming in. This is the default.

- **Convert all Passive conversations to Active**: If set, all outgoing connections from the proxy will be converted to active FTP, regardless of the type of connection coming in.

- **Don't convert anything**: No changes will be made.

Upstream Proxy

FTP Module – Upstream Proxy Tab Fields

Field Name	Description
Enable Next Proxy	If SWG is in a proxy chain, select this check box to enable Next Proxy and to be able to configure upstream Next Proxy parameters,
Next Proxy IP Address	IP address used by the Next proxy.
Next Proxy Port	Port used by the next proxy.

Allowed Server Ports

The **Allowed Server Ports** tab enables you to configure ports used by the FTP protocol. The following table describes the fields in this tab.

- These ports are not relevant if you are working in Transparent Proxy Mode.
- The total number of distinct FTP ports entered must be between 1 and 5 (inclusive).

FTP Module – Allowed Server Ports Tab Fields and Buttons

Field	Description
➕	Click this button to add a port definition line.
From	Lowest port in the range.
To	Highest port in the range.
▤	To delete a port/port range, click this icon and choose **Delete Row**.

5.2.1.8.11 HTTP Module

The **HTTP** module window lets you configure HTTP settings for the deviceCloud Proxy. It contains an **Enable** check box (**Enable HTTP**), and the following tabs:

- HTTP Service Tab

- Advanced Tab

- Headers Tab

- Allowed Server Ports Tab

- URL Rewriting Tab

To edit in the HTTP module window, click **Edit**, and then ensure that the **Enable HTTP** check box is

selected. After editing, click **Save**. To commit the changes, click ⟱ **Commit Changes** in the toolbar.

> When you enable HTTP, you can disable HTTPS (and vice versa); this will close the unused ports, and tighten security.

HTTP Service Tab

The **HTTP Service** tab contains HTTP Service settings.

HTTP Module – HTTP Service Tab Fields

Field Name	Description
Listening IP	Defines the IP address for HTTP listening. If this field is left empty, then HTTP listens on all interface cards configured in the system.
Listening Port	Defines the port (The default port is 8080).

Advanced Tab

The **Advanced** tab contains HTTP Advanced settings.

HTTP Module – Advanced Tab Fields

Field Name	Description
Maximum HTTP Transactions Backlog	Defines the maximum number of queued pending connections waiting to be accepted.
Always try FTP Passive Mode Connection to Server	Check this option in order to enable passive FTP mode when connecting to an FTP server. This is the default mode. If you uncheck it, FTP works only in Active Mode.
Enable Connection-Based Authentication Protocols through Proxy	If an HTTP proxy is used between the client and server, it must take care not to share authenticated connections between different authenticated clients to the same server. If this is shared, then the server can easily lose track of security context associations. A proxy that correctly preserves client to server authentication integrity will supply the "Proxy-support: Session-Based-Authentication" HTTP header to the client in HTTP responses from the proxy. The client must not utilize the SPNEGO HTTP authentication mechanism through a proxy unless the proxy supplies this header with the "401 Unauthorized" response from the server. So when this option is turned on, proxy injects the above header to tell client it is allowed to authenticate with the Web server. This header can only be injected if there are no other proxies between client and server.
Prevent Content Caching by all Downstream Nodes	Enables/disables incoming content from being cached locally. This is disabled by default.
Block Tunneled Protocols (HTTPS)	Blocks tunneling through the proxy (CONNECT requests). When enabling HTTPS, both HTTPS scanning and HTTP tunneling on port 443 are enabled on this device. To disable HTTP tunneling, select the Block Tunneled Protocols (HTTPS) check box.
Enable Trickling	During download of a large file, enables small chunks of data to be sent periodically to the user in order to prevent timeouts. (**Default: enabled**)
Client Wait Time (in seconds)	Defines the amount of time, in seconds, between trickling portions from the Proxy to the Client. The default value for this is 5 (**Do not change this default**).
Client Side / Server Side table	For the Client side and Server side, • select the HTTP version (HTTP 1.0/1.1) • indicate if a Persistent connection should be enabled (select the check box), or disabled (clear the check box.)

Headers Tab

The **Headers** tab enables you to specify Request and Response Headers in the HTTP transaction.

HTTP Module – Header Tab Fields

Field/Button/Value	Description
HTTP Request / Response sections	Fill in the tables in these sections, as needed, to manipulate Request and/or Response Headers in the HTTP transaction.
✚	Click this button to add a Header specification
Header Name	Specify a label for the header.
Value/Source Header	Header value.
Action	Actions to be performed. Select one of the following values:
Add Header	Adds the header to the HTTP Request. or Response
Remove Header	Removes the header to the HTTP Request. or Response
Copy Value to New Header	Creates a new header with the information from the Value/Source Header contained within.
▤	To delete a header specification, click this icon and choose **Delete Row**.

Allowed Server Ports Tab

The **Allowed Server Ports** screen enables you to configure ports to which the proxy is allowed to connect, for each protocol listed – HTTP, HTTPS, FTP over HTTP.

These ports are not relevant if you are working in Transparent Proxy Mode.

HTTP Module – Allowed Server Ports Tab Fields

Field	Description
Specific Ports For *protocol* check box	Select the check box for the particular protocols (**HTTP**, **HTTPS**, and/or **FTP over HTTP**) for which you want to specify ports/port ranges to which the proxy is allowed to connect.
	Then use the following fields/buttons under the check box row to identify the ports.

HTTP Module – Allowed Server Ports Tab Fields

Field	Description
➕	Click this button to add a port definition line.
From	Lowest port in the range.
To	Highest port in the range.
📋	To delete a port/port range, click this icon and choose **Delete Row**.

URL Rewriting Tab

The URL Rewriting feature allows the proxy to direct URLs (or IP addresses) to a specified alternate location. This might be helpful for avoiding expending unnecessary Internet traffic resources when browsing, and/or forwarding users to localized resources.

Warning: The Cache module performs the rewrite; therefore, if Caching is disabled, URL Rewriting will not work. Note, however, that the outcome of the URL Rewrite policy takes precedence over the caching function.

To enable caching, ensure that the **Enable Caching** check box in the Cache module for this device is selected. For more information, see Cache Module.

The GUI provides a clear example of the Source and Destination criteria (the example is located directly under the **Enable URL Rewriting** check box).

HTTP Module – URL Rewriting Tab Fields

Field	Description
Enable URL Rewriting	Select the check box to enable this feature which 'redirects' users to an alternate location.
URL Rewriting table	Define the list of URL Rewrite rules in this table.

HTTP Module – URL Rewriting Tab Fields

Field	Description
✚	Click this button to add an URL Rewrite rule definition line.
number	Sequence number assigned to the rule. Rule priority (that is, the order in which the rules are considered) is set according to this sequence (#1 is highest).
	To change a priority (that is, move a rule up or down in the sequence), click the 📋 icon for the rule, and choose Increase Priority or Decrease Priority.
Enable	Select this check box to enable the rule to be applied.
Source	Intended URL or IP address, such as: **^http:// (.*\.yahoo\.*)/(search.*)**
Destination	Location (URL or IP address) to which the URL is being redirected.
	The following is an example of a Source and Destination URL:
	• **Source — ^http://(.*\.yahoo\..*)/(search.*)**
	• **Destination: — http://\1/\2&vm=r**
Case Sensitive	Select this check box when there are at least two alternate locations, one of them in lower case and one of them in upper case.
Mode	Select the mode (**Server** or **Client**) with which to rewrite, according to administrator preference. Possible values:
	• **Server** — The browser is unaware that a redirect is occurring. Each request is re-directed by proxy.
	• **Client** — The browser is instructed to go to an alternate location, and the client is aware of the change.
📋	Click this button and then select the appropriate option, to change the priority of, or delete a URL Rewrite rule.
Test URL Rewriting area	**Note**: This area is available only if Caching is enabled.
	You can test the URL Rewriting definitions by doing the following in order. It is unnecessary to be in Edit mode to run the URL Rewrite test.
First empty field	(Step1) Enter the **Source URL** in this field.
Test button	(Step2) Click the **Test** button to run the test.
Second empty field	(Step2) Test result: The modified URL is automatically written to this field. (If the URL is not modified, no text is written to the field).

Administration

5.2.1.8.12 HTTPS Module

The **HTTPS** module window lets you configure HTTPS settings for the device. HTTPS scanning is a license based feature (i.e., fields are active only if user has the license).

The HTTPS feature decrypts HTTPS traffic and inspects it for malicious code. It then re-encrypts the communication and sends it through to the end-user.

Administrators can also set Bypass, Inspect Content and User Approval policies for encrypted traffic in order to ensure greater control over the content passing through the system.

The HTTPS feature also integrates with SSL authentication (for more information, see Integrated SSL Scanning Concepts).

The **HTTPS** module window contains an Enable check box (**Enable HTTPS**), and the following tabs:

- HTTPS Service Tab

- Advanced Tab

- Allowed Server Ports Tab

To edit in the HTTPS module window, click **Edit**, and then ensure that the **Enable HTTPS** check box is

selected. After editing, click **Save**. To commit the changes, click ![icon] **Commit Changes** in the toolbar.

> When enabling HTTPS:
>
> - You can disable HTTP (and vice versa); this will close the unused ports, and tighten security.
>
> - Both HTTPS scanning and HTTP tunneling on port 443 are enabled on this device. To disable HTTP Tunneling, select the Block Tunneled Protocols check box in the HTTPS Service Tab section of the HTTP module window.

The HTTPS module node has options that let you import, generate, and export Certificates. For more information, see HTTPS Certificate Management Options. (These options are in addition to the options found on all Scanning Server/ Default **module** nodes.)

Integrated SSL Scanning Concepts

When HTTPS scanning is enabled, SWG Scanning Server serves as an intermediary, providing SSL authentication by not only encrypting the data but also by determining whether the original HTTPS server and the end-user have the expected authentications. The Scanning Server performs this task by acting both as an HTTPS server replying to the end-user requests, and as an HTTPS client requesting the original HTTPS server for the content on behalf of the end-user.

When the end-user requests the server's certificate from the Scanning Server, the Scanning Server retrieves the certificate from the original Web server. The Scanning Server then validates the certificate and, according to the security policy, sends it to the user or blocks it. This transaction includes two sessions, one between the client and the Scanning Server, and another between the Scanning Server and the original Web server.

HTTPS Service Tab

The **HTTPS Service** tab enables you to configure the HTTPS Service settings.

HTTPS Module – HTTPS Service Tab Fields

Field Name	Description
Listening IP	Defines the IP address for HTTPS listening. If this field is left empty, then HTTPS listens on all interface cards configured in the system.
Listening Port	Defines the port that will be listening to incoming HTTPS requests.

Advanced Tab

The **HTTPS Advanced** tab enables you to configure the protocol settings.

HTTPS Module – Advanced Tab Fields

Field Name	Description
Allow SSLv2	Enables support for SSLv2 protocol. This option is disabled by default. This protocol is non-secure and should not be used unless there are some compatibility problems.
Allow SSLv3	Enables support for SSLv3 protocol. This option is enabled by default.
Allow TLSv1	Enables support for TLSv1 protocol. This option is enabled by default.
Use Diffie-Hellman	Enables the use of Diffie-Hellman as the key exchange mechanism between the client and the proxy. This is enabled by default.
Allow weak Ciphersuites	Allows the choice of weak (non-secure) cipher suites while performing an SSL handshake between SWG and the HTTPS server. This option is disabled by default.
Allow Certificate Wildcards	Allows support for Certificate Wildcards. The Certificate Wildcard works in conjunction with an existing Certificate Validation rule. This means that only if there is a policy with a Certificate validation rule will the wildcard support be relevant.
Enable Session Caching	Enables session caching of HTTPS traffic.
Enable Certificate Caching	Enables caching of HTTPS traffic certificates.
SSL Handshake Timeout	Defines the amount of time (in seconds) after which the SSL handshake is timed out if not responsive.
Max HTTPS Transactions Backlog	Defines the maximum number of outstanding connection requests to be served by the system. After this number is reached, the system is timed out. The default value is 36.

Administration

234

HTTPS Module – Advanced Tab Fields

Field Name	Description
HTTPS Timeout	Defines the amount of time (in seconds) after which an idle connection is timed out.
	Important: Entering a zero value will halt all HTTPS traffic. Use at least the default setting value.
Allow Certificates with this key length or longer	Defines the minimum allowable key length (in KB).

> If the Allow SSLv2 protocol is selected, a message appears stating that this protocol is a less secure protocol than the SSLv3/TLSv1 protocols and may compromise your encrypted data. To confirm the selection you must click **OK**.

Allowed Server Ports Tab

The **HTTPS Allowed Server Ports** tab lets you to configure ports allowed (regardless of protocol). For example, the end-user sends the request to the proxy on port 8443, which is the port on which Trustwave is "listening" for HTTPS, but the original server listens on port 444.

> These ports are not relevant if you are working in the Transparent Proxy Mode.

HTTPS Module – HTTPS Allowed Server Ports Tab Fields

Field	Description
➕	Click this button to add a port definition line.
From	Lowest port in the range.
To	Highest port in the range.
📋	To delete a port/port range, click this icon and choose **Delete Row**.

HTTPS Certificate Management Options

In addition to the options found on all Scanning Server/ Default **module** nodes (see Options on Modules Under Scanning Servers/Default Settings), HTTPS modules have additional options for HTTPS Certificate Management.

An HTTPS Certificate guarantees the security of the content.

The task of verifying the certificate can be broken down into two parts:

- Validating each certificate.

- Ensuring that the chain leads back to a trusted authority. (A list of trusted Certificate Authorities is maintained by the system and used for SSL Certificate validation.)

During the installation and setup of SWG, a private key is created by the system, followed by the creation of a self-signed certificate. By default, SWG signs the on-the-fly certificates using the self-generated private key, and the end-user sees the self-signed certificate.

The following right-click certificate options are available:

- Import Certificate

- Generate a Certificate

- Export Certificate

Import Certificate

The SWG system allows you to import a new certificate. Two types of certificates are supported:

- Root CA: This option allows system administrators to import the certificate into the system together with the private key.

- CSR: This option enables you to import a certificate signed by the CA after a CSR was generated by SWG.

This root certificate is uploaded and displayed to users browsing HTTPS sites and is done globally for all scanning servers.

Generate a Certificate

Large organizations, which employ their own CA that is already trusted by end-users, can generate a Certificate Signing Request (CSR). After the generation of the CSR, the system administrator can export the request (which is signed by SWG's private key) and send it to the Certificate Authority. The CA will then generate a certificate, which will be imported into SWG. This procedure makes the process of exporting the certificate to end-users unnecessary.

Export Certificate

System administrators can export the SSL certificate from the system to install it later on end-user machines as a trusted CA. Installing SWG certificates on end-user machines will prevent the security validation error messages to be sent to the end-users.

5.2.1.8.13 ICAP Service Module

The **ICAP Service** module enables SWG to provide ICAP Services to third-party ICAP clients, through relevant scanning servers. (Prior to SWG release 10.2., this module was called **ICAP**.)

> Cloud scanning servers do NOT have or need an ICAP Service module.

It is necessary to set these settings before configuring the ICAP client services in order to enable automatic ICAP client setup (BlueCoat: Sense Settings function). Detailed information can be found in the *Secure Web Gateway Setup Guide*.

The **ICAP Service** module window contains an **Enable** check box, and the following tabs:

- ICAP Service Tab

- ICAP Clients Tab

- Options Tab

- Advanced Tab

- Headers Tab

To edit the tabs of the **ICAP Service** module window, click **Edit**, and then ensure that the **Enable ICAP**

check box is selected. After editing, click **Save**. To commit the changes, click [icon] **Commit Changes** in the toolbar.

> - If you are using the Scanning server only as an ICAP Service provider, you can disable HTTP; this will close the unused ports, and tighten security.
>
> - If there is no direct Internet access, to perform prefetching of Java classes for Applet scanning, ALL Scanning Servers must have the Next proxy configured. If you are using ICAP, ensure that the SWG Appliance Scanning Server appears on the Access List.

ICAP Service Tab

ICAP Service Module – ICAP Service Tab Fields

Field Name	Description
Listening IP	Local IP on which the ICAP Service listens.
Listening Port	Local port through which the ICAP Service listens. Default: 1344

ICAP Clients Tab

ICAP Service Module – ICAP Clients Tab Fields

Field/Button	Description
✚	Click this icon to add an ICAP client definition. Then specify the client details in the fields in added row.
Type	ICAP client type. Valid Values: • **Blue Coat** • **NetApp** • **Generic**
Source IP	IP from which the ICAP client can use this scanner for the ICAP Services.

ICAP Service Module – ICAP Clients Tab Fields

Field/Button	Description
Weight	Percentage of resources (1 - 100) allowed to this client. The sum of all weights specified for all clients must add up to 100%.
	To delete an ICAP Client, click this icon and choose **Delete Row**.

When using SWG as an ICAP Service, the ICAP client should use the following URL format to access the service:

- For request mode:

  `icap://servername:port/Trustwave_REQMOD`

  For example: `icap://192.168.120.150:1344/Trustwave_REQMOD`

- For response mode:

  `icap://servername:port/Trustwave_RESPMOD`

  For example: `icap://192.168.120.150:1344/Trustwave_RESPMOD`

For more information, see the *Secure Web Gateway Setup Guide.*

Options Tab

The **Options** tab controls the response to a special **Options** request that an ICAP client periodically sends to an ICAP server.

