Secure Web Gateway

Version 11.0

User Guide

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
1.0	March 2013	Version 11.0 Release

Formatting Conventions

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

Table 1: 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 SWG User Guide describes the procedures that you perform on the Management Console to implement, use, and maintain Secure Web Gateway (SWG) in your organization. The Management Console is your interface to SWG.

It is important to note that this guide is not a reference guide. It does not provide a detailed description of all Management Console screens, or fields. Nor does it provide a detailed description of concepts that apply to SWG and the Management Console. For that information, see the *Management Console Reference Guide*.

This guide assumes that:

- you have already installed the Secure Web Gateway in your organization. For installation instructions, see the Secure Web Gateway Installation Guide.

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

- you have already planned out your security needs.

This guide is divided into Parts and Chapters. These parts and chapters are organized in the sequence in which you are likely to use them when first implementing SWG. You can, of course, use any procedure at any time that you need.

- **PART 1: Initial Management Console Tasks** - describes how to perform preliminary and basic tasks in the Management Console, and manage devices and device groups.

- **PART 2: Implementing User Security Policies -** describes how to define and manage security policies and users.

- **PART 3: Configuring Advanced Network Settings** - describes how to define and assign Identification, Proxy, and Caching policies.

- **PART 4: Configuring Logging and Alert Settings -** describes how to define Logging policy, configure the Log server, and configure alerts.

- **PART 5: Performing Monitoring And Maintenance -** describes how to view the security status, and manage logs and reports.

- **PART 6: Performing Advanced Configuration -** describes additional advanced configuration tasks such as enabling HTTPS scanning, and implementing Cloud security and ICAP services.

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*

- *Management Console User Guide*

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

- *Secure Web Gateway User Identification Guide*

Table of Contents

PART 1: Initial Management Console Tasks

This part contains the following chapters:

- Getting Started
- Configuring/Adding Scanning Servers

1 Getting Started

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

This section contains the following topics:

- Performing Preliminary Tasks

- Performing Basic Tasks in the Management Console

1.1 Performing Preliminary Tasks

Before performing any preliminary tasks, ensure that:

- SWG is installed. For installation instructions, see the *Secure 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.

This section contains the following topics:

- Performing First Time Login, Password Change, and License Installation
- Configuring the Mail Server

1.1.1 Performing First Time Login, Password Change, and License Installation

When logging onto the Management Console for the first time:

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

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

    The Login window is displayed.

2. Enter the administrator user name (default: **admin**) and password (default: **finjan**).

    The Change Password window is displayed.

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

3. Enter the following:

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

   - **New Password** — A new password

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

4. Click **Change Password**.

   The License window is displayed.

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

   The Trustwave SWG Welcome Screen is displayed.

1.1.1.1 Welcome Screen

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

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

1.1.2 Configuring the 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 need to define the settings for the Mail Server in the Mail Server Setting Screen.

To configure the Mail Server:

1. Select **Administration | System Settings | Mail Server** and click the **Edit** button.

2. To enable the sending of email, ensure that the **Enable Sending Email** check box is selected.

3. In the **Hostname/IP field**, specify the IP address, or hostname, of the SMTP Server you are using (for example, mail.Trustwave.com).

4. In the **Port** field, specify the number of the port that the SMTP Server uses, usually 25 is specified.

5. In the **User name** and **Password** fields, specify the User name and Password used for SMTP Authentication. This is optional, depending on your SMTP requirements.

6. In the **Originating Domain** field, specify the domain from which emails will be sent.

7. In the **Test Recipient** field, specify the email address to which the test email will be sent, to validate that the messages are being received (for example, sarah@Trustwave.com).

8. Click **Test**. A sample email alert will be sent to the Test Recipient email address.

9. Click **Save**.

10. If you are ready to distribute and implement the changes in your system devices, click **Commit** .

1.2 Performing Basic Tasks in the Management Console

This section describes the following tasks:

- Logging In and Logging Out

- Changing Your Password

- Committing Changes

- Working in Multiple Windows

- Customizing the Home Page

- Relocating an Item in a Tree

- Customizing the Management Console Toolbar

- Using Keyboard Shortcuts

1.2.1 Logging In and Logging Out

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 option says that this is not recommended.

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

To log out of the Management Console:

1. Click the **Logout** main menu option.

2. At the confirmation prompt, click **OK**.

1.2.2 Changing Your Password

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

> Administrators can change the passwords of the administrators under them, in the Administrator definition screen accessed via **Administration | Administrators**.

To change your password:

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**.

1.2.3 Committing Changes

To distribute and implement changes that you have saved, you must click the **Commit** ⌄ icon. Depending on how you prefer to work, you can click the icon after each **Save**, or to avoid interrupting your work, you can wait and then click the icon only when it is convenient to distribute and implement the changes.

1.2.4 Working in Multiple Windows

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

To open and work in multiple windows:

1. To open a tab that contains a window, click the ⊞ icon.

    Another tab containing a window opens. By default, it opens the Home page.

2. Navigate to the desired location in the new window.

3. To move to a different window, click the tab of that window.

4. To close a tab, click ⊠ in the right corner of the tab.

1.2.5 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.

1.2.6 Relocating an Item in a Tree

Depending on the item and tree, you can sometimes move an item to a different location in a tree.

To move an item to a different location in a tree:

1. Right-click the item and select **Move** or **Move to**.

2. Right-click the item above or below the location where you want to place the item being moved.

3. Select either **Move Below** or **Move Above**, depending on your requirement.

1.2.7 Customizing the Management Console Toolbar

To display or hide Toolbar icon shortcuts:

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 and, in the drop down list, select only those items that you want displayed. Then click **Update**.

1.2.8 Using Keyboard Shortcuts

The following table indicates the keyboard shortcuts that you can use to perform various actions in the Management Console.

Table 1: 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

2 Configuring/Adding Scanning Servers

SWG comes with default device settings that you can modify if required. Default settings are automatically applied to all new devices that you add. You can then modify the values for specific devices.

> To ensure that optimal defaults values are applied to new devices, you should modify the default values before adding new devices.

SWG also comes with a default Scanning Server device group, **Default Devices Group**. You can create other device groups, and add scanning servers to any scanning server device group. For each Scanning Server device group, you can define schedules for automatic configuration and update of the devices in the group.

You can also move devices from one group to another.

This chapter contains the following procedures:

- Configuring Device General Settings

- Adding Devices and Device Groups

- Moving Scanning Servers To a Different Group

2.1 Configuring Device General Settings

Use the procedure to modify default settings, and after you have added devices, to configure settings for specific devices.

> You can also:
> - configure default and device-specific access lists, which can limit access to specific IPs or IP ranges. For instructions, see Configuring Default and Device-Specific Access Lists.
> - select Scanning Servers for automatic update. For instructions, see Configuring Automatic Update Handling.

To configure Device General settings:

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device configuration tree, do either of the following *under* the **Devices** (root) node:

    - To configure Default settings, select **Default Values** | **Device Settings** | **General**. Values you define here will apply to all new devices that you create.

    - To configure the settings for a specific Scanning Server, select ***<device_group>*** | ***<device_ip>*** | **Scanning Server** | **General**.

    The main window displays tabs for configuring the following: **Downloads**, **Timeouts**, **Transparent Proxy Mode**, and **Device Policies**.

3. Click **Edit**.

4. In the **Downloads** tab, specify in megabytes the maximum scannable sizes for files downloaded or uploaded via the proxy.

5. In the **Timeouts** tab, you can specify the following timeout values:

    > It is highly recommended that you do **NOT** modify the default timeout values in the **Timeouts** tab.

    - **Client Side Timeout** — the maximum lapse time between consecutive requests within the client-proxy connection before a timeout is declared.

    - **Server Side Timeout** — the maximum lapse time between reception of consecutive pieces of data from the server before a timeout is declared.

6. To enable and configure Transparent Proxy Mode, follow the instructions in Configuring Transparent Proxy Mode.

7. In the **Device Policies** tab, you can assign Identification, Device Logging, Upstream Proxy, ICAP Request and Response Modification, and Caching policies, as defaults or to a specific device. If the needed policies are not yet defined, you can perform the policy assignments later. For instructions, see Assigning Policies To Devices.

8. If you want to apply all default settings to existing devices, right-click **Default Values** in the tree and then click **Reset all with default values**.

9. Click **Save**.

10. If you are ready to distribute and implement the changes in your system devices, click ⟱.

    > In addition to the General parameters, you can also define other scanning server related options, depending on particular features that you use. Instructions for configuring **Authentication** and **Caching**, **ICAP** implementation, and for enabling **HTTPS** scanning, are described in this guide.
    >
    > For information on configuring **HTTP**, **WCCP**, and **FTP** settings, see the *Management Console Reference Guide*.

11. Test that your scanner is performing security checks during browsing, as follows:

    a. Browse to an adult site (for example, www.playboy.com).

    b. Browse to and download a test virus, as follows:

        i. Browse to http://www.trustwave.com/EVG/eicar.com.txt

        ii. Connect to the site by entering the user name **getevg** and password **HurNoc45**, and clicking **OK**.

    Each of these tests should result in an appropriate Page Blocked message from the scanner.

2.2 Adding Devices and Device Groups

SWG comes with a default group, **Default Devices Group**, for adding Scanning Servers, but you can add additional groups for holding scanning servers.

This section contains the following procedures:

- To add a Scanning Server Device Group:

- To add a Scanning Server Device:

To add a Scanning Server Device Group:

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device tree that is displayed in the left pane, right-click the **Devices** root and click **Add Group**.

   The New Group window displays two tabs for defining the group.

3. Specify a mandatory group name and optionally add a description.

4. In the **Commit Scheduling** tab, define the schedule by which configuration changes will be committed and applied to the devices in the group.

   > The schedule that you define goes according to the time of the Policy Server, not local client time.

    You can choose between:

   - immediately upon commit

   - specific interval in number of days, at a specified time

   - specific days of the week at a specified time

   - specific day of the month at a specified time

5. In the **Update Scheduling** tab, define the schedule by which security updates will be committed and applied to the devices in the group.

   > The schedule that you define goes according to the time of the Policy Server, not the local client time.

   You can choose between:

   - immediately

   - at a specified time. In this case, you also specify the window of opportunity in minutes by which the update must begin; if the update does not begin within that time, it will be attempted again the next day.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ⩎.

To add a Scanning Server Device:

You should perform this procedure when you add devices for either local Scanning Servers or cloud Scanning Servers. You can identify the device by a specific IP or a range of IPs.

> Before you can add a scanner, you must ensure that the device is accessible and that you have its IP address.

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device tree, right-click the Scanning Server Device Group to which the device should be added, and choose either of the following:

    a. If you will associate the device with a specific IP, choose **Add Device**.

    b. If you add multiple devices within a specific IP range, choose **Add Device By Range**.

    The New Device screen is displayed in the main window. It contains several fields and tabs for configuring the device. The Status tab is informational; you do not define any values in this tab.

3. Specify the device IP, or device IP range after specifying the initial IP in the range, specify the last 3-digit set in the range in the field on the right.

4. Select the Device type. You can choose between **Scanning Server (local)** or **Cloud Scanning Server**. The **All-in-One** option is not available because the Policy server is on a different device.

> If you are defining the device as a cloud scanner, when you are done with the device configuration, you must perform cloud implementation if you have not previously performed it. For instructions, see Implementing Cloud Security.

5. (Optional) Add a description of the server.

6. (Optional) In the **Access List** tab, define an Access List to limit access to specific IPs. For more information and instructions, see Configuring Default and Device-Specific Access Lists.

7. Click **Save**.

8. Configure the device's General settings. For instructions, see Configuring Device General Settings.

9. If you are ready to distribute and implement the changes in your system devices, click ⩎.

2.3 Moving Scanning Servers To a Different Group

To move scanning server devices from one group to another:

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device tree, right-click the **source** Scanning server device group, and choose **Move Devices**.

3. In the displayed window, select the check boxes of the devices to be moved.

4. In the **To** drop down list, select the target group.

5. Click **OK**.

6. If you are ready to distribute and implement the changes in your system devices, click .

PART 2: Implementing User Security Policies

This part contains the following chapters:

3 Defining and Customizing Security Policies

The process of implementing security for users at your site involves performing the following tasks:

- Defining Security Policy, as described in this chapter.

- Defining User Groups and Users, and assigning them security policies. For instructions, see Defining and Managing Users.

- Defining Identification policy. For instructions, see Implementing Identification Policy.

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

Because of the order in which security policies are implemented, some policies might not be implemented due the nature of a preceding policy, which can effect subsequent policies.

Trustwave also provides special purpose Security policies for different users and situations. These include:

- **Trustwave X-Ray Policy** — allows the potential effect of the policy on the system to be evaluated without implementing its security actions. For non-X-ray policies, you can define rules as X-ray rules, also for purposes of evaluation. You can make a policy an X-ray policy by selecting the **X-ray** check box in the policy definition.

- **Full Bypass Policy** — permits users to surf through the Trustwave SWG Appliance without any scanning.

- **Cloud User Policies** — **Trustwave Blocked Cloud Users Policy** and **Trustwave Revoked Cloud Users Policy** for temporarily blocking or revoking the permissions of specific cloud users.

- **Trustwave Emergency Policy** — allows immediate site-wide implementation of special emergency measures.

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

You can also create customized Block/Warn messages for use in Conditions, and edit Message templates.

This chapter contains the following procedures:

- Defining a Rule in a Security Policy

- Defining Conditions in a Security Policy Rule

- Creating a Block/Warn Message

- Editing a Message Template

3.1 Defining a Rule in a Security Policy

When you duplicate a policy, it has the same rules as were found in the original policy. You can edit these rules or create new rules from scratch.

You can specify if the rule should be applied to specific users, or if specific users should be excluded. One method is by specifying User Lists to which the rule should or should not apply.

> If you are using User Lists to identify users to which the rule should or should not apply, be sure to define those lists. For instructions, see Defining User Lists.

To define a rule in a Security Policy:

1. In the Policy tree, expand the policy so that you display its existing rules. Ensure you are working in a duplicated policy.

2. Do any of the following:

   > Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.
   >
   > For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

   - To edit an existing rule, select the rule in the tree and in the main pane, click **Edit**.

   - To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

   - To add a rule directly above an existing rule, right-click the existing rule, and select **Insert New Rule**.

   The main window displays the Rule Definition screen. The screen contains three tabs: **General**, **Apply to**, and **Exception**.