ICAP Service Module – Options Tab Fields

Field	Description	Default
Preview Size (Bytes)	Number of bytes in the portion of the request that ICAP Service will initially look at before determining if it has enough information to continue or if it needs to view the full request.	4096
Options Time to Live (Seconds)	Number of seconds for which the ICAP Service's response to a client's **Options** request is valid. (After this time passes, the client must make a new **Options** request.)	3600
X-Client-IP	Select this check box if the ICAP client is expected to send the client IP address in each ICAP request.	N/A
X-Server-IP	Select this check box if the ICAP client is expected to send the Web server IP address in each ICAP request.	N/A
X-Authenticated-User	Select this check box if the ICAP client is expected to send the authenticated user credentials in each ICAP request.	N/A

Advanced Tab

The **Advanced** tab enables you to define various connections.

ICAP Service Module – Advanced Tab Fields

Field Name	Description	Default
Maximum TCP/IP Connections Backlog	Defines the maximum TCP/IP connections backlog.	256
Enable Trickling check box	To prevent timeouts that would otherwise result from large Response transmissions that take more time than the timeout threshold, ensure that the **Enable Trickling** check box is selected. Trickling sends small, trivial Response transmissions, solely to indicate that it is up and running, before the timeout threshold is reached. Trickling refers only to the Status Page and is only available from NetApp.	N/A

Headers Tab

The **Headers** tab enables you to specify Request and Response Headers in the ICAP transaction.

ICAP Service Module – Headers Tab Fields

Field/Button/Value	Description
ICAP Request / Response sections	Identify any additional **ICAP Request** and/or **Response Headers** that the scanner can send to/receive from the Web, by doing the following in their respective sections:
	Click this button to add a Header specification.
Header Name	Specify a label for the header
Value/Source Header	Header name, and the value details
Action	Actions to be performed on the header. Select one of the following values:
Add Header	Click this value if the header should be added to the Request or Response.
Remove Header	Click this value if the header should be removed to the Request or Response.
Copy Value to New Header	Click this value if a header which originally existed in a Request or Response should be copied (for subsequent use as specified in the Request or Response).
	To delete a header specification, click this icon and choose **Delete Row**.

5.2.1.8.14 ICAP Client Module

Warning: The ICAP client is only suitable for use with SWG Cloud Scanners when deployed in a Private Cloud configuration, otherwise performance degradation and additional bandwidth costs may be incurred.

The **ICAP Client** module window lets you enable an ICAP Client on the device, and configure relevant time-outs. The window contains two tabs:

- Connection Behavior Tab

- Keepalive Services Tab

To edit the fields in the **ICAP Client** module window, click **Edit**, and then ensure that the **Enable ICAP Client** check box is selected. After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

Connection Behavior Tab

ICAP Client Module – Timeouts Tab Fields

Field	Description	Default
Connecting Timeout	Maximum number of second to wait for a connection to be established.	60
Input/Output Timeout	Maximum number of seconds to wait for completion of a message transmission.	120
Connection Reuse Timeout	Maximum number of seconds that the connection will be alive on idle after its previous use.	300

Keepalive Services Tab

The Keepalive Services tab contains the following field:

- **Service Health Check interval** — Number of seconds between each health check of ICAP Services, (the health check determines if the service is up and running). Default 180.

5.2.1.8.15 WCCP Module

Warning: WCCP is suitable for Cloud Scanners only when deployed in a Private Cloud. Other Cloud Scanner deployments may incur bandwidth costs and additional network latency.

The **WCCP** module window lets you configure Web Cache Communication Protocol settings for the device.

This protocol enables WCCP enabled routers (and switches) to redirect traffic to other WCCP enabled servers, without the need for users to configure their browsers or any other proxy settings.

When you send a request, this request is sent to the original server and the WCCP router (or switch) redirects the request to the Scanning Server, which then inspects the request. The Scanning Server then generates a new request and sends the request to the original server. The reply is sent back to the end-user after it was scanned by the Scanning Server

The WCCP protocol limits the number of ports per service to 8. If more than 8 ports are configured, a warning will be issued, and an arbitrary 8-port subset of these ports will be serviced by the WCCP.

> Transparent proxy must be enabled for WCCP to work.

The window contains an **Enable** check box. To edit the fields in the **WCCP** module window, click **Edit**, and then ensure that the **Enable WCCP V2** check box is selected. Besides enabling you to edit the fields, this check box enables the use of WCCP Version 2 protocol in conjunction with the SWG appliance.

After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

The following table describes the WCCP Configuration fields:

WCCP Module Fields

Field	Description
Forwarding Method	Specify the communication protocol between the WCCP enabled router and the Scanning Server. Valid values: **Layer2** or **GRE** (Generic Router Encapsulation). Note the following points when selecting a value: • If the Scanning Server is connected to a switch, choose **Layer2**. **Note**: In this case, the Scanning Servers and WCCP-enabled router must be on the same network. • For a router, choose **GRE**.
Assignment Method	Type of WCCP implementation. Valid values: **Hash** or **Mask** Assignment: • When using a Hash Assignment, the WCCP-enabled router performs a hash function on the IP address. The routers hold a hash table, which maps the result of the hash function to one of the Scanning Servers. • When using a Mask Assignment (must be supported by the WCCP-enabled router), the router performs a logical AND operation at the single-bit level (rather than larger data units) between each mask value and the content of the packet. The WCCP-enabled router compares a list of values for each mask.
Password	Optional authentication password.
Routers	This defines the IP address of the router.
➕	Click this button to add a router definition line.
IP Address	IP address of the router.
Service IDs	Router service number describing one of the following services: **HTTP**, **HTTPS** and **FTP**.

5.2.1.9 Access List

The Access List feature enables you to control access to specific IPs or IP ranges.

Access List definition fields appear in the following locations:

- Access List node under the Device General Settings node — for defining default Access List settings.

- Access List tab in device definitions — for defining Access Lists for the specific device.

The process for configuring Access Lists is the same for Default Access Lists and Scanner-specific Access Lists; only the path for accessing the Access List definition is different.

It is recommended that you configure the Default Access Lists before those for specific Scanning Servers. The Default Access List will apply to the local All-in-One device, if one is installed. In addition, the defaults will apply to any Scanning Server device that is added after the default settings have been defined; you can then modify the Access List settings on the specific device, as needed.

The Access List definition provides separate areas for defining each of the following types of Access Lists:

- Management Access List

- User Access List

- Access to SWG system ports

You can reset Access List values, as follows:

- To apply the default Access Lists settings to the Access Lists in ALL scanners, right-click the **Access List** node under **Device General Settings** and choose **Reset all with default values**.

- To apply the default values to an Access List on a particular device, right-click the device IP node and choose **Apply Default Access List Values**.

- To replace the current default Access List settings with the Access Lists settings of a particular device, right-click the device IP node and choose **Set As Access List Default**.

- (To apply the default settings to the Access Lists and scanner modules in ALL locations, right-click the **Default Values** node and choose **Reset all with default values**.)

This section contains the following topics:

- Access List Fields

- Access List Troubleshooting

5.2.1.9.1 Access List Fields

<div align="center">Access List Fields</div>

Field	Description
Use Access List check box	Enables the use of the Access List.
Access List areas	
Management Access List	Used for specifying the IPs of administrators who can access Management Console, SSH, and SNMP. For example, to block access to the Management Console for certain administrators, specify only the relevant IP addresses of authorized administrators.
	If Access Lists are selected (i.e., the **User Access List** check box is selected), at least one IP must be specified in this list (preferably the IP of the machine accessing the Management Console). This will ensure that access is not totally blocked to the Management appliances.
Users Access List	Used for controlling which Scanning Servers end-users can browse through. You specify the IP ranges that are allowed to use the SWG Scanning Server. Users whose IPs are in the allowed range can browse; other users are blocked.
Access to Trustwave SWG system ports	Used for controlling which device IPs have access to the SWG system.
Fields and buttons in the areas	
✚	Click this button to add an IP Range definition line.
From IP	Lowest IP in the range.
To IP	Highest IP in the range.

5.2.1.9.2 Access List Troubleshooting

If the Access List is enabled, then modifying the Device IP, the Appliance role or adding an additional device to the topology, might cause a possible loss of connection with the modified device. Connection loss may also influence the connection with other devices in this cluster and also for administrators.

To avoid this potential problem, perform the following procedure on the device where the changes will be made:

When changing roles, IPs or adding additional devices to the tree:

1. Disable Access List through the access_list Limited Shell command.

2. Perform the change of role, IP or device addition.

3. Enable Access List through the access_list Limited Shell command.

In situations where the connection to the device is lost or the Access List has not been disabled, Administrators can connect to the device via serial port console and disable the Access List.

5.2.1.10 High Availability

You can implement Policy Server High Availability by dedicating an additional device as a secondary (Passive) Policy Server.

In the event of failure of the Active Policy Server, SWG automatically fails over to the secondary Policy Server, making it the primary Active Policy server. When the failed server can again be used, SWG designates it as the Passive Policy server. To switch it back to being the Active policy server, you must manually perform failover using the failover Limited Shell command.

Implementation of High Availability requires that:

- the primary (Active) Policy Server be on its own device, NOT on an All-In-one device.

- the device that will house the secondary (Passive) Policy Server has the same version as the primary Policy Server, is accessible, and you know its IP address.

- Both active and passive policy servers must be synced with the same NTP server.

To be able to use a Virtual IP address which will automatically route to the Active Policy Server, both Policy Servers must be on the same network.

- Ping Node — Ping node detects a situation in which there is a network communication between active and passive policy servers, but no network to scanners. If no ping between the active policy server and the ping node exists, the system will failover and the passive policy server will become active. It is recommended that the IP of the ping node be the default gateway.

> The Management Console GUI is inaccessible on the Passive Policy server device.

> **Warning:** When disabling HA, ensure that the Passive Policy server is connected to the Active Policy server.

Status Tab Fields in the High Availability Device IP Window

The following table describes the fields in the Status tab in the Device IP window of the High Availability (secondary) server.

<div align="center">Device IP Window – Status Tab Fields</div>

Field	Description
Sync Status	Indicates whether the Device is synchronized with the Policy Server.
Connection Status	Indicates if the device is available (**Active**).
Committing Status	Indicates whether the device is undergoing a **Preparing to Commit** status, **Committing Changes** status, or is Stable.
Replication Status	Status of the replication.
Last Connection Time	Indicates the last time this device was connected to the Policy Server.

5.2.2 Scanning

This menu option provides the following sub-menu options.

- Scanning Options

- Scanning Engines

5.2.2.1 Scanning Options

In the Main Tool bar, select **Administration** | **System Settings** | **Scanning** | **Scanning Options.** This window is used to enable the HTML Repair feature; caching of results of scanned files and a Status page. To edit the Scanning Options screen, click **Edit** in the right pane.

The Scanning Options window (accessed via **Administration** | **System Settings** | **Scanning** | **Scanning Options**) has two Enable check boxes:

- Enable Security Results Caching

- Enable Status Page

To perform editing in this screen, you must click **Edit** (which lets you select/clear the check boxes. To edit the tabs that accompany the **Enable Status Page** check box, the check box must be selected.

After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

Enable Security Results Caching

To enable caching of the results of scanned files, select this check box. This improves system performance by reducing scanning time.

SWG is configured so that the largest CPU and the most time-consuming Scanning engines will use this feature accordingly.

Enable Status Page

Files that are being downloaded from the Internet must be scanned by **SWG** before they reach the browser.

During this download process, the browser can display to the user a Status page with download status details.

> The Status Page is disabled when working with HTTPS.

The **Enable Status Page** check box (when selected) activates the Status Page feature and lets you configure parameters related to the Status Page. The parameters are spread over two tabs:

- General Settings Tab

- Activate Tab

5.2.2.1.1 General Settings Tab

The **General Settings** tab is used for configuring general size and time frame settings (and enabling downstream proxy compatibility) for the Status page, as described in the following table:

<div align="center">Scanning Option Window – General Settings Tab Fields</div>

Field Name	Description
Size Threshold for Immediate Activation (KB)	Minimum Download file size that will activate the Status page.
Immediate Activation for Downloads taking more than (in seconds)	Minimum Download time, above which the Status page will be activated.
Progress Bar Update Interval (in seconds)	Frequency with which the progress bar in the Status page is updated during the download.
Completed Download Lifetime (in seconds)	Number of seconds that the downloaded content should remain on the SWG proxy before it is removed.
Downstream Proxy Compatibility	To enable working with ISA Server, select this check box.

5.2.2.1.2 Activate Tab

The **Activate** tab lets you configure activation rules. These rules have essentially the following format:

> **Activate on *User-Agent* when *Content-Type* has the *Value*, except for *Content-type* with *Value*.**

You can define the rules for as many user agents, content types and values, with as many exceptions, as needed.

Note the following:

- **User Agent** — HTTP header field by which the browser is identified by the Server. Most browsers, including Internet Explorer, specify Mozilla as part of the User-Agent field.

- **Content Type**: Can be either an Extension type (in format **Extension is** ...) or a Mime type (in format **Mime Type contains ...**).

  - The Extensions displayed are provided as default Extensions. For example, you can choose not to activate the Status Page if the file is a PDF file (i.e., its value is defined as pdf).

  - **Mime Type** — Header field content. For example, an HTML page can be sent with Content Type: text/html. The substrings that are displayed in the screen are given as default content types.

  You can add extensions and Mime types.

<div align="center">Scanning Option Window – Activate Tab Fields</div>

Area/Field	Description
	Click this icon to add a detail line to the area.
	Click this button to delete a detail line in the area.
On User Agents area	Specify which User Agent(s) having the specified content type /values will activate the Status page.
User Agent	HTTP header field by which the browser is identified by the Server. (**Default**: **mozilla**)
Activate When area	In this area, specify the file extensions and/or mime types that will activate the Status page on the agent(s).
Content Type / Value	Select the content type and specify the value of that content type. Valid Content Types: • **Extension is** — For specifying File extensions. (**Defaults**: **zip** and **exe**) • **Mime Type contains** — For specifying a Mime Type substring. (A number of defaults are included in the display.)
Unless area	In this area, specify the file extensions and/or mime types that constitute exceptions to the above **Activate When** rule.
Content Type / Value	Select the content type and specify the value of that content type. Valid Content Types: • **Extension is** — For specifying File extensions. (**Defaults**: **zip** and **exe**) • **Mime Type contains** — For specifying a Mime Type substring. (A number of defaults are included in the display.)

5.2.2.2 Scanning Engines

SWG comes with a number of Scanning Engines. Some are Trustwave-proprietary; others are third-party engines. Some are configurable; others are not configurable.

> You cannot run a third-party engine unless you have obtained a license for it.

You can display the tree that lists available scanning engines, by selecting **Administration | System Settings | Scanning | Scanning Engines**. (Each engine has its own main window display.)

By selecting a node in the Scanning Engines tree, you can display (and where permitted, edit) engine details.

To edit a configurable Scanning Engine, after displaying it, click **Edit**. If the editing of a field depends on a check box being selected, ensure that it is selected. After editing, click **Save**. To commit the changes, click

Commit Changes in the toolbar.

Scanning Engines (described below) fall into the following categories:

- Anti-Spyware — Not configurable

- Anti-Virus (Kaspersky, McAfee, and Sophos) — Configurable

- Digital Signature Analyzer — Configurable

- Malware Entrapment —Configurable

- URL Filtering — Not configurable

5.2.2.2.1 Anti-Spyware

The Anti-Spyware engine is a Trustwave proprietary engine, so it requires no license. It contains the following lists that are continuously updated by Trustwave.

The information in these lists cannot be configured or deleted.

Fields in the Anti-Spyware Scanning Engine

- **Spyware Home Black List** — A black list of URLs known to accommodate Spyware

- **Spyware Profiles** — Spyware picked up by the Active Content List content processor.

The Anti-Spyware profile appears as a built-in behavior profile in the Script Behavior Profiles in the Rule Conditions (**Policies | Condition Elements | Binary Behavior**).

5.2.2.2.2 Anti-Virus (Kaspersky, McAfee, and Sophos)

Each of these Anti-Virus engines is a third-party engine, requiring a license — each includes pre-configured profiles generated by the software manufacturers. You can edit the configurations. For more information, see Scanning Engines.

Fields in the Anti-Virus Scanning Engines

All three Anti-Virus Scanning engines (Kaspersky, McAfee, and Sophos) contain the following field:

- **Scanning Time Limit** — Number of seconds, after which the Anti-Virus engines will stop scanning a large file (default: 30; maximum: 300). This option reduces the possibility of system time-outs.

> This time limit refers to a single item; if there are containers containing many items, this time limit will be extended accordingly.

In addition, the McAfee Anti-Virus Scanning engine contains the following check boxes:

- **Enable Macro Scanning** — Select this check box if the engine should scan macros in Office documents.

- **Enable Heuristics** — Select this check box if the engine should use generic methods to scan for potentially unknown threats.

5.2.2.2.3 Digital Signature Analyzer

In the Digital Signature Analyzer engine, the administrator can define the minimum allowed key length (in KB) for a certificate. For more information, see Scanning Engines.