3. Fill in the **General** tab as follows.

   a. Enter a name for the rule.

   b. (Optional) Provide a description of the rule.

   c. For a rule that has an **Enable Rule** check box: Ensure that the check box is appropriately selected or cleared depending on whether or not the rule should be enabled after being committed.

   d. If the rule should be an X-ray rule, but the policy is not an X ray policy, select the **X-Ray** check box.

   e. Select the Action for the rule **Allow**, **Block**, or **Coach**.

   f. Do the following, as appropriate:

   - If you chose **Allow** as the action, select the appropriate **Advanced Action**.

- If you chose **Block** or **Coach** as the action, select the desired End-User Message. For information on creating/editing End User Messages, see Creating a Block/Warn Message.

- For **Block** actions only: If the End User Message should not be displayed, select the **Do Not Display End-User Message** check box.

4. To apply the rule to specific users, select the **Apply to** tab, and select the radio button for the category of users to which the rule should apply. Note the following:

- **All Users** is the default.

- **All Recognized Users** are all users identified by the system.

- **All Unrecognized Users** are Unknown users and/or Unassigned LDAP users. For more information, see the *Management Console Reference Guide*.

- If you chose **Select User Lists**, select the check boxes of the User Lists that contain the users to which the rule should apply.

5. To exclude specific users from application of the rule, select the **Exception** tab, and select the check boxes of the User Lists which contain the users who should be excluded.

6. Click **Save**.

7. To set conditions that should trigger the rule, continue with Defining Conditions in a Security Policy Rule.

8. To define additional rules in this policy, repeat this procedure.

9. If you are ready to distribute and implement the changes in your system devices, click ⊻.

3.2 Defining Conditions in a Security Policy Rule

To define conditions in a Security Policy Rule:

1. In the Policy tree, expand the relevant policy and rule.

2. Do either of the following:

- To edit an existing condition, click the condition in the tree, and then in the main pane, click **Edit**.

- To add a new condition to a rule, right-click the rule and choose **Add Condition**.

The main window displays the Condition Definition screen.

3. In the **Condition Name** field, select the type of condition in the drop down list.

For any selected condition type, the window displays an appropriate check box list. For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

> You can also edit each set of Condition Options via **Policies | Condition Elements**.
> For more information see the *Management Console Reference Guide*.

4. If you chose **Malware Entrapment Profile**, skip to Step 8.

5. If the window displays an **Applies To** area above the list, select whether the condition will apply to the items you select or to the items you do not select.

6. Select the appropriate check boxes in the list. If the window displays a **Select/Deselect All** check box, you can use this if it will be useful.

7. If the condition has any other special fields or requirements to fill in, fill them in appropriately, skip Step 8 and then continue with Step 9.

8. Perform this step only if you chose **Malware Entrapment Profile** as the condition name. The window displays a Security Level setting slider. The default setting is **None**. Depending on the policy type, it might also display an HTML repair check box. Do the following:

   a. To change the security level setting, use the slider to set the appropriate value for example, **Basic** or **Strict**.

   For information about the level, click the relevant level link (for example, **Medium**). The Secure Web Gateway Rule Updates window opens. This window provides relevant information.

9. Click **Save**.

10. If you are ready to distribute and implement the changes in your system devices, click ![icon].

3.3 Creating a Block/Warn Message

Block/Warn messages are sent to end-users in the event that the URL site they are surfing to has been blocked by the Secure Web Gateway or designated as a site requiring user approval or coaching action. User approval and coaching messages are referred to collectively as Warn Messages. The messages include Place Holders which are replaced with real values when displayed to the end-user.

These messages are then selected for each Block, Coach, or User Approval rule in the Security or HTTPS Policies as required.

To create a new Block/Warn message:

1. Select **Policies** | **End User Messages** | **Block/Warn Messages**.

2. Right-click the top level in the tree and select **Add Message**.

3. Type in a **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 within the message. For example, select **Client IP**, **Malware Entrapment Profile Names**, and **Domain**; be sure to click **Add** between each.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ![icon].

The new message can now be selected from the Rule Details screen, in the End-User Message drop down list.

8. 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.

> 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, refer to the *Management Console Reference Guide*.

3.4 Editing a Message Template

> 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 edit a message page:

1. Select **Policies | End User Messages | Message Template**.

2. In the main window, click **Edit**.

3. In the Rule Action drop down list, which displays the **Select Rule Action to Edit** instruction, select one of the listed **block** or **warn** rule actions.

   The Preview window displays the actual message as it will appear on the end-user computer.

4. To add elements to the message:

   a. Place the cursor at the location in the preview where you want the element added.

   b. Select the element in the drop down list. Element options include:

   • **Back Button** — Adds a **Back** button, used for returning control to the previous location.

   • **Redirect Button** — Adds an **OK** button, used for redirecting control to the next appropriate location.

   • **Notification** — Adds a placeholder (**USER-NOTIF**), that will be replaced with the user notification issued in the message.

   c. Click **Add**.

5. To delete an element that you added, select the element and press the keyboard **Delete** button.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

4 Defining and Managing Users

The process of implementing security for users at your site involves performing the following tasks:

- Defining Security Policy, as described in Defining and Managing Users.

- Defining User Groups and Users, and assigning them security policies, as described in this chapter.

- Defining Identification policy. For instructions, see Implementing Identification Policy.

The process for bringing users into the system and assigning them policies, depends on the category to which users belong:

- LDAP Users

- Trustwave non-LDAP Users

Before bringing users into the system and assigning policies, you can alter which policies are set as the user defaults.

The rules of certain Security, Logging, and HTTPS policies allow you specify to which users the rule should apply, and which users should be excluded from the application of the rule. One of the methods for identifying these users is by defining **User Lists**, which can then be specified in the rule definitions.

This chapter contains procedures for the following tasks:

- Setting Default User Policy Assignments

- Defining and Managing LDAP Users

- Defining and Managing Trustwave (Non-LDAP) Users

- Defining User Lists

4.1 Setting Default User Policy Assignments

You can set default user policies for the following types of policies: *Emergency, Master, Security, Logging*, and *HTTPS*. Note the following points:

- Security, Logging and HTTPS policies are automatically apply to all User Groups, LDAP Groups, and Unknown Users, except where you assign different policies of those types to specific groups or users.

- HTTPS and HTTPS Emergency policies are relevant only if HTTPS be licensed.

- Master Policy applies to Super Administrators. Most sites do not use this feature or policy. For information on Super Administrators, see Defining Administrators.

Emergency Policies — Emergency, and HTTPS Emergency when licensed apply across the board. You cannot assign a different Emergency policy to different user g*roups or users.*

To change which policies are set as the User defaults:

1. Select **Policies | Default Policies Settings**.

    The Default Policies Settings screen is displayed. This screen lists the types of policies for which defaults can be set at the site level, and for each type it provides a drop down list of all defined policies. The currently displayed policy for each type is the current default.

2. In the main window, click **Edit**.

    Ensure that the **Enable Emergency Policy** check box is **NOT** selected. You should only select this check box in an emergency. Selecting this check box implements Emergency policy that overrides all other Security policies defined for all devices, user groups, and independent users.

3. In the Default Policy Values area, set which policy will be the default for the particular policy types. Do not set a Master Policy unless you intend to implement Master Policy usage.

4. When done, click **Save**.

5. If you are ready to distribute and implement the changes in your system devices, click ⬇.

4.2 Defining and Managing LDAP Users

This section contains the following topics:

- Adding and Configuring LDAP Directories

- Importing LDAP Groups

- Configuring LDAP Group Settings

- Importing LDAP Users

- Setting a Schedule For LDAP Directory Update

- Assigning Policies to Unassigned LDAP Users

4.2.1 Adding and Configuring LDAP Directories

To add and configure an LDAP Directory:

1. Select **Users | Authentication Directories | LDAP**.

   Decide which type of LDAP directory to add (for example, add a Microsoft Active Directory). Then, right-click on the corresponding node (for example, **Microsoft AD**) in the LDAP Directory tree on left pane, and choose **Add Directory**.

   The main window displays a field for specifying a name for the directory, and two tabs for defining the directory: **General** and **Advanced Settings**.

2. Specify a unique, descriptive directory name in the **Name** field. Two LDAP directories cannot have the same name.

   Fill in the details of the **General** tab, as follows:

   > It is recommended that you **not** modify the default values in the Advanced Settings tab, so instructions for doing so are omitted from this procedure. However, if you do want to change those settings, see Modifying LDAP Directory Advanced Settings for instructions.

3. In the **Base DN** field, enter the DNS domain component name (for example, dc=trustwave, dc=com).

4. In the **Address** field, specify the IP address or host name. 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**.

5. For each additional needed address, click ➕ to add a new entry row.

6. Fill in the **Realm/Domain** name, the directory's identifier in the authentication process between the browser and the scanning server; for example, Trustwave.

   > If the directory type is **Microsoft Active Directory**, do not specify a Realm/Domain.

7. In the **User** field, enter the Authorized User DN for connecting to the directory.

   > If the directory type is **Microsoft Active Directory**, enter the user's account name, that is, the name that appears on emails before the @company.com, instead of its DN.

8. In the **Password** field, enter the password for logging into your organization's directory.

   > LDAP passwords cannot include the **< , >** or space characters. Do not use non-English characters if you will be using the Kerberos authentication method.

9. To enable the import of LDAP groups over SSL, select the **Use secure connection** check box. If you selected this check box:

- If the Policy Server should not perform certificate validation before starting the SSL session, select the **Ignore Certificate Validation** check box.

- If the Policy Server should validate the certificate on each connection, leave the **Ignore Certificate Validation** check box cleared. In this case, if the certificate is invalid, user import fails and an event such as a log, trap, or email is created.

10. To use Kerberos Authentication:

> You cannot use Kerberos authentication if you use SSL authentication. To use Kerberos authentication:
>
> • A DNS server must be present, and all directory servers must be resolved via the Trustwave SWG Appliance.
>
> • The times on the Policy Server and the directory machine must be synchronized.
>
> • You must have or create a Kerberos keytab file.

a. Click the **Do not check configuration settings on next save** check box.

b. Click **Save** and exit this window.

c. Create the needed Kerberos keytab file if it is not already created.

d. Import the keytab file as follows:

i. Right-click this LDAP directory node in the LDAP directory configuration tree, and selecting **Import Keytab**. This displays the Kerberos Keytab Upload screen.

ii. Upload the keytab file.

e. Reopen this LDAP directory definition.

f. Select the **Use Kerberos Authentication** check box.

g. Clear the **Do not check configuration settings on next save** check box.

h. Skip to Step 12.

11. If you do not want the connection to the server to be checked after you save the definition, make sure that the **Do not check configuration settings on next save** check box at the bottom of the window is NOT selected.

12. Click **Save**.

13. If you are ready to distribute and implement the changes in your system devices, click ⚌.

The directory will appear in the LDAP Servers tree. You can also check in the logs for verification.

> To check the address that is, that the connection to the server was successful, right-click on the Active Directory LDAP server in tree, and select **Check Connection** from the drop down menu. If there was a problem connecting to the servers, an error message is displayed.

4.2.2 Importing LDAP Groups

This procedure assumes that the required LDAP directories are defined.

To import LDAP Groups:

1. Display the list of LDAP directories by selecting **Users | Authentication Directories | LDAP**.

2. If multiple LDAP directories have the same Base DN, to import the users from an LDAP directory in the set that was not created first, right-click that directory and select **Set Importable**.

3. Right-click the LDAP directory and choose **Add Group**.

4. In the main pane:

    a. If the list of LDAP Groups in the directory is not displayed, retrieve the list by clicking **Retrieve LDAP Groups**.

    b. Select the **Select** check box.

    c. In the list of LDAP Groups, click each group that should be imported.

    d. When done, click **OK**.

5. If you are ready to distribute and implement the changes in your system devices, click ⬇.

4.2.3 Configuring LDAP Group Settings

Several LDAP Group parameters are relevant only if your site supports a Cloud in **Internal** mode. In this case, you must configure the cloud. For instructions, see Configuring Cloud Settings in Internal Mode **before** you configure the relevant LDAP Group parameters.

When you add an LDAP Group, it is automatically assigned default Security, Logging and HTTPS policies. When configuring the group's setting, you can change the policy assignments for the group.

To configure an LDAP group's settings:

1. Select **Users | Authentication Directories | LDAP**.

2. In the LDAP tree, click the group.

3. In the LDAP Group policy screen, click **Edit**.

4. To change policy assignments, select the desired policy in the drop down list.

5. If in Internal mode, enable certification of new users in the group, and prevent disabling Mobile Security Client, see To enable automatic certification of all new users in a group, and to prevent disabling of the Mobile Security Client:.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ⬇.

4.2.4 Importing LDAP Users

LDAP users can only be imported into LDAP directories that you have already created.

This section describes how to manually import LDAP users. You can also define a schedule for automatically updating LDAP directories with users. For more information, see Setting a Schedule For LDAP Directory Update.

It is highly recommended that you import and configure relevant LDAP Groups **before** LDAP users are imported.

When LDAP users are imported, those users belonging to groups that are already imported are placed in, and assigned the policies of, those groups. LDAP users whose groups are not already imported are treated as Unassigned LDAP users.

You can import LDAP users at any of several levels.

To import LDAP Users:

1. Select **Users | Authentication Directories | LDAP**.

2. Do any of the following:

    • To import all LDAP Users into all LDAP directories, right-click the **Directories** root note, and select **Import Users**.

    • To import LDAP Users into a specific LDAP directory, right-click the LDAP directory and select **Import Users**.

    • To import LDAP Users into a specific LDAP group, right-click the LDAP group and select **Import Users**.

3. If you are ready to distribute and implement the changes in your system devices, click ⊻.

4. To verify that the import was performed, navigate to **Logs and Reports | View System Logs**, and check the log.

4.2.5 Setting a Schedule For LDAP Directory Update

You can define an import schedule for LDAP, which will schedule automatic import of LDAP users into LDAP directories.

To define an LDAP user Import Schedule:

1. Select **Users | Authentication Directories | LDAP**.

2. Under the Directories tree, select **Settings and Defaults**.

3. Click **Edit**.

4. In the S**chedule Settings** tab, set when the import should be run, by specifying a time when the import should be run each day, or by specifying an interval between import runs which generates multiple imports each day.

5. Click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click 🗇 .

4.2.6 Assigning Policies to Unassigned LDAP Users

Unassigned LDAP Users refers to imported LDAP users whose groups have not been imported. Therefore, instead of having policy assignments specific to their group, they will be subject to the policies that you assign to Unassigned LDAP Users.

To assign policies to Unassigned LDAP Users:

1. Select **Users | Authentication Directories | LDAP**.

2. Under the Directories tree, select **Settings and Defaults**.

3. Click **Edit**.

4. Select the **Unassigned LDAP Users** tab.

5. For each of the listed policy types Security, Logging, or HTTPS that you want to change, select the desired policy in the drop down list.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click 🗇 .