5.2.2.2.4 Malware Entrapment

This engine is a Trustwave proprietary script behavior engine, so it requires no license. It is based on monitoring security behaviors and profiles that are subsets of all available behaviors. For more information, see Scanning Engines.

Behavior Profiles are lists of actions that could be considered malicious or suspicious when executed by Web pages, VB Script files, Java Script files or other relevant files.

Behavior Profiles are divided into five different security levels: **None**, **Basic**, **Medium**, **High** and **Strict**. The security levels pertain to the efficacy with which these behavior profiles are enforced.

The groups at various levels define language tokens, semantic patterns of Active Code, forbidden combinations of operations, parameters and programming techniques. These groups are created by security experts from the Malware team at Trustwave, and fed into the Behavior Profile scanning engines, enabling the identification of malicious active content.

The SWG system is pre configured, by default, at the Medium security level. Administrators can set an appropriate security level on a per policy basis.

Fields in the Malware Entrapment Scanning Engine

You can configure the Malware Entrapment Scanning Engine settings. The window contains three areas:

- **HTML Repair** area — Select the check box in this area if suspicious code should automatically be removed.

- **Scanning** area — Set the number of seconds after which scanning will timeout.

- **External Resources** area — Contains two check boxes:

- **Enable ... prefetching** — Select this check box to enable pre-fetching of content from a Web page.

- **Enable ... caching** — Select this check box to enable caching of pre-fetched content.

5.2.2.2.5 URL Filtering

URL Filtering blocks, allows or classifies content based on the URL. To this end, a proprietary Trustwave List Categorization engine is deployed as the URL Categories Filter in Secure Web Gateway. SWG can also classify URL pages using TextCensor in cases where the URL Categorization engine fails to classify them. TextCensor is Trustwave's proprietary DLP and URL categorization engine.

For more information, see Scanning Engines.

> Every SWG deployment has only a single URL Categorization Engine License. The appropriate license is selected upon initial acquisition of the primary SWG license and is dependent on the number of Users.

The Trustwave URL Categories Filter identifies embedded URLs.

The filter offers a set of logical groupings to the categories they provide. This is used to simplify the policy settings and enable actions to be set by category group and not by every individual category. These category groups are also used for Reports and Logging, which provide the necessary information for administrators to set policies accordingly. (Block/Allow/Coach specific categories, such as Entertainment or Games).

Dynamic Categorization

Select the **Enable dynamic URL categorization** check box if you want SWG to classify the content of URL pages using TextCensor in cases where the URL Categorization engine fails to classify them specifically.

You can see if actions taken by SWG were as a result of Dynamic Categorization by checking the Web Logs. The Contents details tab will include the URL Category and whether the item was dynamically categorized.

> If the **Enable sending customer feedback information** check box is selected (via **Administration | System Settings | Administrative Settings**), relevant dynamic categorization data will be provided to the Malware team at Trustwave for review.

Fields in the URL Filtering Scanning Engines

Numbers and signature/DAT file numbers are displayed.

- **Version** — Engine version.

- **DAT Version** — .dat file version

5.2.3 Mail Server

The Mail Server controls the sending of emails for system events, application events, and software updates. The server uses Simple Mail Transfer Protocol (SMTP).

You must configure the settings for the Mail Server. You do this in the Mail Server Settings window (accessed via **Administration** | **System Settings** | **Mail Server**)

To edit the fields in the window, click **Edit**, and then select the **Enable Sending Email** check box. After editing, click **Save**. To commit the changes, click [icon] **Commit Changes** in the toolbar.

Mail Server Fields and Buttons

Field/Button	Description
Enable Sending Email	Enables emails to be sent (and enables the screen fields to be edited)
Hostname/IP	IP address (or hostname) of the SMTP Server you are using (e.g., mail.Trustwave.com).
Port	Number of the port that the SMTP Server uses (this is usually 25).
User Name/Password	User name and password used for SMTP Authentication (e.g. VS_NG. This might be optional, depending on your SMTP requirements).
Originating Domain	Domain from which emails will be sent.
Test Recipient	Email address to which a test email will be sent, to validate that the messages are being received (for example, sarah@Trustwave.com).
Test button	Click this button to test the configuration. A sample email alert will be sent to the test recipient email address.

5.2.4 Administrative Settings

The Administrative Settings window (accessed via **Administration | System Settings | Administrative Settings**) contains the following two tabs:

- General Tab
- Toolbar Tab

To edit the fields in either or both tabs, click **Edit**. After editing, click **Save**.

5.2.4.1 General Tab

Administrative Settings Window – General Tab Fields

Field	Description
Console Timeout Console Timeout is *nnn* minutes	If there is no activity detected on the Management Console after the specified number of minutes, the session times out. This is useful for security purposes to prevent unauthorized access to the Management Console.
Grid Default Display	Set the default for how grids are displayed when accessed by users. • **Display all values** shows all available options whether or not they are selected. • **Display only selected values** shows only the options that are currently selected, or that have sub-options selected. Irrespective of this default setting, users can change the display in view by selecting either **Display Selected** or **Display All** above each grid.
Commit Changes Mandatory Audit log note on commit changes check box	Select this check box to send a note to the audit log every time a configuration change has been committed. Once this feature is enabled, filling in the Note box becomes mandatory any time ⬇ **Commit Changes** in the toolbar is clicked.
Enable sending customer feedback information check box	This check box should be selected. This option confirms the approval from the customer to provide data to the Malware team at Trustwave for review. (The data sent to Trustwave is comprised mainly of blocked transactions and browsing habits. Gathering this information helps Trustwave uncover unknown malicious dangers that can, in turn, be prevented in future versions of the SWG product or security updates to keep the customer protected.) **Note:** This check box is also available in the Trustwave End User License agreement. In the accompanying fields, the customer can set the optimal schedule for transmitting the data.
Run Daily at:	For specifying a particular time (*hh:mm*) to run each day.
Run weekly on	For specifying particular days of the weeks at a specific time (*hh:mm*)

5.2.4.2 Toolbar Tab

The **Toolbar** tab lists available shortcut icons for display in the SWG toolbar. Select/deselect the icons according to which ones you want included/excluded from the toolbar. For more information about the icons, see Toolbar.

5.2.5 Digital Certificates

The use of digital certificates adds another layer of security when users download ActiveX controls, and other executables, from the Internet.

Digital Signature-based technology identifies the publisher of signed software, and verifies that there has been no tampering with the code.

Digital certificates use a cryptographic technology called public-key cryptography to sign software publications and to verify the integrity of the certificate itself.

By importing Digital Certificates, you can ensure that only authorized and certified active content is downloaded.

You can import Digital Certificates in the Digital Certificates window (accessed via **Administration | System Settings | Digital Certificates**).

This window contains a tree pane that lists Digital Certificate Lists. Two of the lists in the tree are actually certificate revocation lists.

By selecting a list in the tree pane, you can display certificates that comprise that list, and details about the certificates. Most, but not all, of the Lists are editable.

> The details displayed for the certificate revocation lists differ from those displayed for the certificate lists. Furthermore, the Trustwave Security Certificate Revocation details window contains a check box that lets you enable/disable the Certificate Revocation mechanism. For more details, see Update and Fields in the Certificate Revocation List.

The following options are available in the Digital Certificates tree:

- **Import Certificate** — Displays a window that enables you to import certificates to a list. Only available for Editable lists. For more information, see Import Digital Certificate Window.

This section contains the following topics:

- Available Digital Certificate Lists

- Fields in the Certificate List Details Window

- Update and Fields in the Certificate Revocation List

- Import Digital Certificate Window

Available Digital Certificate Lists

The following Digital Certificate lists are available:

- **Customer CAs for Cloud** — List of certificates used in the cloud context. If the CA provided in the cloud configuration page is not self signed, and is not trusted by SWG, the CA that signed the imported CA must be imported. All CAs in the certificate signing chain between the signing CA and the CA in the cloud context must also be imported.

  All files must be in a PEM format before being imported. PEM is a Base-64 encoded X.509 certificate text file format.

- **Customer Certificate Revocation List** — External list of certificates which have been cancelled.

  To update this list, you must subscribe to the Certificate Revocation List thereby receiving pre-defined files which can be imported into the Policy Server. Subscribing to the Certificate Revocation List is done outside the system.

  All files must be in a PEM format before being imported. PEM is a Base-64 encoded X.509 certificate text file format.

- **Customer Trusted Publishers (code signing only) and Customer Untrusted Publishers** — These two lists contain certificates from trusted/untrusted publishers. These files are received from an external source.

  All files must be in a PEM format with a PEM extension before being imported.

  Each file to be imported may contain a number of certificates, but SWG only displays the first one in the file.

- **Customer Trusted Root CA** — Root Certificate Authorities (CA) refer to "self-signing" certificates, that is, certificates that are issued on their own authority.

- **Trustwave Security Certificate Revocation List** — Non-editable list of certificates which have been revoked.

  > This list is automatically updated as part of Security updates (for more information, see Updates and Upgrades).

- **Trustwave Trusted**, and **Untrusted Publishers** — Two Trustwave-predefined, non-editable lists of trusted and untrusted publishers respectively. These lists are regularly updated via Trustwave Updates.

- **Trustwave Trusted Root CA** — Non-editable list. Root Certificate Authorities (CA) refer to "self-signing" certificates, that is, certificates that are issued on their own authority.

5.2.5.1 Fields in the Certificate List Details Window

> This section applies to all Certificate Lists except the revocation lists (**Customer Certificate Revocation List** and **Trustwave Security Certificate Revocation List**). For a description of those lists, see Update and Fields in the Certificate Revocation List.

To edit the details in an editable window, click **Edit**. After editing, click **Save**. To commit the changes, click

Commit Changes in the toolbar.

Certificate List Details Window Fields

Field	Description
Certificate Name	Name of the Digital Certificate list.

Administration
254

Certificate List Details Window Fields

Field	Description
Digital Certificates area	Displays the details of the certificates in the list.
	Let's you perform an operation on the list. To delete a certificate from the list, click this icon next to the certificate and choose **Delete Row**.
Issued By	Name of the Certificate Authority who issued the certificate
Issued To	Name of the organization who the certificate is issued by and issued to (In the case of root certification authorities or self-signed certificates, the names are the same.)
Expiration	Expiration date of the certificate
Friendly Name	Name of certificate presented externally

5.2.5.2 Update and Fields in the Certificate Revocation List

This section applies only to the **Customer Certificate Revocation List** and **Trustwave Security Certificate Revocation List**.

Update of the listings in the Certificate Revocation Lists works as follows:

• **Customer Certificate Revocation List** — External list of certificates which have been cancelled.

To update this list, you must subscribe to the Certificate Revocation List thereby receiving pre-defined files which can be imported into the Policy Server. Subscribing to the Certificate Revocation List is done outside the system.

All files must be in a PEM format before being imported. PEM is a Base-64 encoded X.509 certificate text file format.

• **Trustwave Certificate Revocation List** — Non-editable list of certificates which have been cancelled.

This list is automatically updated as part of Security updates (for more information, see Updates and Upgrades).

Both Certificate Revocation List windows have an **Enable CRL** check box. When cleared (i.e., the CRL is disabled), SWG ignores the listed Revocations, and the list does not get updated. (The customer default is selected, the Trustwave default is cleared). Enabling one list does not affect the other list.

To select/clear the **Enable CRL** check box, first click **Edit**, and after making the change click **Save**. To commit the change, click ![icon] **Commit Changes** in the toolbar.

<div align="center">Certificate Revocation Lists Fields</div>

Field	Description
Certificate Name	Name of the Digital Certificate list.
Enable CRL check box	Select/clear this check box to enable/disable usage of the Certificate Revocation List.
![icon]	Let's you perform an operation on the list. To delete a certificate from the list, click this icon next to the certificate and choose **Delete Row**.
Issuer	Name of the Certificate Authority who issued the certificate
Last Update	Date of the last update of the CRL.
Next Update	Date of the next planned update of the CRL.

5.2.5.3 Import Digital Certificate Window

To import a certificate into a Digital Certificate list, right-click the Digital Certificate list in the tree and select **Import Certificate**. The **Import Digital Certificate** window is displayed.

Browse to the location of the certificate file, make sure that the file has the correct PEM extension, and then click **Import**.

The imported certificate appears in the Digital Certificate list.

5.2.6 License

SWG must be licensed. You can use a single license key for multiple Policy Servers (that is, for separate deployments). The same license can be re-used if it becomes necessary to reinstall the system.

Two types of licenses are available:

- **Evaluation License:** When entering the Management Console for the first time, an installation Wizard runs and the administrator must enter a license key (both for an Evaluation and a long term license). An evaluation key entitles you to a 30 day evaluation period with full SWG functionality. Once the 30 days evaluation period has passed, SWG will start forwarding Internet content through without scanning it. The Management Console will be disabled until the administrator enters a permanent license key.

  ![info icon] The Policy Server will update Trustwave Headquarters as to the status of the License. This information is confidential and will be kept at the Trustwave Financial offices.

  Ten days before the evaluation license is about to expire, an informative message will be displayed.

The evaluation license can only be installed on one Policy Server.

- **Permanent License**: A permanent license is generated by Trustwave and sent to the customer. Its expiration date is based on a service agreement with the customer. Starting three months before the expiration date, the administrator will receive notifications that the license must be renewed. Once the license has expired, you will be treated to a thirty day grace period where traffic will be scanned but administrators will have very limited access to the Management Console. After the grace period is complete, SWG will no longer function as required.

5.2.7 Debug Log

The Debug Log window (accessed via **Administration | System Settings | Debug Log**) is for use by Trustwave Support personnel only.

5.2.8 GUI Log Level

The **GUI Log Level** configuration window (accessed via **Administration | System Settings | GUI Log Level**) is used for determining the level of support information sent to Trustwave; it is primarily reserved for Trustwave support personnel, or until Trustwave support personnel ask you to adjust the settings.

The window contains two tabs:

- Basic

- Advanced

To edit the fields in either or both tabs, click **Edit**. After editing, click **Save**. To commit the changes, click

Commit Changes in the toolbar.

Basic

The **Basic** tab in the Log Level screen enables the system to be set to varying levels of debugging:

- Trace

- Debug

- Info

- Warn

- Error

- Fatal

The level of debugging should not be modified without consulting Trustwave's Support personnel, as it may have an effect on product performance.

The recommended debug level is set to Error. Only Error level is intended for the production environment.

Advanced

Whereas the **Basic** tab controls the general level of log messages, the **Advanced** tab allows more detailed control in deciphering the components involved with different loggers.

This tab enables you to set the log level (**Trace**, **Debug**, **Info**, **Warn**, **Error**, or **Fatal**) individually for the following components.

- **Root** — All the other loggers

- **Hibernate general** — All hibernating loggers

- **Migration Engine** — Controls migration engine logging. Troubleshoots rollback

- **SQL** — All SQL queries

- **JDBC Parameters** — Database connection parameters

- **HBM DDL** — DDL info

- **Hibernate Entity** — Contents of objects, containing database data

- **Hibernate Cache** — Contents of 1st and 2nd level hibernating cache

- **Database Transaction** — Transactions held with database

- **JDBC** — Logging level of jdbc database driver

- **AST** — Translation of Java commands into native SQL

- **JAAS** — Authentication and authorization information

5.3 Cloud (Hybrid Deployment)

Hybrid deployment is a Trustwave SWG product feature extending Web filtering/security to Windows and Mac Personal Computer (PC) off-premise users - that is, users connecting to the Internet from hotels, airports, Internet cafes, working from home or working from remote offices. Hybrid deployment can also be used to secure remote offices using a local Web proxy.

Hybrid deployment combines on-premise SWG Scanning Servers, SWG Cloud Scanners and Trustwave Mobile Security Client software. Cloud Scanners are a special type of virtualized scanning server configured to support connections only from user computers running Trustwave Mobile Security Client (MSC), or specifically defined proxy servers, for example in remote offices. The client software directs Web traffic to the appropriate and optimal scanner (on-premise or Cloud) depending on user location and available scanners.

The client also provides mutual certificate authentication between the user and the target Cloud Scanner. Multiple, distributed Cloud Scanners can be deployed to cover the geographic locations from which users operate.

Consult the Trustwave *SWG Hybrid Deployment Guide* to study the wider context of Hybrid Deployment including preparation, decisions, platform selection, client and certificate distribution before starting to configure the SWG Policy Server.

Configuring Cloud (Hybrid Deployment) includes the following areas:

- Configure email settings, see Mail Server, ensuring SWG can send client provisioning emails.

- Define the Cloud Scanner devices (not Cloud Load Balancers) used in the deployment, see Scanning Servers.

- Define the Cloud Configuration settings, see Cloud Configuration.

- Customize the Email Template used with Internal Certificate mode to communicate with users (described under Cloud Configuration).

- Define the users and groups that use the cloud, see Users/User Groups.

Cloud implementation also requires managing cloud users and their certificates. For more information, see User Grouping and Certificate Management.

Cloud (hybrid) implementation spans the following sub menu options, located under **Administration | Cloud**. The following configuration commands are provided:

- Configuration (Cloud Configuration)

- Certificate Management Tab - PKI Mode

- Downloads

- Certificate Mgmt Mode (See Cloud Configuration)

- Email Template

5.3.1 Cloud Configuration

The certificate management method can be either **Internal Certification** or **Enterprise PKI** Mode.