4.3 Defining and Managing Trustwave (Non-LDAP) Users

This section contains the following topics:

- Creating/Configuring User Groups

- Adding and Defining Users

- Moving Users To a Different Group

4.3.1 Creating/Configuring User Groups

SWG comes with a number of predefined User Groups. However, you can create additional user groups according to need.

This section contains the following tasks:

- Defining and Assigning Policies to User-Defined User Groups

- Assigning Policies to Trustwave-Predefined User Groups

4.3.1.1 Defining and Assigning Policies to User-Defined User Groups

Several user-defined User Group parameters are relevant only if your site supports a Cloud in **Internal** mode. In this case, you must configure the cloud. For instructions, see Configuring Cloud Settings in Internal Mode, **before** you configure the relevant user-defined User Group parameters.

You can create and define user-defined User Groups according to need.

To define a user-defined User Group and assign it policies:

1. Select **Users | Users/User Groups**.

2. In the tree, do either of the following:

    *   To create a user group, right-click on the **User Groups** main node and select **Add Group**. The User Group Details screen is displayed in the main window.

    *   To edit an existing user-created user group, select the group. Then, in the User Group Details screen that is displayed in the main window, click **Edit**.

3. Specify or edit a name for the group.

4. To assign the group different Security, Logging, and/or HTTPS policies, select the desired policies in the drop down lists.

5. If in Internal mode, enable certification of new users in the group, and prevent disabling Mobile Security Client, see To enable automatic certification of all new users in a group, and to prevent disabling of the Mobile Security Client:.

6. In the **IP Ranges** section displayed for all groups except the Unknown Users group, specify the IP address ranges, from/to values, for the group. Click ✚ to add a row.

7. Click **Save**.

8. If you are ready to distribute and implement the changes in your system devices, click ⬇.

4.3.1.2 Assigning Policies to Trustwave-Predefined User Groups

SWG comes with the following predefined User Groups

*   Cloud User Groups **Blocked Cloud Users** group and **Revoked Cloud Users** group do not hold users, but the policies you assign to these groups are applied to users whose certificates are blocked or revoked.

*   **Independent Users** group— this is where you create users who do not belong to a User Group. You can therefore assign Security, Logging, and HTTPS policies to each independent user.

*   **Unknown Users** group —used for assigning appropriate Security, Logging and HTTPS policies to unidentified users who are browsing through SWG.

To assign policies to Trustwave-predefined User Groups:

1. Select **Users | Users/User Groups**.

2. In the tree, select the group. Then, in the User Group Details screen that is displayed in the main window, click **Edit**.

> The **Independent Users** group does not have a details screen, because you assign it policies. Rather, you can only assign policies individually to the users within the group.

3. For user-created groups only: If you are creating a new group, specify a name for the group. If you previously created the group, you can edit the name, if desired.

4. To assign the group different Security, Logging, and/or HTTPS policies, select the desired policies in the drop down lists.

5. For the predefined **Unknown Users** group only: If you want unidentified User IDs or IP addresses added to the Unknown Users group, select the check box in the **New Users** area.

> In the **Blocked Cloud Users** and **Revoked Cloud Users** groups, the IP Ranges section is not relevant and should be ignored.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ⇲.

4.3.2 Adding and Defining Users

You can create users in the relevant user-defined User Groups, or in the pre-supplied **Independent Users** group if the user should not belong to a group.

Users in user-defined User Groups are automatically assigned the group's Security, Logging, and HTTPS policies; these assignments cannot be changes at the user level.

Users in the **Independent Users** group are automatically assigned the site-default Security, Logging, and/or HTTPS policies. You can, however, change these assignments individually for each user.

To add/define a user:

1. Select **Users | Users/User Groups**.

2. In the tree, do either of the following:

   • To create a user, right-click the user-defined User Group to which the user will belong or the **Independent Users** node if the user will not belong to a group, and select **Add User**. The User Details screen is displayed in the main window.

   • To edit an existing use, select the user. Then, in the User Details screen that is displayed in the main window, click **Edit**.

3. Specify a User Name and email address for the user. Note that you can supply descriptive name instead of the real or full name. You can specify the real or full name in the **Identifiers** area below.

4. In the **Identifiers** section, specify the identifiers that can be used to uniquely identify the user to the system. You can specify an IP address or range, and/or a user name: Select the identifier type and specify the value. Click ![icon] to add a row. For user name, you can specify an appropriate domain_name\user_name.

5. **For Independent Users only**: If the user should be assigned Security, Logging, and/or HTTPS policies other than those defined as the site-defaults, select the desired policies in the drop down lists.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ![icon].

4.3.3 Moving Users To a Different Group

To move a user from one Group to another:

1. If the User Group is not displayed, select **Users | Users/User Groups**.

2. In the tree, right-click on the node of the source User Group from which you want to move users, select **Move Users**.

    In the main window, the Move Users screen displays the Users in the selected group.

3. Select the check box of the users that should be moved. Note the following:

    • To select all the users, select the check box in the gray Name header line.

    • If the user list spans multiple pages, you can page through using the **Next**/**Previous** buttons.

    • You can search on a user name prefix by entering the prefix in the **Find All** field and clicking **Search**. Note that the search is case sensitive. To clear the search results and re-display the full list, click **Clear**.

4. In the **To** field, select the destination User Group.

5. Click **OK**.

6. If you are ready to distribute and implement the changes in your system devices, click ![icon].

4.4 Defining User Lists

You can define and use User Lists to identify to which users rules of Security, Logging, and HTTPS policies should apply, and to identify which users should be excluded from those rules.

User lists can contain LDAP Groups and Users, and Trustwave User Groups and users.

To define a User List:

1. Select **Users | User Lists**.

2. In the tree, do either of the following:

   • To create a new user list, right-click on the **User Lists** main node and select **Add List**. The User List definition window is displayed in the main pane.

   • To edit an existing user list, select the list. Then, in the User List window, click **Edit**.

   The User List definition window contains 5 tabs, in addition to a **Name** field:

   • The first **Selected Members** tab displays a summary of the details that you selected in the other lists.

   • The other tabs, **LDAP Groups**, **LDAP Users**, **Trustwave User Groups**, and **Trustwave Users**, allow you to select existing values from those respective categories. Each of the tabs has the same format and works the same as the others. You can select values using any combination of the tabs.

3. Specify a name for the User List.

4. In any combination of tabs according to need, select the check boxes of the items that you want to include in the list. For any tabs, select items or edit a name for the list. To simplify the selection process, you can do the following:

   • To filter the display on a specific value, specify the value in the Find All field and click . To clear the filter, click .

   • If useful, you can select/clear the **Select** check box to select/clear all items in the list, and then adjust the selected items as needed.

5. When done, click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click .

PART 3: Configuring Advanced Network Settings

This part contains the following chapters:

- Chapter 5: Implementing Identification Policy
- Chapter 6: Implementing Authentication
- Chapter 7: Defining and Customizing Upstream Proxy Policy
- Chapter 8: Enabling and Customizing Caching
- Chapter 9: Assigning Policies To Devices

5 Implementing Identification Policy

The process of implementing security for users at your site involves performing the following tasks:

- Defining Security Policy. For instructions, see Defining and Customizing Security Policies.

- Defining User Groups and Users, and assigning them security policies. For instructions, see Defining and Managing Users.

- Defining the Identification policy, as described in this chapter.

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

Regardless of the type of Identification policy, as soon as the Secure Web Gateway identifies a user by confirming a matching identifier, the assigned Security policy is enforced.

This chapter includes the following procedures:

- Defining and Customizing Identification Policy

- Defining an Active Directory

5.1 Defining and Customizing Identification Policy

Trustwave provides several predefined Identification Policies.

Unlike other pre-supplied policies, you can directly edit some pre-supplied Identification Policies.

Possible Identification Policies are:

- **Authentication** — authenticates end-users using an Authentication Server.

- **Default Cloud Scanners Read Headers Policy** — identifies users based on pre-authenticated HTTP headers for regular and Cloud scanners.

- **Get User Credentials** — identifies users via USERID information using the NTLM protocol without verifying user password against the authentication server.

- **Read Headers** — identifies users based on pre-authenticated HTTP headers for regular scanners only.

- **Source IP Only** — identifies users by Source IP. This is the default policy.

For more information, see the *SWG User Identification Guide*.

To set and customize Identification Policy:

1. Decide which policy should be used for the Identification Policy.

2. If you choose Authentication as the policy, before proceeding with the rest of the steps in this procedure, define the Active Directory. For instructions, see Defining an Active Directory.

3. Select **Policies | Device Policies | Identification**.

4. In the tree, expand the **Policies** root, and select and expand the policy that you are implementing.

5. To edit the rules in the policy, do the following:

   Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.

   For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

   a. Select the rule and click **Edit**.

   b. Choose the **Action** according to the following table. Then fill in the accompanying fields which vary according to the action chosen.

   For more information, see the *Management Console Reference Guide*.

If...	Then...
...the end-user should be identified by source IP:	Choose the default **Identify by Source IP**. There are no accompanying fields.
...SWG should communicate with the client to get User ID information, and then validate the information against an external Authentication site:	Choose **Authenticate**. Then, in the accompanying displayed fields: 1 Select the Authentication Protocols **Basic**, **NTLM**, or **Basic and NTLM**. 2 Select the Authentication site. The drop down list includes all customer Authentication domains defined in the Authentication Directories.
...the SWG should get user identification via NTLM or other method:	Choose **Get User Credentials**. Then, in the accompanying displayed field, select the Authentication Protocols **Basic**, **NTLM**, or **Basic and NTLM**.
...a downstream device proxy provides user information by forwarding device specific HTTP headers within the request:	Choose **Identify by Headers**. Then, in the accompanying displayed field, select the type of pre-authenticated headers. The drop down list includes the headers that have been pre authenticated. SWG comes with default pre authenticated values. You can modify these values via **Policies	Condition Elements	Pre Authenticated Headers**.

6. Click **Save**.

7. Add Conditions to extend authentication functionality, for example where a header field condition is used to exclude a specific user agent.

   a. To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

   b. To add a new condition to a rule:

      i. Right-click the rule and choose **Add Condition**. The main window displays the Condition Definition screen.

      ii. In the **Condition Name field**, select the type of condition in the drop down list. The list contains the following Condition types:

      - **Destination Port Range** — distinguishes client application connecting to Trustwave SWG by the target destination port. The default rule allows the administrator to exclude a list of Port ranges.
      - **Header Fields** — limits direct internet access according to header name and value.
      - **IP Range** — limits direct internet access according to IP ranges.
      - **Location** — limits direct internet access according to location of the scanning server both for Cloud or Local.
      - **URL Lists** — limits direct internet access according to the target URL.

   For any selected condition type, the window displays an appropriate check box list. For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide.*

8. Click **Save**.

9. Set the defined policy as the Identification Policy, as follows:

   a. Select **Administration | System Settings | Trustwave Devices**.

   b. Expand the tree for the device and choose **Scanning Server | General**.

   c. In the main screen on the right, click the **Device Policies** tab, and then click **Edit**.

   d. In the **Identification Policy** field, select the policy.

   e. Click **Save**.

10. If you are implementing an Authentication-type Identification policy, you should configure device Authentication parameters (for example, if and how long to retain Authentication data). For instructions, see Implementing Authentication.

11. If you are ready to distribute and implement the changes in your system devices, click ⚡.

12. Test the identification policy by having a user browse, and then check the log to ensure that the Identification policy has been enforced.

Defining an Active Directory

This procedure needs to be performed only if you are defining an Authentication type policy as your Identification Policy. In this case, it should be performed *before* defining the Identification Policy.

1. Select **Users | Authentication Directories | Active Directories**.

2. In the configuration tree, right-click the **Active Directory** root branch, and click **Add Site**.

3. Define the Active Directory as follows:

    a. Assign a name to the Active Directory.

    b. Ensure that the **Active** check box is selected unless there is a reason why you would not want it active.

    c. Specify the Domain Name.

    d. In the Domain Controller Selection Method, select the appropriate value **Primary-Backup** or **Load Balancer**.

    e. For each Domain Controller, do the following:

        i. Click the icon.

        ii. Fill in the Controller Name.

        iii. If the Authentication Server requires it, select the **Force NTLM v2** check box.

    f. For each Trusted Domain, do the following:

        i. Click the icon.

        ii. Fill in the domain name.

4. Click **Save**.

5. If you are ready to distribute and implement the changes in your system devices, click .

6 Implementing Authentication

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

If you will be assigning a Scanning Server an Authentication-type Identification policy, you must configure Authentication parameters for that Scanning Server (for example, if and 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.

You can figure default Authentication settings, and then alter the defaults for specific Scanners, as needed.

> Before performing the following procedures, ensure that you:
>
> • Created an Active Directory. For instructions, see Defining an Active Directory.
>
> • Defined/customized an Authentication-type Identification Policy. For instructions, see Defining and Customizing Identification Policy.

6.1 Configuring Default and Scanning Server Authentication

> For instructions on configuring NTLM Authentication on Windows 7, 2008 Server, and Vista, see the *SWG Identification Guide*.

To configure Authentication Settings:

1. Select **Administration | System Settings | Trustwave Devices**.

2. Do either of the following in the configuration tree:

    • To configure Default Authentication settings, choose **Devices | Default Values | Device Settings | Authentication**.

    • To configure Authentication settings for a specific Scanning Server, choose *<device_group>* | *<device_ip>* **| Scanning Server | Authentication**.

3. In the main screen on the right, click **Edit**.

4. In the **Configuration** tab, configure the Authentication Retention Method parameters by doing one of the following:

    • If the Scanning server should not retain authentication data but should instead request authentication for each call, select **No Retention**, and then continue with Step 5.

    > If the Scanning Server is configured to work in Transparent mode, *No Retention* is not a valid option.

- If during the session the Scanning server should only authenticate the first transaction from the IP address and treat the remaining transactions from that address as already authenticated:

    i. Choose **IP Caching**.

    ii. Set the time-out interval in minutes that ends the session.

    iii. Continue with Step 5.

- If during the session the Scanning server should perform authentication for different Web sites:

    i. Click **Cookie**.

    ii. If the cookie should be encrypted, select the **Use Encryption** check box.

    iii. If the cookie should be retained for the duration of the time-out interval, select the **Persistent** check box and set the time-out interval.

    iv. Continue with Step 5.