To change modes, select **Administration | Cloud | Certificate Mgmt Mode**. Then click **Edit** and select the relevant radio button.

- **Internal Certification:** The policy server acts as the Certificate Authority for all certificate management (creation and signing). For more information, see Cloud Configuration in Internal Certification Mode.

- **Enterprise PKI:** The policy server integrates Cloud configuration with an external Public Key Infrastructure. For more information, see Cloud Configuration in PKI Mode.

After editing, click **Save**. To commit the change, click **Commit Changes** in the toolbar.

> **Important:** Before configuring cloud settings, ensure that you have added the required cloud scanning server(s). For instructions, see Scanning Servers.

> **Warning:** After defining cloud configuration settings, switching between Internal and PKI modes will lose the settings, and you will have to re-define them (even if you do NOT save the changes).

To configure Cloud settings, select **Administration | Cloud | Configuration**. The window for configuring Cloud settings contains several tabs. The number of tabs and their names depends on the implementation mode (Internal or PKI). The mode type is displayed in the window's title bar.

To edit the tabs in the window, click **Edit**. After editing, click **Save**. To commit the change, click **Commit Changes** in the toolbar.

> Fields that are yellow are mandatory. A ⚠ symbol on a tab indicates that the tab contains a mandatory field that has not been filled in.

Cloud (Hybrid) implementation also requires the following Deployment decisions:

- Client types to be used (PC and/or Mac).

- Number, type and distribution of Cloud Scanners.

- Cloud Scanner server platform set-up

  - Private Cloud Scanner platform set-up

  - Other Cloud Scanner platform set-up (e.g. Amazon Web Services EC2 or Trustwave SWS-Hybrid)

- SWG Policy Server Configuration

  - Scanning Server device definition

  - Cloud Settings configuration in Internal Certification Mode, or

  - Cloud Settings configuration in PKI Mode

- Deployment of Mobile Security Client

- Certification and Management of Hybrid Users

5.3.1.1 Cloud Configuration in Internal Certification Mode

In **Internal Certification Mode**, the Policy Server acts as the Certificate Authority for all certificate management (creation and signing). In this mode, you designate which users are cloud users, and manage users' certificates and certification status.

You can also designate specific User Groups and LDAP Groups as dedicated Cloud groups (that is, all users in such a group are cloud users), and configure how certain cloud/certification activities should be handled for the group. For more information, see Users/User Groups and LDAP.

> When in internal certification mode only, you must configure users and email settings before starting with the Provisioning.

The recommended sequence for filling in this window (and the CA Management window) is not the same as the sequence in which the tabs appear. The following table identifies the tabs in this window. The table lists the tabs in both the sequence in which the tabs appear and the sequence in which it is recommended that you complete the procedure.

Internal Certification Mode Window – Cloud Configuration Tabs

Tabs (in GUI Sequence)	Tabs (in recommended filling in order)
• Provisioning Tab	• CA Management Window (and CA Generation Options)
• Client Configuration Tab	• Bypass Tab
• Proxies (Cloud) Tab	• Proxies (On-premise) Tab
• Proxies (On-premise) Tab	• Proxies (Cloud) Tab
• Bypass Tab	• Client Configuration Tab
• CA Management Window (and CA Generation Options)	• Provisioning Tab

5.3.1.1.1 CA Management Window (and CA Generation Options)

CA Management in Internal Mode is used to generate a certificate authority to sign SWG and mobile worker's certificates. The window is divided into two functional sections (top and bottom).

> As part of certificate management, you must identify which new cloud users (that is, the User Groups /LDAP Groups whose new cloud users) should receive the required material. You must also manage the certificates of those cloud users.
>
> These tasks are NOT performed in the Cloud Configuration window. You perform these tasks via the **User** menu option. For more information, see User Grouping and Certificate Management.

The description of this window contains the following topics:

• Top Section of the CA Management Window

• Bottom Section of the CA Management Window

• How to Use the CA Management Window

Top Section of the CA Management Window

The top section of the window contains two columns of side-by side fields:

• **Subject column** — Will hold the relevant details of the Certificate Authority that will sign the end-user certificate, once you import or generate the certificate and its details.

- **Issued By column** — Will hold the relevant details of signer of the CA certificate.

The following table describes the fields in this top section of the window. **Note**: Only the **Common Name** field is mandatory.

Internal Certification Mode Window – CA Management Tab Fields - Top Section)

Field	Description
Common Name	Generally refers to global company name but may also reference a smaller group. Mandatory.
Country Name	Generally refers to company headquarters, or the country in which the physical server sits.
State or Province	Company details
City or Locality	Company details
Organization	Company details
Organization Unit	A unit within the company, for example, specific departments such as IT or Finance.
Email	Email of the system administrator.
Expiration Date	Expiration date of the certificate issued.
Issued By	Either self-signed authority or external Certificate Authorization.

Bottom Section of the CA Management Window

The bottom of the window contains an options area that enables you to import or generate certificates:

How to Use the CA Management Window

Note: Entering a name in the **Common Name** field is mandatory.

When working in the CA Management window, you actually begin with the bottom section — you import or generate a certificate, which is then used for filling in the top details.

1. Consider (and decide) which of the following methods you will use for certification:

   - **Import a CSR-based CA certificate** — With this method, SWG generates a CSR (Certificate Signing Request), which the administrator sends to the external CA for signing; after it is signed, the system administrator imports the signed certificate.

   - **Import a CA** — This method allows the system administrator to import the certificate and private key into the system, from an external Certificate Authority.

2. Depending on the method you decided on, click **Edit**, select the **Import** check box, and then generate or import the certificate, as described in the following table.

<div align="center">Internal Certification Mode Window – Methods Using CA Management Tab</div>

Method	Steps
Import a CSR-based CA certificate	
	1. Click the **Generated CSR** link that is under the **CSR-based CA** radio button.
	The window displays fields for defining the Certificate Authority.
	2. In the **Common Name** field, specify a name for the CA (mandatory).
	3. Optionally, fill in relevant data in the other fields.
	4. Click **OK**.
	A CA Certificate request is generated and displayed in the **Generate CSR Based CA** window.
	5. Copy the Certificate request into the Clipboard buffer (so that you can provide it to the CA for signing), and click **OK**. (Note that in Internet Explorer, the window will display a **Copy to Clipboard** button that you can use.)
	6. Have the CA sign the Certificate Request.
	7. When you have received the signed CA certificate fro the CA, open the certificate details in a text editor (such as Notepad), and copy the certificate, private key, and password information into your clipboard buffer.
	Note: Certificate information must be copied precisely. This includes beginning and ending information such as spaces and dashes. It should be in base64 format (.pem)
	8. Select the **CSR-based CA** button radio button and click **Next**.
	9. In the displayed **Certificate** field, paste the signed Certificate and click **OK**.
Import a CA certificate	
	1. Select the **CA** button radio button and click **Next**.
	2. Paste the certificate information into the appropriate entry fields in the window.
	3. Click **OK**.

Regardless of the method chosen, the CA Management tab will be re-displayed, and all information provided will be displayed in the appropriate column and fields in the Top section of the window.

5.3.1.1.2 Bypass Tab

The **Bypass** tab is the same in both Internal mode and in PKI mode.

The **Bypass** tab enables you to identify non-routable networks and trusted URLs that security can bypass when you use the Mobile Security Client to browse via the Cloud Proxy or on-premise proxy.

Internal Certification Mode Window – Bypass Tab Fields

Fields/Buttons	Description
Non-routable Networks	This table shows all networks or domains (IPs) to bypass while using Mobile Security Client when browsing in Cloud Proxy or local proxy.
✚	To add a non-routable network and its details, click this icon.
Network	Network address.
Mask	Network mask.
	To delete a detail, click this icon by the detail line and select **Delete Row**.
Trusted URLs	Choose the list of URLs that you want the Cloud Proxy to bypass. This field allows the organization to bypass certain URLs that the administrator deems safe.

5.3.1.1.3 Proxies (On-premise) Tab

The **Proxies (On-premise)** tab is the same in both Internal mode and in PKI mode. An On-premise Proxy can refer to any proprietary Proxy Scanner.

Use the **Proxy (On-premise)** tab to provide the on-premise proxy details and the On-premise/Off-premise indicators.

Internal Certification Mode Window – Proxies (On-premise) Tab Fields

Field	Specify the following
On-premise Proxy Details area	Use the fields in this area to define the details of the explicit proxy servers to which roaming users will connect when they are on-premise.

Internal Certification Mode Window – Proxies (On-premise) Tab Fields

Field	Specify the following
➕	Click this icon to add a line for defining on-premise (corporate) proxy details. Then fill in the details.
Address	IP or Hostname of the on-premise proxy server.
Proxy HTTP Port	HTTP port to which roaming users will connect when on-premise.
Proxy HTTPS Port	HTTPS port to which roaming users will connect when on-premise.
On-Premise/Off-Premise Indicator area	Use this area to provide details that can only be resolved for a roaming user when that user is on-premise.
Corporate Hostname	Corporate address (for example, www.Trustwave.com). When the user is within the corporate network, this name must be resolvable to the Internal Hostname IP (see the next field in this table). When the user is outside the corporate network, this name should not be resolvable to the Internal Hostname IP.
Internal Hostname IP	IP of the corporate hostname. You can either specify this name manually, or click the **Resolve IP** button (in which case the application will look up the IP address of the internal hostname and display the results in the Internal Hostname IP field.)
Resolve IP button	Click this button to resolve the Internal Hostname IP (see the previous field in this table).
Enable on premise PAC file	Select this check box to optimize the MSC configuration by using the customer's standard PAC file when on-premise and the SWG-maintained PAC file when off-premise.
PAC file URL	If required, enter the URL address of the PAC file.

5.3.1.1.4 Proxies (Cloud) Tab

The **Proxies (Cloud)** tab is the same in both Internal mode and in PKI mode. A Cloud Proxy can refer to a Cloud Load Balancer or a Cloud Scanner.

Tip: Aim to use the provided default port values unless there are conflicts.

Use the **Proxies (Cloud)** tab to configure the server-side and client-side Cloud Proxy details.

Internal Certification Mode Window – Proxies (Cloud) Tab Fields

Field	Specify the following
Server Side area	Use the fields in this area to define the port numbers on which all Cloud Proxies and cloud-based load balances listen, and to which all clients connect.
	IMPORTANT: These port numbers must be open on the firewalls between the client and the cloud proxies regardless of client location, for example, WiFi hotspots (airports, hotels, and so on), home office, remote office.
	Note: All communications from the client to the cloud proxies is encrypted regardless of protocol or port.
Cloud Proxy HTTP Port	A server-side HTTP port number on which all cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.
	Note: The administrator can select the port number, however port 80 may not work if intermediate firewalls detect encrypted traffic. Port 443 is often open and used as the default.
Cloud Proxy HTTPS Port	A server-side HTTPS port number on which all cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.
Client Side area	Use the fields in this area to define the port numbers that the client will use to identify specific cloud scanners and load balancers.
✚	Click this icon to add a line for defining identifying details of each cloud scanner and load balancer that the client can use.
Cloud instance identifier	Internal label for this scanner/load balancer.
	A suggested use is to identify the Cloud Proxy type and location, for example, US East scanner, or EU scanner, APAC load balancer, and so on.
Address	IP Address or Hostname of the Cloud scanner/load balancer.
Local Client HTTP Port	Client-side port number used to uniquely identify a specific Cloud Proxy or cloud-based load balancer for HTTP.
	Note: This port number is internal to the client. It is used as an index to identify the cloud proxies for HTTP traffic.

Internal Certification Mode Window – Proxies (Cloud) Tab Fields

Field	Specify the following
Local Client HTTPS Port	Client-side port number used to uniquely identify a specific Cloud Proxy or cloud-based load balancer for HTTPS.
	Note: This port number is internal to the client. It is used as an index to identify the cloud proxies for HTTPS traffic.

5.3.1.1.5 Client Configuration Tab

The **Client Configuration** tab includes the following options:

- **Prevent user from disabling client:** (Selected by default) Selecting this check box ensures that the user cannot disable the agent in the browser, thereby allowing surfing through a Trustwave client only.

  Warning: Disabling the Mobile Security Client client might contravene your site's Acceptable Use Policy. Therefore, consider carefully before clearing this check box (thereby giving users the ability to disable the client).

- **Enable Client Uninstall Warning Text**: (Selected by default) Selecting this check box ensures that a warning is displayed if the user attempts to uninstall the client. This check box is accompanied by the warning text, which you can edit. This enables the Acceptable Use policy to be invoked if the client is uninstalled without permission.

This tab also contains the following options:

- **Client unable to connect to Cloud proxies when off premise:** This area enables the administrator to control how the MSC behaves when it cannot connect to any Cloud Scanners or there is no Cloud Scanner available; for example, when working in a hotel. Three options are provided:

  - **Disable** Web access

  - **Allow** direct Web access

  - **Enable "hotel mode"** for a specified duration

  Client connectivity behavior can be tuned according to company policy.

- **User certificate not present:** The administrator can force the use of a specified Security Policy if no user certificate is present.

- **Allow the Mobile Security Client to send system logs:** Instructs the client to write to system logs.

5.3.1.1.6 Provisioning Tab

Before Provisioning parameters are configured in Internal Mode, the following should be configured:

- Mail Server (see Mail Server).

- User Groups/LDAP Groups (see User Groups and LDAP Groups).

This tab contains:

- an area for defining Client Email Provisioning parameters.

- a User Certificate Security area for specifying the Mobile User Private Key password.

- Options to enable automatic client upgrades and automatic distribution of certificates.

Clients are installed for remote worker laptop computers or in situations in which the LAN desktop, whether at headquarters or a branch office, is not a domain member and the user is not authenticated with the domain. A Client can also be installed in a branch office scenario as an alternative network solution to route the traffic to the cloud scanners.

The Mobile Security Client client serves two main purposes:

- **Routing** — Routing the traffic to the nearest scanner, cloud, or on-premise scanner.

- **Authentication** — Establish mutual certificate authentication between the logged-on user and the target cloud scanner.

The Client can be installed on Windows or Mac.

The PAC file defines how browsers can automatically choose the appropriate proxy server for retrieving a given URL. PAC files contain a "FindProxyForURL(url, host)" function that returns a string with one or more access method specifications. These specifications cause the user to use a particular proxy server or to connect directly.

Trustwave provides a PAC file for your use, but a third-party PAC file can be used instead. If the third party PAC file will be used, the **Enforce Trustwave PAC file usage** check box in the **Client Configuration** tab must be cleared, and the local host proxy within the PAC file must belong to Trustwave.

After Cloud configuration, you can download the desired Windows Client Installer, PAC, or Mac Client Installer files from **Administration | Cloud | Downloads.**

These files can only be downloaded after you have configured all mandatory settings in the other tabs.

Internal Certification Mode Window – Provisioning Tab Fields

Field/Check box	Description
Client Email Provisioning area	

Administration
268

Internal Certification Mode Window – Provisioning Tab Fields

Field/Check box	Description
Client Installer URL	Location from which the administrator wants the users to download the Client Installation package. **Note:** This is required in Internal Mode.
Automatically send an email with provision instructions to new cloud members	Select this check box (default) if the Policy Server should automatically send emails with provisioning instructions to new cloud users.
Send an email update upon configuration changes	Select this check box (default) if the Policy Server should automatically send emails to existing cloud users notifying them that relevant changes have been committed.
User Certificate Security area	
Mobile User Private Key Password	Specify the password that the end user will use when installing the certificate. (Mandatory)
Confirm Private Key Password	Confirm the password. (Mandatory)
Enable automatic client upgrade	Select this check box if all upgrades should be applied automatically. This option increases control of the roll-out of client code (MSC) by allowing the Administrator to enable or disable automatic client code updates globally.
Enable automatic distribution of certificates	Select this check box if certificates should be distributed automatically.

5.3.1.2 Cloud Configuration in PKI Mode

In **Public Key Infrastructure (PKI) Mode**, the Policy Server integrates Cloud configuration with an external Public Key Infrastructure.

In this mode, identification and certification of cloud users is performed externally and independently of SWG. Therefore, in **PKI** mode, you do not manage cloud users or their certificates, and there is no designation or configuration of groups as cloud groups.

The recommended sequence for filling in the tabs in this window is not the same as the sequence in which the tabs appear. The following table identifies the tabs in this window. The table lists the tabs in both the sequence in which the tabs appear and the sequence in which it is recommended that you complete the procedure.

Tabs (in GUI Sequence)	Tabs (in recommended filling in order)
• Provisioning Tab	• Proxies (Cloud) Tab
• Client Configuration Tab	• Proxies (On-premise) Tab
• Proxies (Cloud) Tab	• Certificate Management Tab - PKI Mode
• Proxies (On-premise) Tab	• Bypass Tab
• Bypass Tab	• Client Configuration Tab
• Certificate Management Tab - PKI Mode	• CRL Handling Tab
• CRL Handling Tab	• Provisioning Tab

5.3.1.2.1 Proxies (Cloud) Tab

- The **Proxies (Cloud)** tab is the same in both Internal mode and in PKI mode. A Cloud Proxy can refer to a Load Balancer or a Cloud Scanner.
- Be sure not to confuse the Local ports and Listening ports.
- **Tip:** Aim to use the provided default port values unless there are conflicts.

Use the **Proxies (Cloud)** tab to configure the server-side and client-side Cloud Proxy details.

Cloud Configuration in PKI Mode – Proxies (Cloud) Tab Fields

Field	Specify the following
Server Side area	Use the fields in this area to define the port numbers on which all Cloud Proxies and cloud-based load balances will listen, and to which all clients will connect.
	IMPORTANT: These port numbers must be open on the firewalls between the client and the cloud proxies regardless of client location, for example, WiFi hotspots (airports, hotels, and so on), home office, remote office.
	Note: All communications from the client to the cloud proxies is encrypted regardless of protocol or port.
Cloud Proxy HTTP Port	A server-side HTTP port number on which all cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.
	Note: The administrator can select the port number, however port 80 may not work if intermediate firewalls detect encrypted traffic. Port 443 is often open and used as the default.
Cloud Proxy HTTPS Port	A server-side HTTPS port number on which all cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.

Cloud Configuration in PKI Mode – Proxies (Cloud) Tab Fields

Field	Specify the following
Client Side area	Use the fields in this area to define the port numbers that the client will use to identify specific cloud scanners and load balancers.
✚	Click this icon to add a line for defining port details.
📋	Click this icon to increase or decrease the priority of the selected item (and move it up or down the list).
Cloud instance identifier	Internal label for this scanner/load balancer. A suggested use is to identify the Cloud Proxy type and location, for example, US East scanner, or EU scanner, APAC load balancer, and so on.
Address	IP Address or Hostname of the Cloud scanner/load balancer.
Local Client HTTP Port	Client-side port number used to uniquely identify a specific Cloud Proxy or cloud-based load balancer for HTTP. Note: This port number is internal to the client. It is used as an index to identify the cloud proxies for HTTP traffic.
Local Client HTTPS Port	Client-side port number used to uniquely identify a specific Cloud Proxy or cloud-based load balancer for HTTPS. **Note:** This port number is internal to the client. It is used as an index to identify the cloud proxies for HTTPS traffic.

5.3.1.2.2 Proxies (On-premise) Tab

The **Proxies (On-premise)** tab is the same in both Internal mode and in PKI mode. A Cloud Proxy can refer to any proprietary Proxy Scanner.

Use the **Proxy (On-premise)** tab to provide the on-premise proxy details and the On-premise/Off-premise indicators.

Cloud Configuration in PKI Mode – Proxies (On-premise) Tab Fields

Field	Specify the following
On-premise Proxy Details area	Use the fields in this area to define the details of the explicit proxy servers to which roaming users will connect when they are on-premise.

Field	Specify the following
✚	Click this icon to add a line for defining on-premise (corporate) proxy details. Then fill in the details.
Address	IP or Hostname of the on-premise proxy server.
Proxy HTTP Port	HTTP port to which roaming users will connect when on-premise.
Proxy HTTPS Port	HTTPS port to which roaming users will connect when on-premise.
On-Premise /Off-Premise Indicator area	Use this area to provide details that can only be resolved for a roaming user when that user is on-premise.
Corporate Hostname	Corporate address (for example, www.Trustwave.com). When the user is within the corporate network, this name must be resolvable to the Internal Hostname IP (see the next field in this table). When the user is outside the corporate network, this name should not be resolvable to the Internal Hostname IP.
Internal Hostname IP	IP of corporate hostname. You can either specify this name manually, or click the **Resolve IP** button (in which case the application will look up the IP address of the internal hostname and display the results in the Internal Hostname IP field.)
Resolve IP button	Click this button to resolve the Internal Hostname IP (see the previous field in this table).
Enable On-premise PAC File	Select this check box to use a non-Trustwave PAC file. Then enter the URL of the PAC file.

5.3.1.2.3 Certificate Management Tab - PKI Mode

The **Certificate Management** tab is used to generate Certificates.

The top section of the tab includes:

- **CA Certificate** column — Will hold the relevant details of the Certificate Authority certificate, once you generate the certificate.

- **Server Certificate** column — Will hold the relevant details of the Server certificate, once you generate the certificate.

- **Generic Certificate** column — Will hold the relevant details of the Generic certificate, once you generate the certificate.

Cloud Configuration in PKI Mode – Certificate Management Tab Fields

Field	Description
Common Name	Generally refers to global company name but may also reference a smaller group. Mandatory.
Expiration Date	Expiration date of the certificate issued.

How to Use the Certificate Management Tab

When working in the Certificate Management tab, you actually begin with the bottom section, and perform the following tasks, in sequence:

1. Enter the **EKU** (Extended Key Usage) Object ID provided by the domain administrator. This property allows the client to identify the certificate with which it should connect to cloud scanners. The domain administrator defines this EKU and must use it in the certificate template from which all cloud users certificates are created.

2. Ensure the **Generate Certificates** check box is selected and click **Save** to automatically generate the CA Certificate, Server Certificate and Generic Certificate. The certificate details are shown in the relevant columns.

5.3.1.2.4 Bypass Tab

The **Bypass** tab is the same in both Internal mode and in PKI mode.

The **Bypass** tab enables you to identify non-routable networks and trusted URLs that security can bypass when you use the Mobile Security Client to browse via the Cloud Proxy or on-premise proxy.

Cloud Configuration in PKI Mode – Bypass Tab Fields and Buttons

Fields/Buttons	Description
Non-routable Networks	This table shows all networks or domains (IPs) to bypass while using Mobile Security Client when browsing in Cloud Proxy or local proxy.
✚	To add a non-routable network and its details, click this icon.
Network	Network address.
Mask	Network mask.
📋	To delete a detail, click this icon by the detail line and select **Delete Row**.
Trusted URLs	Choose the list of URLs that you want the Cloud Proxy to bypass. This field allows the organization to bypass certain URLs that the administrator deems safe.

5.3.1.2.5 Client Configuration Tab

The **Client Configuration** tab includes three check boxes, each selected by default.

- **Prevent user from disabling client:** Selecting this check box ensures that the user cannot disable the client in the browser, thereby allowing surfing through a Trustwave client only.

> **Warning:** Disabling the Mobile Security Client might contravene your site's Acceptable Use Policy. Therefore, consider carefully before clearing this check box (thereby giving users the ability to disable the client).

- **Enforce PAC file usage via the Mobile Security Client:** Selecting this check box assures that the PAC file being used is a Trustwave PAC file. Administrators should keep this check box cleared if a proprietary PAC file is used.

> If Enforce PAC file usage via the Mobile Security Client is enabled, any changes implemented after the initial installation requires the browser to be restarted before the changes can take effect. This is for all browsers including Internet Explorer, Firefox, Google Chrome and Safari.

- **Enable Client Uninstall Warning Text**: Selecting this check box ensures that a warning is displayed if the user attempts to uninstall the client. This check box is accompanied by the warning text, which you can edit.

- **Client unable to connect to Cloud proxies when off premise:** This area enables the administrator to control how the MSC behaves when it cannot connect to any Cloud Scanners or there is no Cloud Scanner available; for example, when working in a hotel. Three options are provided:

  - **Disable** Web access

  - **Allow** direct Web access

  - **Enable "hotel mode"** for a specified duration

  Client connectivity behavior can be tuned according to company policy.

- **User certificate not present:** The administrator can force the use of a specified Security Policy if no user certificate is present.

- **Allow the Mobile Security Client to send system logs:** Instructs the client to write to system logs.

5.3.1.2.6 CRL Handling Tab

The Certificate Revocation List (CRL) is a list of all revoked certificates. The list specifies each revoked certificate, the entity that issued it, the date of certificate issue, the reason for revocation, and a proposed date for the next release of the CRL.

When a user tries to access a server, the server allows or denies access based on specific CRL entries.

CRL handling is defined in the **CRL Handling** tab. In this tab, you specify the location of the CRL list and an optional schedule for automatically retrieving that latest CRL list. You can also run a test to check that the specified CRL location is accessible.

<div align="center">Cloud Configuration in PKI Mode – CRL Handling Tab Fields</div>

Field	Description
Enterprise CA CRL location area	
entry-field	HTTP or HTTPS location of the CRL. LDAP is not an option in this field. For example, http://ntydc2.ila.sun85.local/certenroll/nty-ca.crl
Test Location	Click this button to test that the location of the address entered in the **Enterprise CA CRL location** field is accessible.
Scheduling area. Choose one of the following, and set the values:	
Run daily at	Click, and set a specific time (hh:mm) that retrieval should be performed each day.
Run every	Click, and set a time interval (in hours) at which retrieval should run (e.g., every 2 hours)
No Scheduling	No automatic scheduling (default). Retrieval is performed only upon manual request (made by clicking the **Retrieve Now** button).
Retrieve now	Click this button to issue a manual retrieval request. (**Note**: This button is only active when *not* in **Edit** mode)

5.3.1.2.7 Provisioning Tab

> You can only use this tab after you have configured all mandatory settings in the other tabs.

In **Enterprise PKI** mode, the **Provisioning** tab contains only the **Enable automatic client upgrade** check box.

Select this check box if all upgrades should be applied automatically. This option increases control of the roll-out of client code (MSC) by allowing the Administrator to enable or disable automatic client code updates globally.

5.3.2 Downloads

After Cloud configuration, you can choose to download one of the following:

• Windows Client Installer

• PAC File

- Mac Client Installer

  You can only download after you have configured all mandatory settings in the other tabs. If necessary, click the relevant link in the Notifications area of the Downloads tab (**Administration | Cloud | Downloads**).

You use this tab to download the Client Installer or PAC (Proxy Auto-Configure) file.

The following paragraphs provide some information about Clients and the PAC File:

Clients are installed for remote worker laptop computers or in situations in which the LAN desktop, whether at headquarters or a branch office, is not a domain member and the user is not authenticated with the domain. A Client can also be installed in a branch office scenario as an alternative network solution to route the traffic to the cloud scanners.

The Mobile Security Client serves two main purposes:

- Routing the traffic to the nearest scanner, cloud, or on-premise scanner.

- Establishing mutual certificate authentication between the logged-on user and the target cloud scanner.

The PAC file defines how browsers can automatically choose the appropriate proxy server for retrieving a given URL. PAC files contain a "FindProxyForURL(url, host)" function that returns a string with one or more access method specifications. These specifications cause the user to use a particular proxy server or to connect directly.

Trustwave provides a PAC file for your use, but you can choose to use a third-party PAC file instead.

To use a third party PAC file, you must clear the **Enforce Trustwave PAC file usage** check box in the **Client Configuration** tab, and ensure that the local host proxy within the PAC file belongs to Trustwave.

5.3.3 Email Template

The email template is relevant only if the cloud is implemented in Internal mode.

The Secure Web Gateway provides several predefined email templates that SWG uses when sending emails during different stages of the provisioning/certification process. These templates are also used when administrators manually send provisioning emails to users.

You can edit these templates in the **Email Template** window (accessed via under **Administration | Cloud | Email Template**). When editing an email template, you can modify the contents of the **From**, **Subject** and **Message** fields, including adding dynamic-parameter placeholders.

You can also view the message contents in HTML format.

To edit a template, click **Edit**. After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

<div align="center">Email Template Window Fields and Buttons</div>

Field/Button	Description
Provisioning Email Template	Select the email type to be edited from the following drop down list.
Standard Template	Email is sent with the certificate attached.
Standard Template for Re-installation	Email is sent to inform user that a certificate was re-issued and that the user should follow the included instructions.
Template with Client	Email arrives with both a certificate and link to the Client installation.
Template with Client for Re-installation	Email arrives with both a certificate and link to the Client installation after certificate has been re-issued or a new Client added.
From area	
entry-field	Sender of the email. Default: Explicit value of the **Sender** field in the Mail Server configuration page.
Add placeholder	Adds a Policy Server Hostname placeholder.
✚	Click to append the selected placeholder to the end of the From value.
Subject area	
entry-field	Subject to be included in the email
Add placeholder	Can add a placeholder for the MSC Client installer URL and/or the recipient's user name.
✚	Click to insert the selected placeholder at the current cursor location in the Display area.
display area	Displays the message text and placeholders as it is (being) defined at the moment.
HTML view button	Displays how the message will appear to the user.

5.4 Policy Server DB Backup

The Policy Server Database Backup feature (backup and restore) is used to restore the system back to a previous stable state. This, of course, requires that you have a backup to which you can restore the system.

A backup consists of all data that an administrator can customize in the Management Console (including Policies, settings and so on). **Note**: System backups do not include information in the Log Server database, Report Server database and Updates.

The Backup and Restore feature is useful at various times, including the following:

- Before applying major configuration and settings changes, the administrator can back up the current settings.

- The administrator may choose to have periodic backups of the system to guarantee against unknown catastrophes.

- In the rare instance that a failed update caused the system to function incorrectly, it might be useful or necessary to perform a restore.

- In the rare instance of a system hardware failure (for example, if the hard disk of the Policy Server stopped working), it might be useful or necessary to perform a restore on a different machine after replacing the HDD.

Backups are saved to an external location. Before the system can be backed up, it must be configured with necessary backup information such as the target location of the backup file and connection details.

You can define a schedule for the automatic performance of backups, and you can manually perform an immediate backup (on demand).

The Backup feature has the following windows:

- Backup Settings Window — Used for configuring the backup details, such as location and connection details, and for configuring an automatic backup schedule.

- Backup Now Window — This window lets you manually perform an immediate backup.

- Backup Restore Window — Provides a list of available backups. From this list, you can choose which one to restore.

5.4.1 Backup Settings Window

During the backup process, the Policy Server settings are saved to an external network location (using an external location helps ensure a smooth system restore process after a failed hardware has been replaced).

Before backup can be performed, you must configure location, connection, and other required details. You do this in the Backup Settings window (accessed via **Administration | Policy Server DB Backup | Backup Settings**).

To provide/edit the details, click **Edit**. After editing, click **Save**. To commit the changes, click **Commit Changes** in the toolbar.

The following topics describe the fields/buttons of this window:

- Connection Method and associated Location, User, and Password fields

- Scheduling fields

- Check Connection check box

Connection Method and associated Location, User, and Password fields

Connection Method — Select the connection method that SWG should use to connect to the Backup file storage location. Valid Values:

- **FTP** — Connect using regular File Transfer Protocol.

- **FTP Passive** — Connect using File Transfer Protocol (there is a firewall located between the Policy Server and the remote FTP site).

- **Samba** — Connect using Server Message Block (SMB) communication protocol.

- **SFTP** — Connect using Secure File Transfer Protocol (available for System backups only).

The selected Connection method determines the format of the **Backup Location**, **User** Name and **Password** values that you must provide. The following table describes these formats, depending on the connection method.

Backup Settings - Connection Methods

Connection Method	Backup Location, User Name, and Password Format
FTP, FTP Passive, or SFTP	**Backup Location** format is: • For **FTP** or **FTP Passive**: *<server_ip_address>*/**dir** (for example, 10.194.5.104/Sarah_FTP) • For **SFTP**: *<server_ip_address>* (for example, 10.194.5.104/). **User to connect with** is the user name used when connecting to the Backup Location. **Password** should be the password used by the user connecting to the Backup Location.
Samba	**Backup Location** must include the server IP address and directory for your selected location, in the following format: **//***<server_ip_address>*/**dir**, (for example, //192.168.1.10/backup.) **User to connect with** must include the workgroup name and the user name used when connecting to the Backup Location, in the following format: workgroup/user, for example, marketing/nicole. **Password** should be the password used by the user connecting to the Backup Location.

Scheduling fields

To enable automatic scheduling of backups, select the **Enable scheduling** check box, and then define a schedule:

- In the **Every _n_ days** field, specify the number of days between backups.

- In the **Starting at** field, specify the time (hh:mm) that backup should begin.

Check Connection check box

To verify the connection to the backup location you defined in this window, select the **Check connection** check box before performing a **Save**. The connection will be tested during the **Save**.

5.4.2 Backup Now Window

The **Backup Now** window lets you manually perform a backup when desired, regardless of automatic scheduling.

For example, you might want to manually perform a backup before applying updates, or before performing major configuration or making changes to your system.

> Before you can perform a manual backup, you must first ensure that the location/ connection parameters in the Backup Settings Window are configured.

To perform a manual backup, display the Backup Now window (**Administration | Policy Server DB Backup | Backup Now**), and in the **Name/Description** field specify an identifying name and/or description. Then click **Backup**.

The Backup file details will appear in the **Restore** screen.

5.4.3 Backup Restore Window

> If High Availability is enabled, you must disable the High Availability Policy Server feature before performing the restore.

The Backup Restore window displays a table that lists the available backups (scheduled and manual), so that you can choose which backup to restore.

After you select the backup for the restore, a prompt requests confirmation that you want to perform the restore. Confirm the request.

When the restore is performed, the settings are read from the backup file and uploaded back on to the disk.

The following table describes the columns in the table that lists the available backups.

Restore Window Options

Column	Description
	Click the icon next to the backup that you want to restore, and select **Restore**. At the prompt, confirm that you want to perform the restore.
Date	Date the backup was performed.
Type	The options are as follows: • **Manual** – Backup was created manually • **Scheduled** – Backup was scheduled for specific times • **Automatic** – Backup was created automatically prior to a Trustwave Operating System update
Version	Trustwave Operating System version in use when backup was created.
Description	Description of the backup file.

5.5 Reports DB Backup

Partitioning of the Reports database is done on a weekly basis, and as such, provides all reports data from the previous week.