5. In the **Advanced** tab, configure the Advanced Authentication Settings, as follows:

    a. To enable token reuse, select the **Enabled Challenge Token Reuse (NTLM Settings)** check box.

        i. In the **Random Challenge Token Reuse Number** field, specify the number of times a Challenge Token can be reused.

        ii. In the **Challenge Token Lifetime** field, specify the time in seconds before SWG generates a new Challenge Token.

    > Using this option, and increasing the token usage number and time interval, saves authentication time and proxy resources, but decreases the system security level.

    b. In the **Active Directory Connection to Authentication Servers** area, set the time-out and retry values for situations where the Active Directory does not respond to the Scanning Server requests for authentication:

        i. In the **Connection Timeou**t field, set the time-out, in seconds, before the Scanning Server considers the Active Directory as not in service.

        ii. In the **Try Reconnect After** field, set the time-out, in seconds, before the Scanning Server re-tries to connect to the Active Directory.

    c. If the Secure Web Gateway should work in Transparent Proxy mode, do the following in the **Transparent Authentication** area:

        i. In the **Virtual Redirection Hostname** field, 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.

        ii. In the **Virtual Redirection Port** field, specify the TCP port number to be used for redirection.

d. In the **Replace Domain With** field, specify the correct domain that should be used to replace erroneously-specified "domains" by the user (for example, if the user specified a computer name instead of a domain name).

e. If an upstream proxy can and should authenticate users through the Secure Web Gateway system, select the **Forward Upstream Proxy Authentication** check box. In this case, Secure Web Gateway will not perform authentication, but will instead forward proxy authentication from the downstream client.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

7 Defining and Customizing Upstream Proxy Policy

By default, that is when using the only pre-supplied Upstream Proxy policy, Scanning servers are allowed direct access to the internet in every situation.

To limit Scanning server direct access in certain situations, and instead direct the Scanning server to an Upstream Proxy, you need to define and assign it an appropriate Upstream Proxy policy.

This chapter contains the following procedures:

- Defining an Upstream Proxy Policy

- Defining a Rule in an Upstream Proxy Policy

- Defining Conditions in an Upstream Proxy Rule

7.1 Defining an Upstream Proxy Policy

You cannot edit a pre-supplied Upstream Proxy Policy. However, you can duplicate such a policy and edit the duplicate; you can also create an Upstream Proxy policy from scratch.

To define an Upstream Proxy Policy

1. Select **Policies | Device Policies | Upstream Proxy**.

2. Do one of the following:

   - To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

   - To duplicate an Upstream Proxy policy, right-click the policy in the tree that you want to duplicate, and choose **Duplicate Policy**.

   - To edit a policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

   The Policy Definition screen is displayed in the main window.

3. If adding a policy enter a name for the policy.

4. If adding a policy enter the policy description, and if duplicating or editing a policy, the policy description can be modified.

5. When done, click **Save**.

6. Continue with Defining a Rule in an Upstream Proxy Policy.

7.2 Defining a Rule in an Upstream Proxy Policy

If you duplicated a policy, it already has the same rules as were found in the original policy. You can edit these rules. You can also create new rules from scratch.

> Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.
>
> For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

To define a rule in an Upstream Proxy policy

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining an Upstream Proxy Policy.

2. Do any of the following:

   - To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

   - To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

   - To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**.

   The main window displays the Rule Definition screen.

3. Enter a name for the rule.

4. (Optional) Provide a description of the rule.

5. If the rule has an **Enable Rule** check box, ensure that the check box is appropriately selected or cleared, depending on whether or not the rule should be enabled after being committed.

6. Choose the Action. The only allowed action is **Direct**.

7. Click **Save**.

8. To make triggering of the rule conditional, continue with Defining Conditions in an Upstream Proxy Rule.

9. To define additional rules in this policy, repeat this procedure.

10. If you are ready to distribute and implement the changes in your system devices, click .

7.3 Defining Conditions in an Upstream Proxy Rule

To define conditions in an Upstream Proxy Rule:

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define an Upstream Proxy Policy.

2. Do either of the following:

   - To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

   - To add a new condition to a rule:

   a. Right-click the rule and choose **Add Condition**.

   The main window displays the Condition Definition screen.

   b. In the **Condition Name field**, select the type of condition in the drop down list. The list contains the following Condition types:
   - **Header Fields** — limits direct internet access according to header name and value.
   - **IP Range** — limits direct internet access according to IP ranges.
   - **Location** — limits direct internet access according to location of the scanning server for both Cloud or Local.
   - **URL Lists** — limits direct internet access according to the target URL.

   For any selected condition type, the window displays an appropriate check box list.

   For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide.*

3. If the condition has any other special fields or requirements to fill in, fill them in appropriately.

4. Click **Save**.

5. If you are ready to distribute and implement the changes in your system devices, click .

8 Enabling and Customizing Caching

You can enable caching as the device defaults or enable caching for specific Scanning Servers. When caching is enabled, content is stored in the Server for future use, thereby speeding up performance time.

Before enabling caching, the pre-requisites of installing the **Caching Kit** with the relevant licenses must be completed.

After you enable caching, you must ensure that an appropriate caching policy is set.

Only HTTP responses are cached.

By default, when caching is enabled, all content is cached. But you can use Caching policies to bypass caching or to determine which URLS or File extensions are cached.

This chapter contains the following procedures:

- Enabling Caching

- Defining a Caching Policy

- Defining a Rule in a Caching Policy

- Defining Conditions in a Caching Rule

8.1 Enabling Caching

To enable caching:

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device configuration tree, do either of the following:

   - To configure caching as the device default, select **Devices | Default Values** | **Device Settings** | **Cache**.

   - To configure caching for a specific Scanning Server, select *<device_group>* | *<device_ip>* | **Scanning Server** | **Cache**.

3. In the Cache main window, click **Edit**.

4. Select the **Enable Caching** check box.

5. Click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click ![icon].

8.2 Defining a Caching Policy

You cannot edit a pre-supplied Caching Policy. However, you can duplicate such a policy and edit the duplicate; you can also create a Caching policy from scratch.

To define or duplicate and edit a Caching Policy

1. Select **Policies | Device Policies | Caching.**

2. Do one of the following:

    - To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

    - To duplicate a Caching policy, right-click the policy in the tree that you want to duplicate, and choose **Duplicate Policy**.

    - To edit a policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

    The Policy Definition screen is displayed in the main window.

3. Enter a name for the policy.

4. (Optional) Add or modify the policy description.

5. Click **Save**.

6. Continue with Defining a Rule in a Caching Policy.

8.3 Defining a Rule in a Caching Policy

If you duplicate a policy, it will have the same rules as in the original policy. You can edit these rules or create new rules from scratch.

Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.

For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

To define a rule in a Caching policy:

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining a Caching Policy.

2. Do any of the following:

   - To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

   - To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

   - To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**.

   The main window displays the Rule Definition screen.

3. Enter a name for the rule.

4. (Optional) Provide a description of the rule.

5. If the rule has an **Enable Rule** check box, ensure that the check box is appropriately selected or cleared, depending on whether or not the rule should be enabled after being committed.

6. Choose the **Rule Action,** as follows:

   - If Web content should be cached, choose **Cache**.

   - If Web content should not be cached, choose **Bypass Cache**.

7. Click **Save**.

8. To make triggering of the rule conditional, continue with Defining Conditions in a Caching Rule.

9. To define additional rules in this policy, repeat this procedure.

10. If you are ready to distribute and implement the changes in your system devices, click .

8.4 Defining Conditions in a Caching Rule

To define conditions in a Caching Rule

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define or duplicate and edit a Caching Policy.