Using the **Reports DB Backup** feature, administrators can backup and restore data that has been backed up from the Reports database.

To enable Reports Database Backup, appropriate backup settings, such as location of the backup file and connection settings must be configured.

You can enable automatic performance of backups, and you can manually request backup on demand.

The **Reports DB Backup** feature has the following windows:

• Backup Settings Window

• Backup Restore Window

5.5.1 Backup Settings Window

Before Reports DB backup can be performed, you must configure location, connection, and other required details. You do this in the **Backup Settings** window (accessed via **Administration |Reports DB Backup | Backup Settings**).

This window also contains a:

• button to let you check the connection that you defined.

• check box that lets you enable automatic backup.

- **Backup Now** button, to request an ad-hoc, manual backup.

To provide/edit the details, click **Edit**. After editing, click **Save**. To commit the changes, click ![icon]
Commit Changes in the toolbar.

The following topics describe the fields/buttons of this window:

- Connection Method and associated Location, User, and Password fields

- Backup Area

Connection Method and associated Location, User, and Password fields

Connection Method — Select the connection method that SWG should use to connect to the Backup file
storage location. Valid Values:

- **FTP** — Connect using regular File Transfer Protocol.

- **FTP Passive** — Connect using File Transfer Protocol (but there is a firewall located between the Policy
  Server and the remote FTP site).

- **Samba** — Connect using Server Message Block (SMB) communication protocol.

- **SFTP** — Connect using Secure File Transfer Protocol (available for System backups only).

The selected Connection method determines the format of the **Backup Location**, **User** Name and
Password values that you must provide. The following table describes these formats, depending on the
connection method.

Backup Settings Window – Connection Methods

Connection Method	Backup Location, User Name, and Password Format
FTP, FTP Passive, or SFTP	**Backup Location** format is: • For **FTP** or **FTP Passive**: **<server_ip_address>/dir** (for example, 10.194.5.104/Sarah_FTP) • For **SFTP**: **<server_ip_address>** (for example, 10.194.5.104/). **User to connect with** is the user name used when connecting to the Backup Location. **Password** should be the password used by the above user.
Samba	**Backup Location** must include the server IP address and directory for your selected location, in the following format: **//<server_ip_address>/dir**, (for example, //192.168.1.10/backup.) **User to connect with** must include the workgroup name and the user name used when connecting to the Backup Location, in the following format: workgroup/user, for example, marketing/nicole. **Password** should be the password used by the above user.

Check Connection check box — To verify the connection to the backup location you defined in this window, select this check box before performing a **Save**. The connection will be tested during the **Save**.

Backup Area

To enable automatic scheduled backups, select the **Enable automatic backup** check box. Automatic backup will then be performed weekly, and include the data in the weekly partition.

To perform an ad-hoc, manual backup, click the **Backup Now** button.

> **Warning:**
>
> - Before the manual backup can be performed, you must click **Save**, and then click **Commit Changes** in the toolbar.
>
> - This action runs a backup of all data in the Reports database, beyond the one week partition. It does not change previously configured settings (that is, the Connection method, location, and other settings remain unchanged).

# 5.5.2 Backup Restore Window

The **Backup Restore** window displays a table that lists the available Report DB backups (scheduled and manual), so that you can choose which backup to restore.

After you request the restore, a prompt requests confirmation.

> **Warning:** As indicated in the confirmation prompt, if you choose to proceed with the restore, the restore data will overwrite any pre-existing data in the partition. Consider carefully before confirming the restore.

When the restore is performed, the selected Reports data will be restored to the system (and overwrite the current partition(s). Note that the **Database Restore** action does not change previously configured settings (that is, the location and Connection method information remain unaffected).

You can check the System log to verify that the operation was successful.

The following table describes the columns in the table that lists the available backups.

<div align="center">Backup Restore Window – Available Backups</div>

Column	Description
	Click the icon next to the backup that you want to restore, and select **Restore**.
Date	Date the backup was performed.

5.6 Export/Import

Administrators can export Security, HTTPS, Identification, the Logging policy database, and condition options on a Policy Server to a file. They can then import policies, rules, conditions, and condition options from the exported database file into the same Policy server or the Policy Server of another SWG.

5.6.1 Export

Administrators can export Security, HTTPS, Identification, the Logging policy database, and condition options on a Policy Server to a file.

The exported information is encrypted.

To perform an export:

- Select **Administration | Export/Import | Export**. A prompt message (not a window) is displayed. At the prompt, choose **Save**.

- Depending on your workstation configuration, either the exported file will be saved in your default location (for example, **Downloads**), or you will be able to browse to/specify the desired path.

5.6.2 Import Database Window

To import files to a Policy Server, you must be logged into the target SWG.

You perform imports on the **Import Database** page (accessed via **Administration | Export/Import | Import**). The tree pane of this window has a root node called **Database Files**, under which it displays the imported Policy Databases on this Policy Server.

You can import the following types of objects from exported database files, which will then appear in corresponding sections in GUI:

- Policies (and their Rules and Conditions)

- Condition Component settings (that is, settings related to the **Policies | Condition Elements** menu)

When importing items that have the same name as existing items, to avoid potential conflicts, you can choose to leave the existing items in place. overwrite existing items, or save the imported items under different names.

This section contains the following topics:

- Importability of Policies and Condition Element Settings

- Database Files Tree

- Export/Import Troubleshooting

5.6.2.1 Importability of Policies and Condition Element Settings

Policies and Conditions have different import options available for them as a function of administrator permissions and other object properties.

When determining if a Policy or Condition Element can be imported, the following criteria is used:

- Importing Policies criteria:

  - One of the following situations exist:

  All Conditions attached to a Policy Rule can be imported

  Or

  The Condition is already present in the target database

  - The administrator, performing an Action, has update permissions for the policy type including the appropriate license for the appliance.

- Importing Condition Element settings:

  - The administrator, performing an Action, has update permissions for the object class including the appropriate license for the appliance.

The following table outlines the available actions dependent on the administrators class and object permissions as described in Default Permissions.

Importability of Policies and Condition Component Settings

Object Existence Status	Class Permission			
	None/View		Update	
	Object Permission			
	None/View	Update	None/View	Update
Object exists in target database	Leave Original	Leave Original Overwrite	Leave Original Rename	Leave Original Overwrite Rename
Object does not exist in target database	Cannot Be Imported		Add As Is Rename	

5.6.2.2 Database Files Tree

Once you have imported the back-up file, the following nodes appear in the **Database Files** tree:

- Policies
- Conditions

Importing a Policy:

Expand the tree in the left pane, right-click the respective Policy, and select **Import**. The Policy Import pane is displayed.

Database Files Tree – Policy Import Fields

Field	Description
Policy Name	Name of the Policy
Action	The available actions may vary depending on the policy being imported. You can select from a drop down list to:
	Rename: This action enables you to rename the Policy so as not to overwrite an existing Policy with the same name.
	Add as is: This action imports the Policy to the Management Console as is.
	Leave Original: This action leaves the original policy as is. This choice allows changes to one or more policy conditions while leaving the remaining conditions unchanged**.**
	Overwrite: This action imports the Policy to the Policy Server thereby overwriting the Policy that exists with the same name.
New Name	If you have chosen **Rename** in the **Action** above, then enter the new name for the Policy in this field.
Conditions	Conditions attached to this Policy can also be selected for the following actions:
	Rename: This action enables you to rename the Condition so as not to overwrite an existing Condition with the same name. On **Rename**, enter the new name for the condition in the New Component Name column.
	Add as is: This action imports the condition to the Management Console as is.
	Leave Original: This action leaves the original Condition as is, while the Policy change affects the other Conditions attached to it.
	Overwrite: This action imports the Condition to the Policy Server thereby overwriting the Condition that exists with the same name.
	The available actions may vary depending on the Condition being imported.

Importing a Condition Element Setting

Expand the tree in the left pane, right-click the respective Condition, and select **Import**. The Condition Element Import pane is displayed.

<div align="center">Database Files Tree – Condition Element Setting Fields</div>

Field	Description
Name	Name of the Condition Element setting.
Action	You can select from a drop down list to:
	Rename: This action enables you to rename the Condition Element so as not to overwrite an existing Condition Element with the same name.
	Add as is: This action imports the Condition Element to the Management Console as is.
	Leave Original: This action leaves the original Condition Element as is**.**
	Overwrite: This action imports the Condition Element to the Policy Server thereby overwriting the Condition Element that exists with the same name.
	The available actions may vary depending on the Condition Element being imported.
New Name	If you have chosen **Rename** in the **Action** above, then enter the new name for the Condition Element in this field.

You can perform either of the following procedures in this window:

- To import policies, rules, and conditions from an exported database file:

- To import condition options from an exported database file:

To import policies, rules, and conditions from an exported database file:

1. Select the **Database Files** (root) node (or alternatively right-click it and choose **Import Policies**).

2. Then, in the main window, browse to and select the file to be imported, and click **Import**. The folders for import appear in the **Import Policies** tree.

3. Select and import the policy as follows:

4. Expand the tree pane, and right-click the policy that you want to import and choose Import.

    The policy import window is displayed.

    a. Select the desired action:

    - To change one or more policy conditions while leaving the remaining unchanged, choose **Leave original**.

- To completely overwrite the existing policy with the imported policy having the same name, choose **Overwrite**.

- To rename the policy so as not to overwrite the existing policy with the same name, choose **Rename**, and specify the new name for the policy.

b. For individual conditions that are displayed in the Conditions table, select the desired actions (the same actions available for the policy in **Step a** are available for conditions).

c. If you chose to rename conditions, specify their new names in the **New Element Name** column.

d. Click **OK**.

- After importing any policy, be sure to check that it reflects the new licensed engine.

- Policies/Condition options that cannot be imported are not displayed in the import tree.

- After the import process all rules referring to engines that are not licensed, are not displayed in the policies.

5. If you are ready to distribute and implement the changes in your system devices, click **Commit Changes** in the toolbar.

To import condition options from an exported database file:

The procedure is used to import sets of condition options (such as appear under **Policies | Condition Elements**; for example, File Extension Lists, URL Lists) from an exported database file.

1. Select **Administration | Export/Import | Import**.

   The Import window is displayed.

2. Expand the tree pane, and right-click the condition that you want to import and choose Import.

   The element import window is displayed.

3. Select the desired action:

   - To leave the original conditions unchanged, choose **Leave original**.

   - To overwrite the existing condition with the imported condition of the same name, choose **Overwrite**.

   - To rename the condition so as not to overwrite the condition with the same name, choose **Rename**, and specify the new name for the condition.

4. Click **OK**.

5. If you are ready to distribute and implement the changes in your system devices, click **Commit Changes** in the toolbar.

5.6.2.3 Export/Import Troubleshooting

When importing a Condition from one Policy Server to another and one of the components in the Condition does not exist on the target Policy Server, and it is due to one of the Trustwave predefined lists having an added component, an error message is displayed.

To solve this issue, make sure you have the latest Security Update Version installed on the target Policy Server and repeat the Import process.

5.7 Updates and Upgrades

Under **Administration | Updates and Upgrades** are two options, each displaying its own window:

- **Management** — Displays the Updates and Upgrades Management Window

- **Configuration** — Displays the Updates and Upgrades Configuration Window

5.7.1 Updates and Upgrades Management Window

The **Updates and Upgrades Management** window (accessed via **Administration | Updates and Upgrades | Management**) enables you to:

- view the list of updates available for installation, and upload and install the updates, as needed

- view the list of updates which are already installed

- generate a key, if needed for downloading updates

> The Generate a Key feature is intended for customers who use the appliance in an isolated network not connected to the Internet, and who must instead download updates using an Offline Updates application. This feature requires a special license.
>
> For more information on Offline Updates, contact your Trustwave representative and/ or refer to the **_Offline Updates Technical Brief_**.

This window contains the following tabs:

- Available Updates Tab

- Installed Updates Tab

- Update Key Tab

5.7.1.1 Available Updates Tab

The **Available Updates** tab displays a table that lists currently available updates and provides options for uploading local or remote updates to be installed. You can filter the list by selecting an **Update type** from the drop down list and clicking **Apply**.

- If you are working remotely, click the **Retrieve Updates** button to display available updates.

- If you are working locally, click the **Import Updates** button (see the description in the following table) to import updates.

Updates Management Window – Available Updates Tab Fields and Buttons

Field/Button	Description
⊞	Click to display the relevant Release Information. (You can then click the link to view the associated Release Notes, if applicable.)
(icon)	To install an update, click this icon next to the update and select **Install Now**. (To delete an update, click this icon next to the update and select **Delete**.).
Status	This column indicates the retrieval status of the available update. (icon) — Indicates that an available update has been retrieved successfully. (icon) — Indicates that an available update is in the process of being uploaded/installed. (icon) — Indicates that an upload/install has failed.
Type	Type of update is available (for example, security update, software release update, maintenance update).
Release Date	Date and time the release became available for update (*YYYY:MM:dd HH:mm:ss*)
Description	Brief description of the available update.
Retrieve Updates button	If you are working remotely, to retrieve (all) updates, click this button; then wait for the updates to be loaded. Each successfully retrieved update detail will have a check mark in the **Status** column of the detail line.
Import Updates button	Click this button to install an update when the update file is saved locally. This will display the Import Local Update screen. In the Import Local Update screen, do either of the following, and then click **Import**: • Fill in the URL where the updates reside, or • Browse to the local location where the updates reside (provided by Trustwave)

5.7.1.2 Installed Updates Tab

The Installed Updates tab displays the updates both automatically and manually installed. You can filter the list by selecting an **Update type** from the drop down list and clicking **Apply**.

Updates Management Window – Installed Updates Tab Fields and Buttons

Field	Description
➕	Click to expand. The Installed Update will display the relevant Release Information. Click the link to view the associated Release Notes (if applicable)**.**
Type	Type of update installed (for example, security update, software release update, maintenance update).
Release Date	Date and time the release became available for update (YYYY:MM:dd HH:mm:ss).
Install Date	Date the release was installed (YY:MM:DD HH:MM:SS).
Description	Brief description of the available update.

5.7.1.3 Update Key Tab

The **Update Key** is primarily designed for customers who are using the appliance in an isolated network that is not connected to the Internet.

Using this key, you can download updates using an Offline Updates application.

> This feature requires a special license. For more information on Offline Updates, contact your Trustwave representative and/or refer to the *Offline Updates Technical Brief.*

To generate the Update Key:

1. Click **Generate Key**. The key is generated and appears in the tab.

2. Select and copy the key to the clipboard or click **Copy to Clipboard**.

> The **Copy to Clipboard** button exists only for users of Internet Explorer. Firefox users will not have this option.

5.7.2 Updates and Upgrades Configuration Window

The **Updates and Upgrades Configuration** window (accessed via **Administration | Updates and Upgrades | Configuration**) enables you to configure:

- the proxy to be used for update routing if the Internet connection is blocked for the SWG appliance.

- whether updates should be checked for automatically or manually; and if automatically, how often.

- the install policy for available updates; **Download** (automatically), **Download and Install** (automatically), or **Do nothing** (download and install manually).

- exceptions to the check for updates configuration and the install policy - by update type.

To edit the configuration, click **Edit**. When done, click **Save**. To commit the changes, click ⬇ **Commit Changes** in the toolbar.

Updates Configuration Window Areas and Fields

Area/Field	Description
Proxy Configuration area	In this area, you configure the proxy that should be used for update routing if the Internet connection is blocked for the SWG appliance.
Proxy Server	IP of the next proxy server
Port	Port of the next proxy server
User Name	User Name required to access the next proxy server
Password	Password required to access the next proxy server
Scheduling Configuration area	In this area, you configure the default and exception check schedule and install policy for available updates.
Check for Updates	Select the relevant radio button to configure how often the check is performed automatically, or whether the check is performed manually only.
Install Policy	From the drop down list, select how available updates must be handled: Downloaded automatically, downloaded and installed automatically, or downloaded and installed manually.
Except For	If applicable, use the **Add Exception** button ➕ to configure any update types that should NOT follow the default **Check for Updates** and **Install Policy** settings. Then specify a unique install policy for that type. You can click **Revert to default** ✗ to restore an exception update type to the default check schedule and install policy.

5.8 Alerts

Through the Alerts mechanism, SWG can notify you of system events, application events, update events, and security events.

The following table indicates the alerts available for each type of system event.

Alerts Window – Available Alerts

Event Type
Details included in the event
System Events
Hard Drive Threshold, System Load, Memory Usage Threshold
Application Events
Emergency Policy Selected, Archive Upload Failed, Backup Failed, Log Handler Down, Scanning Process is Unexpectedly Down, License Expiry, License Modification or Update, Active/Standby Policy Server, No Connection to Policy Server for Past Hour. Security Updates are Not Installed! Connection to Policy Server Restored, Connection to Email Server Failed
Update Events
OS Update Available, Security Update Available, Security Update Failed, OS Update Failed, Security Update Successfully Installed, OS Update Successfully Installed, Could Not Download the Update File, Error in Validating Checksum, Update Failed due to Internal Error, Received Update with Unsupported Version, Update Exceeded Maximum Installation Time, Could not find the Update File, The Update File was not Created Properly, Update Installed Successfully, OS Update Available, Security Updates Available, Update Added to Available Updates, Update already Installed, Update already Exists, A Later Version of Update Exists, Installing Update, Update Dependence Problem, All Scanners in the topology must have the same Trustwave Operating System as Policy Server before you start Update Process, Update Installer - Cannot install OS Update when Standby Policy Server Trustwave Operating System is different from Active Policy Server Version
Security Settings
Anti-Virus triggered (settings configurable), Behavior Analysis (settings configurable), Blocked URL List (settings configurable), URL Filtering (settings configurable)

SWG can send alerts through two different communication channels (besides System Log messages):

- Email messages

- Simple Network Management Protocol (SNMP) notification. (SNMP is an application-layer Internet protocol designed to facilitate the exchange of management information between network devices.)

If alerts notification will go through SNMP, you must configure SNMP settings.

You can also enable and configure alert notifications if certain security thresholds are passed by incoming or outgoing traffic.

The Alerts feature contains the following windows:

- Alert Settings Window

- SNMP Settings Window

- Security Window

5.8.1 Alert Settings Window

The Alert Settings window (accessed via **Administration | Alerts | Alert Settings**) lets you configure, for each event type (System, Application, Update, and Security), the type of alerts (Email and/or SNMP) that should be sent.

> For Email alerts to be sent: You must configure the Mail Server, including selecting the **Enable Sending Email** check box, (in **Administration | System Settings | Mail Server**; for details, see Mail Server.
>
> For SNMP alerts to be sent: You must configure SNMP settings, including selecting the **Enable Trap Sending** check box in **Administration | Alerts | SNMP Settings**; for instructions, see SNMP Settings Window below.

To edit the details, click **Edit**. After editing, click **Save**. To commit the changes, click [icon] **Commit Changes** in the toolbar.

The window contains a table. Each row in the table identifies an event type, and has check boxes representing the two possible channels (Email and SNMP).

To specify the channels for the event type:

1. For each event type, select the check boxes of the channel(s) that should be used. If you select the Email check box, provide at least one email address in the accompanying Email Address field.

2. To specify additional email addresses for an event type, click the [icon] icon and choose **Add Row**. (To delete an email address, click this same icon and choose **Delete Row**.)

5.8.2 SNMP Settings Window

If your site will be using SNMP alerts, you must configure the SNMP settings. You do this in the SNMP Settings window (accessed via **Administration | Alerts | SNMP Settings**).

To edit the details, click **Edit**. After editing, click **Save**. To commit the changes, click [icon] **Commit Changes** in the toolbar.

The SNMP Settings screen contains two tabs:

- General Tab — In this tab, you configure the SNMP protocol for MIB Monitoring/Trap sending, as well as the ports. You also configure the Hostname/IP destination servers for receiving the SNMP traps.

- SNMP Version Tab — In this tab, you select with which version of SNMP the system will work, and define any required parameters.

5.8.2.1 General Tab

When defining SNMP configuration settings, you can enable and configure MIB Monitoring and SNMP Trap Sending:

- MIB (Management Information Base) is a database of objects that can be monitored by the network management system (SNMP). This collection of information is organized hierarchically and comprises managed objects identified by object identifiers.

- SNMP traps are deployed as a means of notifying the management station of specific events by way of an SNMP message.

The **General** tab enables you to configure the SNMP protocol for MIB Monitoring/Trap sending, as well as the ports. The tab also enables configuration of the Hostname/IP destination servers for receiving the SNMP traps, and allows you to test the connections to the trap destination servers.

SNMP Settings Window – General Tab Fields and Buttons

Field/Button	Description
Enable MIB Monitoring check box	To enable SWG to perform MIB monitoring, select this check box, and specify the **Listening Port** (below).
Enable Trap Sending check box	To enable SWG to send traps, select this check box, and specify the **Trap Port** (below).
Trap Port (output)	If you enabled Trap sending, specify the corresponding output Trap Port (**Default: 162**).
Listening Port (input)	If you enabled MIB monitoring, specify the port against which SWG should perform SNMP queries (**Default: 161**).
Trap Destination Servers area	The fields in this area are only relevant if the Policy Server should be the Trap Destination Server.
Set Policy Server as Trap Destination Server check box	If the Policy server should be the Trap Destination Server, select this check box.
check boxes and entry fields (3)	In the three entry fields to the right of associated check boxes, optionally specify the IP address for up to three destination servers. Note: If the device is set up to query a Domain Name System (DNS) server, you are permitted to specify a host name instead of an IP address for the trap destination. To have the traps sent to any or all of these servers, select the check box beside the server. (A cleared server check box results in that server not receiving the SNMP trap).

SNMP Settings Window – General Tab Fields and Buttons

Field/Button	Description
Test button	To test that the traps are successfully sent to the SNMP servers, click the **Test** button. A test message will be sent to the defined server(s) with the SNMP name, IP and SWG Software Version.

5.8.2.2 SNMP Version Tab

The **SNMP Version** tab lets you define with which version of SNMP the system works.

SWG supports two versions of SNMP: **SNMP v2.c** and **SNMP v3**. Both versions support MIB Monitoring and SNMP Traps Sending.

However, **SNMP v3** provides greater security by securing device access for MIB Monitoring and SNMP Trap Sending through authentication and encryption over the network. Therefore, when configuring SNMP3, you define a number of configuration parameters relating to authentication, privacy, and access control.

If you select **SNMPv2.c** you must enter a community name.

SNMPV3 – SNMP MIB Monitoring: The Management Information Base (MIB) is a database of objects that can be monitored by the network management system (SNMP). This collection of information is organized hierarchically and comprises managed objects identified by object identifiers.

SNMP Settings Window – SNMP Version Tab Fields

Field Name	Description
SNMPv2 radio button	Check this button to use SNMP v2, and then fill in the Community field (below).
Community	Specify the group to which the devices and the management stations running SNMP belong (**Default string: Trustwave**).
SNMPv3 radio button	Check this button to use SNMP v3, and then fill in the fields below.

Administration
296

SNMP Settings Window – SNMP Version Tab Fields

Field Name	Description
SNMP MIB Monitoring area	The fields in this area define the security protocol and encryption methods used to obtain information from the SNMP client on the machine. The information retrieved is part of a MIB. **Note**: *The same fields, with the same meanings, also appear in the SNMP Traps area (described below).*
Security Name	SNMP user name. If the Security name in the SNMP MIB Monitoring section is the same as in the SNMP Traps section, then the rest of the parameters must be the same as well. Therefore, the **Use SNMP MIB Monitoring Information** check box must be selected.
Security Level	Select whether the messages should be sent unauthenticated (None), authenticated, or authenticated and encrypted. **Note**: If you selected **None**, do not fill in the remaining (authentication and encryption) parameters in this area.
Authentication Protocol	Either **MD5** or **SHA** (verification checksums)
Authentication Key	Authentication is performed by using the user's authentication key to sign the message being sent. Must be a minimum of 8 characters.
Encryption Key	Authentication is performed by using the user's encryption key which encrypts the data portion of the message being sent. Must be a minimum of 8 characters **Note**: *The encryption mode or privacy protocol used is DES (encryption algorithm).*

SNMP Settings Window – SNMP Version Tab Fields

Field Name	Description
SNMP Traps area	SNMP traps are deployed as a means of notifying the management station of specific events by way of an SNMP message. SNMPv3 mandates that trap messages are rejected unless the SNMPv3 user sending the trap already exists in the user database. The user database in an SNMPv3 application is referenced by a combination of the user's name (Security Name) and an identifier for the given SNMP application (engineID).
Use SNMP MIB Monitoring information check box	If the Security Name used for SNMP Traps is the same as SNMP MIB Monitoring, the rest of the details must also be the same for MIB Monitoring and SNMP Traps. Therefore, select this check box to copy all other information.
Security Name, Security Level, Authentication Protocol, Authentication Key, Encryption Key	These fields define the security protocol and encryption methods used to obtain information from the SNMP client on the machine. They are the same as the corresponding fields in the **SNMP MIB Monitoring** area (above).

5.8.3 Security Window

You can have administrators alerted when blocked incoming events (**Malicious Activities**, **Viruses**, **Scripts**, **Binary Content**) and/or blocked outgoing events (**URL Categorization**, **URL Lists**, **Blocked Files according to file types**) reach certain thresholds.

You do this in the Security Window (accessed via **Administration | Alerts | Security Alerts Settings**).

To edit the details, click **Edit**. After editing, click **Save**. To commit the changes, click ⚡ **Commit Changes** in the toolbar.

To enable security alert notification:

Select the **Enable Security Alerts When** check box. Then do the following:

- To enable alerts based on incoming traffic, select the check box dealing with **incoming** traffic notification and specify the following blocked incoming traffic figures:

  - the amount of blocked incoming traffic as a percentage of total incoming traffic, as measured over a specified period of minutes, above which an alert will be triggered.

    An average percentage of blocked incoming events would be approximately 1%-5%. Above 7% percent of blocked data might indicate that there is some kind of security breach.

- the amount of blocked incoming traffic as a percentage of total incoming traffic, below which the alert will be cleared (this should be lower than the percentage that triggers the alerts)

- To enable alerts based on outgoing traffic, select the check box dealing with **outgoing** traffic notification and specify the following blocked outgoing traffic figures:

  - the amount of blocked outgoing traffic as a percentage of total outgoing traffic, as measured over a specified period of minutes, above which an alert will be triggered.

  - the amount of blocked outgoing traffic as a percentage of total outgoing traffic, below which the alert will be cleared (this should be lower than the percentage that triggers the alerts).

5.9 System Information

The **System Information** screen provides a simple way for the administrator to view the status of the system with respect to license and module information such as available modules, versions, license expiration date and so on.

The System Information screen comprises three tabs:

- General

- Licensed Modules

- Installed Components

5.9.1 General

The **General** tab includes the Appliance MAC (eth0 interface MAC address of the Policy Server), the number of licensed seats (system users), the number of licensed virtual cores within the system, and the license expiration date.

The system has a maximum allotment of virtual cores per license. If cores are added to a particular appliance and the maximum quota is surpassed, the customer is given a 30 day grace period to reduce the total number. If the number of cores is not reduced to within the allowable amount, the Management Console will be blocked and only the license page will be available. Once the core number is reduced to stay within the limit, the system will return to normal functionality.

5.9.2 Licensed Modules

The **Licensed Modules** tab includes Trustwave and third party engine licenses.

5.9.3 Installed Components

The **Installed Components** tab displays information per component and includes the Component name (for example, the Trustwave Operating System, update, engine and data file) together with the corresponding Version, Release date and Install date.

5.10 Change Password

The Change Password screen enables the administrator to change passwords when necessary.

6 Help

The Help menu contains the following options:

- Help

- Manuals

- External Links

- About

6.1 Help

The Help comprises detailed information and procedures per screen designed to help you navigate around the Management Console and to perform configuration and monitoring tasks.

In addition to the Help found here, you can click the Help icon at the top of each screen (or press **F1** on the keyboard) to receive context-sensitive help highlighting only the information relevant to that screen.

6.2 Manuals

Four core manuals are provided with the Trustwave Secure Web Gateway Management Console:

- *Management Console Reference Guide* (this manual): This Reference Guide provides an expansive and thorough navigation through the Secure Web Gateway Policy Server Management Console, with detailed examples and tutorials to aid administrators in their daily tasks.

- *Secure Web Gateway User Guide*: This Guide provides the procedures that you perform on the Management Console to implement, use, and maintain Secure Web Gateway (SWG) in your organization.

- *Secure Web Gateway Setup Guide*: This Guide provides detailed procedures on all aspects of setup and configuration for the Secure Web Gateway System, and includes interoperability details with third-party clients.

- *Secure Web Gateway User Security Policies In-Depth Guide*: The Trustwave predefined Security Policies for HTTP and HTTPS are detailed in this manual. Rule demonstrations, courtesy of the Malware team at Trustwave, provide the administrator with hands-on material with which to validate the Security Rules.

6.3 External Links

The following links are supported:

Trustwave SpiderLabs: Opens the SpiderLabs subsite on Trustwave.com. Trustwave Spiderlabs are the leading research departments at Trustwave, dedicated to the research and detection of security vulnerabilities in Internet and email applications as well as other popular applications.

Trustwave: Opens the Trustwave Website.

Access Trustwave Support: Opens the Support subsite on the Trustwave Website. Here you can choose several options including opening a Case Form or review helpful articles in the Knowledge base Portal.

6.4 About

Contains information about the Trustwave Secure Web Gateway product and version.

Appendix A: Reports

The following table contains a list of the SWG Reports designed to provide ease-of-use and flexibility.

<div align="center">SWG Reports</div>

Report	Description
Anti-Virus	
Top Viruses	A summary report, displaying all viruses found by the Sophos/ McAfee/Kaspersky anti-virus engine, sorted by the number of viruses found. In Graph View of all reports, only the ten most frequent viruses are displayed.
Compliance	
Blocked Web Sites	This report displays blocked Websites. The information in the Report is dependent on the Logging Policy.
Data Leakage Prevention	This report displays all documents upload attempts blocked by DLP.
Transaction Usage by Hour	This report displays the specific hours that users are surfing the Internet, and thereby showing productivity by time, traffic peaks, and so on. The information in the Report is dependant on the Logging Policy.
Transactions with Legal Liability by Users	This report displays blocked Websites that might have exposed the company to legal liability issues.The information in the Report is dependant on the Logging Policy.
Potential Disclosure of Confidential Information	This report displays all blocked upload attempts of Microsoft Office documents.
IT Operation	
Infected Client Computers	This report displays the IP addresses of computers detected trying to send malicious code, and hence showing which computers need treating. The information in the Report is dependant on the Logging Policy.
Top URLs by Volume	This report displays the top URLs visited according to bandwidth consumed. The information in the Report is dependent on the Logging Policy.
Top Users by Volume	This report displays the most active users, sorted by total bandwidth consumed. The information in the Report is dependent on the Logging Policy.

SWG Reports

Report	Description
Traffic Analysis by Content Type	This report displays traffic analysis details by content type. For example, the total size of images or executables that were downloaded, and so on. The information in the Report is dependent on the Logging Policy.
Traffic Analysis by Hour	This report displays the traffic analysis according to the specific hour of the day, thereby showing when the highest load occurs. The information in the Report is dependant on the Logging Policy.
Traffic Analysis by User	This report displays the traffic analysis details according to the most active users. The information in the Report is dependant on the Logging Policy.
Client Computers With Trojans	This report displays the IP addresses of computers with Trojans installed on them, detected trying to communicate over the Internet. The information in the Report is dependant on the Logging Policy.
Instant Messaging and P2P	
Instant Messaging Activity	This report provides in-depth details as to how many users are Instant Messaging and what specific applications and operations they are using. The information in the Report is dependant on the Logging Policy.
Use of Instant Messaging by User	This report displays Instant Messaging Activity per user name.The information in the Report is dependant on the Logging Policy.
Productivity	
Most Visited Website Categories	This report displays the most visited Website categories by users, thereby showing the type of content users are looking at. The information in the Report is dependent on the Logging Policy.
Most Visited Website Domains	This report displays the most visited Websites (for example,. cnn.com, google.com). The information in the Report is dependent on the Logging Policy.
Risk Assessment – Business Usage	This report allows you to assess Web usage for business reasons by users. The information in the Report is dependant on the Logging Policy.
Most Visited Website Categories	This report displays the most visited Website categories by users, thereby showing the type of content users are looking at. The information in the Report is dependant on the Logging Policy.
Risk Assessment – Employment	This report enables you to assess the employment risk based on the number and frequency of employment Websites visited by users. The information in the Report is dependant on the Logging Policy.

SWG Reports

Report	Description
Risk Assessment – Legal Liability	This report enables you to assess the legal risks based on the type and frequency of Websites visited by users. The information in the Report is dependant on the Logging Policy.
Risk Assessment – Productivity Loss	This report enables you to assess the productivity risk based on the type and frequency of Websites visited by users. The information in the Report is dependant on the Logging Policy.
Top URLs by Hits	This report displays the most visited URLs. The information in the Report is dependent on the Logging Policy.
Top Users by Hits	This report displays the most active users, sorted by number of Web requests (hits). The information in the Report is dependent on the Logging Policy.
Traffic Analysis Raw Data	This report lists all transactions matching the report filters. The transactions are listed in a chronological order. The information in the report is dependent on the Logging Policy.
Website Categories by User	This report displays Website categories grouped by user name. The information in the Report is dependent on the Logging Policy.
Websites by User	This report displays a detailed list of Websites the user visited, sorted by the amount of transactions for each Website.
Website Categories Violating Policy	This report displays Website categories that violated the security policy, indicating potentially malicious site categories that users requested to visit. The information in the Report is dependant on the Logging Policy.
Web Security	
Adware Sites Accessed by User	This report displays the number of adware sites accessed by the user.
Anti-Virus (Sophos / Kaspersky / McAfee)	This report displays the name and amount of viruses detected and blocked by Kaspersky/Sophos/McAfee with their original URL.
Blocked Active Content	This is a summary report, displaying blocked active content types and the number of times that each type was requested.
Blocked Trojan Activities	This report displays the details of transactions blocked due to Trojan activity.
Known Threats – Signature Based	This report displays the malicious code detected by SWG's third-party engines and lists.
Policy Rules Violations	This report displays the number of violations for each Security rule.
Potentially Malicious Websites	This report displays the Websites according to URL categories that were blocked for being potentially malicious.

SWG Reports

Report	Description
Security Policy Violations – (Binary Behavior Profile)	This report displays the URLs that were blocked due to binary behavior policy violations.
Security Policy Violations	This report displays all security policy violations. It counts the number of violations per policy rule. Use this report to review your company's compliance with the defined security policy.
Security Policy Violations – Malware Entrapment Profile	This report displays the URLs that were blocked due to the Malware Entrapment Profile.
Spyware Sites Accessed by User	This report shows and counts the number of spyware sites accessed by the user.
Top Domain Names by Security Rule	This report displays top domain names blocked for every security rule. The security rules are sorted by the total number of blocks and sorted further by the number of transactions for each domain.
Unknown Threats – Behavior Based	This report displays all threats that were detected by SWG's behavior-based proprietary technology.

Appendix B: End User Messages

The following Message Texts are used in the Page Blocked End User Messages sent when a URL is blocked (or coached).

End User Messages

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Active Content List	Blacklisted active content: `<binary_profile_list>`. Transaction ID is `<ID no.>`	Block ActiveX, Java Applets and Executables by ACL
Application Level Vulnerability Detected	This page (or part of it) has been blocked because it attempts to exploit an application level vulnerability. Transaction ID is `<ID no.>`	Block Application Level Vulnerabilities
Archive Assembly Error	The item you requested contained a forbidden object. Transaction blocked. Transaction ID is `<ID no.>`	
Binary VAD Violation	Binary content was blocked due to discovered exploit. The violation is `<binary_vad>`. Transaction ID is `<ID no.>`	Block Binary VAD Vulnerabilities
Blacklisted URL	Access Denied! Access to this URL: `<site URL>` is forbidden. Transaction ID is `<ID no.>`	Block Access to Blacklisted Sites
Blocked Adware URL	Access Denied! The requested URL is an Adware site.Transaction ID is `<ID no.>`.	Block Access to Adware Sites
Blocked Binary Exploit In Textual File	Potential Binary Exploit detected! An attempt was made to download a textual file with binary content. Transaction ID is `<ID no.>`	Block Binary Exploits in Textual Files

End User Messages

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Blocked since AV could not scan	The file you are trying to download could not be scanned by AV. Transaction ID is `<ID no.>`	Block Unscannable (Sophos/McAfee/Kaspersky)
Blocked Spyware URL	Access Denied! The requested URL is a Spyware site. Transaction ID is `<ID no.>`	Block Access to Spyware Sites
Blocked URL Category	Forbidden URL. URL Category is `<Trustwave_category>`. Transaction ID is `<ID no.>`	Block Access to High-Risk Site Categories
Certificate Validation Mismatch	The detected certificate validation mismatch is `<certificate_validation_mismatch>`. Transaction ID is `<ID no.>`	Block Certificate Validation Errors
Container Type	Forbidden container type: `<container_type>`. Transaction ID is `<ID no.>`	
Container Violation	Container Violation: `<container_violation>`. Transaction ID is `<ID no.>`	Block Potentially Malicious Archives Block Illegitimate Archives (Including Password-Protected Archives)
Corrupted Container	The file you are trying to download is corrupted. Transaction ID is `<ID no.>`	
Data Leakage Prevention	Forbidden operation. Content is blocked due to supposed data leakage. Transaction ID is <ID no.>	Data Leakage Prevention
Digital Signature Violation	Active content was blocked due to digital signature violation. The violation is `<digital_signature_violation>`. Transaction ID is `<ID no.>`	Block Binary Objects without a Digital Certificate Block Binary Objects with Invalid Digital Certificate

End User Messages

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Emergency Policy Active	Due to an elevated security risk, only access to specified sites is currently allowed. Transaction ID is `<ID no.>`	
Fatal Error	The service is unavailable, please try again later. If the problem persists, please contact the administrator.	
File Extension	Forbidden file extension: `<file_extension>`. Transaction ID is `<ID no.>`	Block Blacklisted File Extensions Block Files With COM Extension
File Spoofed as Archive Detected	An attempt was made to spoof an ordinary file as an archive file. Transaction ID is `<ID no.>`	
Forbidden Content Size	Forbidden content size: <size_category>. Transaction ID is `<ID no.>`	
Forbidden Direction	Forbidden direction: `<direction>`. Transaction ID is `<ID no.>`.	
Forbidden Header Field	Forbidden header field: `<header_fields>`. Transaction ID is `<ID no.>`.	
Forbidden URL	Forbidden URL! Posts to social media sites are prohibited <nl>. URL blocked: <url list name>.Transaction ID is <transaction id>	Social Media Post Control Allowed Requests Social Media Post Control
Hash Scanner	Known malicious content found in list `<static_content_list> was stopped`. Transaction ID is `<ID no.>`	Block Known Malicious Content
Instant Messenger Detected	Access Denied! Use of `<IM>` is not allowed. Transaction ID is `<ID no.>`	Block IM Tunneling

End User Messages

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Internal Error	The service is unavailable, please try again later. If the problem persists, please contact the administrator.	
Malicious Behavior Detected	Malicious Behavior Detected! The page or file you requested contains malicious code. Transaction ID is <ID no.>	Block Malicious Scripts by Behavior Block Malicious ActiveX, Java Applets and Executables Block Unscannable Web Pages and Scripts
Mobile Malicious Code: Binary	Active content violation. The violation is <binary_behavior_profile_names>. Transaction ID is <ID no.>	
Mobile Malicious Code: Scripts	Found behavior blocking violation. The violation is <script_behavior_profile_names>. Transaction ID is <ID no.>	
Multiple Extensions	Forbidden file extension: multiple extensions. Transaction ID is <ID no.>	Block Files with Suspicious Multiple Extensions
Old or Unsafe Browser	An old or unsafe browser is used. Transaction ID is <ID no.>.	
Outgoing Microsoft Office File Detection	Transmission of Office Documents is blocked. File type: <file_extension> <content_type_name>.Transaction ID is <ID no.>	Block Outgoing Microsoft Office Documents
Partial Download Detected	Access Denied! Partial download detected. Transaction ID is <ID no.>.	
Policy Violation	Policy Violation. Transaction ID is <ID no.>.	

End User Messages

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Potential Shellcode Detected	Potential shellcode exploit detected. Transaction ID is `<ID no.>`.	
Revoked Cloud User	User has been restricted from using the Cloud	
Service Stopped	Service is stopped. Transaction ID is `<ID no.>`.	
Spoofed Content Detected	An attempt was made to download a spoofed file. The spoofing type is: `<spoofing_type>`. Transaction ID is `<ID no.>`	Block Spoofed Content
Spoofed Executable Detected	Spoofed Executable Detected! An attempt was made to download a disguised executable file. Transaction ID is `<ID no.>`	
Spyware Behavior Detected	Spyware Behavior Detected! The requested file or page contains Spyware: `<spyware_name>`. Transaction ID is `<ID no.>`	Block Known Spyware (CLSID)
Spyware Object Detected	Spyware Detected! An attempt to download a forbidden Spyware program has been blocked. `<spyware_name>`. Transaction ID is `<ID no.>`	Block Known Spyware (ACL)
Suspected Trojan Traffic Detected	Suspected Trojan traffic detected. Access to the Internet is blocked.	Detect Known Trojan Network Activity
Suspicious File Type Detected	Forbidden File Type! An attempt was made to download a forbidden file type. Transaction ID is `<ID no.>`	Block Microsoft Office Documents containing Macros and/or Embedded Files Block Suspicious File Types
Temporarily Blocked Cloud User	User is temporarily Blocked from using the Cloud	

End User Message	Page Block Message Text	Security Policy Rule it Applies to (if any)
Temporary Error	The service is unavailable, please try again later. If the problem persists, please contact the administrator.	
Time Frame	Forbidden time: `<time_frame>`. Transaction ID is `<ID no.>`.	
Trojan traffic detected	Trojan traffic detected. Access to the Internet is blocked.	Block Trojan Communication based on Malicious Traffic
Type Detector	Forbidden data type. The data type is `<content_type_name>`. Transaction ID is `<ID no.>`	Block Unscannable Archives Block Potentially Malicious Packed Executables
Unscannable Content Detected	Unscannable content detected! The page or file you requested contains unscannable ActiveX, Java Applets or Executables. Transaction ID is `<ID no.>`	Block Unscannable ActiveX, Java Applets and Executables
URL List	Found item in a forbidden URL list. The URL is <url_list_name>. Transaction ID is `<ID no.>`	
Virus Detected	Virus Detected! The page or file you requested is infected with the following virus `<McAfee_virus_name>` `<Sophos_virus_name>` `<Kaspersky_virus_name>`. Transaction ID is `<ID no.>`	Block Known Viruses (Sophos/McAfee/Kaspersky)
Wrong Configuration Error	The service is unavailable, please try again later. If the problem persists, please contact the administrator.	

Appendix C: Limited Shell Commands

You can optionally use the commands of the Limited Shell to manage and monitor the functionality of an appliance.

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

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

This section contains the following subsections:

- Limited Shell Commands — Summary List

- Limited Shell Configuration Commands

- Limited Shell Monitoring Commands

Limited Shell Commands — Summary List

The following monitoring and configuration commands are available:

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

Limited Shell Commands — Summary List

Command	A/C/M	Description
access_list	C	Enables/disables the Access List
arp	M	Displays arp table
change_password	C	Change password
check_connectivity	M	Checks connectivity to the remote devices (for Policy server or All-in-One appliances)
config_ …	C	Network or service configuration. Double tab to view the config_network, config_time, config_hardware, config_upgrade, config_support, config_psweb, config_exclude and config_bridge commands.
df	M	Displays disk usage
disable_ …	C	Disables service. Double tab to view the disable_service_snmpd and disable_service_ssh commands.
enable_ …	C	Enables service. Double tab to view the enable_service_snmpd and enable_service_ssh commands.
ethconf	C	Menu interface to ethtool
failover	C	Performs a manual swap between active and passive mode. Available only on the Active Policy Server.
flush_dnscache	C	Flushes the DNS cache
ifconfig	M	Displays NIC configuration and statistics
ip2name	M	Resolve IP to hostname
iptraf	M	Interactive IP LAN monitor
last	M	Displays last login
name2ip	M	Resolve hostname to IP
netstat	M	Displays Network statistics
ping	M	Sends ICMP ECHO_REQUES to network hosts
poweroff	A	Power off the system

Limited Shell Commands — Summary List

Command	A/C/M	Description
reboot	A	Reboots the system
reset_config	C	Sends full configuration to appliance
restart_role	A	Restarts the role
save_exclude_logs	M	Saves Exclude logs
save_support_logs	M	Saves Support logs
setup	C	Runs configuration setup
show_...	M	Shows system or service status.
		Double tab to view the show_bridge, show_config, show_network, show_service, show_dbsize, show_proxy_buffers, show_proxy_connections, show_route, show_time, and show_version commands
show_hardware	M	Shows the hardware specs of a given SWG device.
supersh	A	Provides access to privileged shell
tcpdump	M	Dumps traffic on a network.
		Results files will be under sftp chroot/ tcpdump_captures. Files can be downloaded using any sftp client
top	M	Displays linux tasks
traceroute	M	Prints the route packets taken to network host (traceroute
uptime	M	Displays uptime
vmstat	M	Reports information about system usage (usage: vmstat,
w	M	Shows who is logged on
wget	M	Retrieves files using HTTP, HTTPS and FTP

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

Limited Shell Configuration Commands

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

access_list

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

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

Enter the access_list command and choose **enable** or **disable**.

change_password

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

Enter the change_password command and confirm current and new passwords.

config_ ...

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

config_network

Allows system administrators to configure network parameters, such as the IP addresses, routing information, DNS parameters. Enter the config_network command.

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

Select an option from the following commands:

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

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

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

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

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

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

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

  > **Important:** It is mandatory to configure the DNS Server that has the ability to resolve external IP addresses.

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

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

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

config_time

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

config_hardware

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

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

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

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

config_upgrade

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

config_support

Enables you to install support packages.

config_psweb

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

config_exclude

Defines bypass rules in intercepting proxy mode.

config_bridge

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

config_access_log

Enables or disables the access log.

disable_ ...

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

disable_service_snmpd

Disables the snmpd network service. Enter the disable_service_snmpd command.

disable_service_ssh

Disables the ssh network service. Enter the disable_service_ssh command.

enable_ ...

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

enable_service_snmpd

Enables the snmpd network service. Enter the enable_service_snmpd command.

enable_service_ssh

Enables the ssh network service. Enter the enable_service_ssh command.

failover

Performs a manual swap between active and passive mode. Available only on the Active Policy Server.

When performed on an Active Policy Server where HA is configured the following question will be displayed:

"**Would you like to perform a High Availability failover? [Y/N**]"

If a positive answer is given the following message is displayed as the failover starts:

"**Running High Availability failover.**"

Otherwise the following message appears:

"**Failover aborted by user.**"

ethconf

Enables configuring the Network Interface parameters.

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

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

The settings for the selected interface are displayed.

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

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

flush_dnscache

Flushes the dns cache.

reset_config

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

Limited Shell Monitoring Commands

arp

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

check_connectivity

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

df

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

Enter the df command to display the disk usage.

ifconfig

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

ip2name

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

iptraf

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

- IP traffic monitor

  - General Interface Statistics

  - Detailed Interface Statistics

  - Statistical breakdowns

- LAN station monitor

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

last

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

name2ip

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

netstat

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

ping

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

poweroff

Enables you to remotely shut down the appliance.

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

reboot

Enables you to remotely reboot the appliance.

restart_role

Restarts all role services.

save_exclude_logs

Saves Exclude logs in the Exclude directory.

save_support_logs

Saves Support logs in the Support directory.

setup

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

show_...

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

show_bridge

Shows the Bridge role configuration.

show_config

Shows the current configuration.

show_hardware

Shows the hardware specs of a given SWG device.

show_network

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

show_service

Allows system administrators to view the service configuration status.

The following options are available:

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

• **show_service_snmpd:** Displays the service configuration status for snmpd.

• **show_service_ssh:** Displays the service configuration status for ssh.

show_dbsize

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

show_proxy_buffers

Shows the status of proxy buffers.

show_proxy_connections

Shows the status of proxy connections.

show_route

Allows system administrators to view the Kernel IP routing table.

show_time

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

show_version

Shows the currently installed SWG version.

supersh

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

tcpdump

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

top

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

traceroute

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

uptime

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

vmstat

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

w

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

wget

Enables you to download Web files using HTTP, HTTPS and FTP protocols.

Appendix D: Application Control Actions

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

- Facebook

- Google +

- LinkedIn

- Twitter

- YouTube

> User actions provided by the various social media applications supported in SWG are continuously maintained. Where deemed necessary, these lists will be extended or adapted to reflect changes or extend the functionality.
>
> For the latest available lists, refer to the SWG online Help.

Facebook

Action	Enables the user to ...
Add Friend	Add someone to the 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
Find Friends	Search for facebook accounts that could be added as friends
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

Action	Enables the user to ...
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

Google +

Action	Enables the user to ...
+1	Mark a post/comment/picture/video as liked
Add a Person	Add a user to a circle, or group
Chat	Chat with other users
Create a Page	Create a page for any business, group, cause, or product
Create Community	Create ongoing conversations about particular topics
Create Event	Create an event and invite people
Create New Circle	Create a group of people to follow and share with
Find People	Find people to add to a circle
Join Community	Join an ongoing conversation
Post Comment	Post a comment or reply to a post
Share (A Post, Event, Photo, Video, Link)	Share something with other users
Video Chat	Chat with a friend or group of friends using video
Watch Video	Watch a video

LinkedIn

Action	Enables the user to ...
Add Connections (Invite Contacts)	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
Find Alumni	Find fellow alumni
Follow Company	Follow the posts that a specific company is posting
Inbox	Go to the inbox that holds the user's messages
Join Group	Join a group
Like	Mark a post or comment as liked
Post a Job	Post a job in order to recruit
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

Twitter

Action	Enables the user to ...
Activity	View activities of the user's friends
Create List	Gather profiles into a list
Delete	Delete a tweet
Favorite	Mark a tweet as favorite
Find Friends	Search for friends or people the user might know
Follow	Start following a user
Mentions	Get a list of tweets that mentioned the user
Receive Message	Receive a direct message from another user

Action	Enables the user to …
Send Message	Send a direct message to another user
Tweet or Retweet	Tweet or retweet

YouTube

Action	Enables the user to …
Create a Playlist Tag	Create a tag to a playlist
Create New Collection	Create a Group of subscriptions using collections
Delete Video	Delete an uploaded video
Edit Playlist	Edit a playlist
Like or Dislike a Video	Mark a video as liked or disliked
Play Video	Play a video
Post	Post a new status
Post Comment	Comment on a video
Post Share	Share a video
Report Video	Report a video as offensive
Subscribe/Unsubscribe	Include or exclude a channel from a collection
Upload Video	Upload a video
VideoManager.Favorites	Manage the videos marked as favorites
VideoManager.Likes	Manage the likes the user gave
VideoManager.Playlists	Manage the user's playlists
VideoManager.Search History	Manage the search history
VideoManager.Tags	Manage the tags a user created
VideoManager.Upload	Manage properties of the videos uploaded
Vote Up/Down	Vote up/down on a comment
Watch Later	Go to the list of videos the user marked to watch later

329

About Trustwave[R]

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper[R] portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide.

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