2. Do either of the following:

   - To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

   - To add a new condition to a rule:

   a. Right-click the rule and choose **Add Condition**.

   The main window displays the Condition Definition screen.

   b. In the **Condition Name field**, select the type of condition in the drop down list.

   For any selected condition type, the window displays an appropriate check box list.

   For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

3. If the condition has any other special fields or requirements to fill in, fill them in appropriately.

4. Click **Save**.

5. If you are ready to distribute and implement the changes in your system devices, click .

9 Assigning Policies To Devices

The following types of policies are relevant at the device level: **Identification**, **Device Logging** (described in Performing Additional Configuration Tasks), **Upstream Proxy**, **Caching,** and **ICAP clients**.

Some policy types (for example, Caching) require that relevant functionality be enabled and defined. For details, see the *Management Console Reference Guide*.

SWG comes with specific policies of the above types assigned as the device defaults. You can set different policies of the above types as defaults, and you can assign other policies of the above types to specific devices.

This chapter contains the following procedures:

- Setting Device Policy Defaults

- Assigning Policies to Specific Devices

9.1 Setting Device Policy Defaults

To assign device default policies:

1. Select **Administration** | **System Settings** | **Trustwave Devices**.

2. In the Trustwave Devices tree, expand the Devices root note, and select **Devices | Default Values** | **Device Settings** | **General**.

3. In the main window, click **Edit**.

4. In the **Device Policies** tab, set which policy will be the default for the particular policy types.

5. When done, click **Save**.

6. In the Trustwave Devices tree, right-click **General**, then click **Reset all General modules with default values**.

7. If you are ready to distribute and implement the changes in your system devices, click .

9.2 Assigning Policies to Specific Devices

To assign policies for specific devices:

1. Select **Administration** | **System Settings** | **Trustwave Devices**.

2. In the Trustwave Devices tree, expand the Devices root note, and select *<devices_group>* | *<device_ip>* | **Scanning Server** | **General**.

3. In the main window, click **Edit**.

4. In the **Device Policies** tab, set which policy will be the default for the particular policy types.

5. When done, click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click .

PART 4: Configuring Logging and Alert Settings

This part contains the following chapters:

10 Defining and Customizing Logging Policy

Logging policy determines, at the user level, what types of user transaction events, either blocked, allowed or all, will be logged, and to where the information is sent (logs, archives, reports, etc.). The only action that a Logging Policy rule can perform is to log the transaction or not log it. You can set different logging policies for different user groups and independent users.

This chapter contains the following procedures:

- Defining a Logging Policy

- Defining a Rule in a Logging Policy

- Defining Conditions in a Logging Rule

10.1 Defining a Logging Policy

> You cannot edit a pre-supplied Logging Policy. However, you can duplicate such a policy and edit the duplicate; you can also create a Logging policy from scratch.

To define a Logging Policy:

1. Select **Policies | Logging**.

2. Do one of the following:

    - To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

    - To duplicate a Logging policy, right-click the policy in the tree that you want to duplicate, and choose **Duplicate Policy**.

    - To edit a Logging policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

    The Policy Definition is displayed in the main window.

3. Enter a name for the policy.

4. (Optional) Add or modify the policy description.

5. When done, click **Save**.

6. Continue with Defining a Rule in a Logging Policy.

10.2 Defining a Rule in a Logging Policy

If you duplicated a policy, it already has the same rules as were found in the original policy. You can edit these rules or create new rules from scratch.

You can specify if the rule should be applied to specific users and/or if specific users should be excluded. One method is by specifying User Lists to which the rule should or should not apply.

> If you will be using User Lists to identify users to which the rule should or should not apply, be sure to define those lists.
>
> For instructions, see Defining User Lists.

To define a rule in a Logging policy

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining a Logging Policy.

2. Do any of the following:

   > Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.
   >
   > For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

   - To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

   - To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

   - To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**. The main window displays the Rule Definition screen.
     The screen contains three tabs: **General**, **Applies**, and **Except**.

3. Fill in the **General** tab as follows.

   a. Enter a name for the rule.

   b. (Optional) Provide a description of the rule.

   c. If the rule has an **Enable Rule** check box, ensure that the check box is appropriately selected or cleared, depending on whether or not the rule should be enabled after being committed.

   d. In the **Send To** area, check the locations to which the transaction data should be sent. The options are as follows:
      - Weblog — Sends information to the Trustwave log database, which is viewable via the Log View.
      - Archive — Sends log information in files to an external remote location. This selection ensures that relevant information is archived.
      - Report — Sends information to the Trustwave reports database.
      - Syslog — Sends information to one or two UNIX Syslog facilities logging data.

4. To apply the rule to specific users, select the **Applies** tab, and click the radio button for the category of users to which the rule should apply. Note the following:

   - **All Users** is the default.

   - **All Recognized Users** All users identified by the system.

   - **All Unrecognized users** are all transactions that have only IP address information and belong to the unknown users groups. For more information, see the *Management Console Reference Guide*.

   - If you chose Select User Lists, select the check boxes of the User Lists that contain the users to which the rule should apply.

5. To exclude specific users from application of the rule, select the **Except** tab, and select the check boxes of the User Lists which contain the users who should be excluded.

6. Click **Save**.

7. To make triggering of the rule conditional, continue with Defining Conditions in a Logging Rule.

8. To define additional rules in this policy, repeat this procedure.

9. If you are ready to distribute and implement the changes in your system devices, click .

10.3 Defining Conditions in a Logging Rule

To define conditions in a Logging Rule:

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define a Logging Policy:.

2. Do either of the following:

   - To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

   - To add a new condition to a rule:

   a. Right-click the rule and choose **Add Condition**.

   b. The main window displays the Condition Definition screen.

   c. In the **Condition Name field**, select the type of condition in the drop down list.

   d. For any selected condition type. except **Malware Entrapment Profile**, the window displays an appropriate check box list.

   For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

3. If the condition is **Malware Entrapment Profile**, skip to Step 7.

4. If the window displays an **Applies To** area above the list, select whether the condition will apply to the items you check or to the items you do not check.

5. Select the appropriate check boxes in the list. If the window displays a **Select/Deselect** All check box, you can use this if it will be useful.

> **For Logging policy rules:**
> - The conditions selected must match those of the Security Policy rule in order for the relevant transactions to appear in the Log View.
> - The condition type called **Rule Action** logs transactions based on checked end-user actions (for example, Allow, Block).
>   - To select more than one Rule Action, but not all of them, in the Rule Action list, you must add a separate rule for each action you want to select.
>   - To log all end-user actions do not include the condition called **Rule Action**.

6. If the condition has any other special fields or requirements to fill in, fill them in appropriately. Then skip Step 7, and continue with Step 8.

7. Perform this step only if the condition name is **Malware Entrapment Profile**. The window displays a Security level setting line with the default setting; **None**. Depending on the policy type, it might also display an HTML repair check box. Do the following:

   a. To change the Security level setting, slide the sliding button to the appropriate value (for example, **Basic** or **Strict**).

   For information about the level, click the relevant level link (for example, **Medium**). The Secure Web Gateway Rule Updates window opens. This window allows you access relevant information.

   b. If HTML pages should be repaired if needed, and the **HTML Repair** check box is displayed, select the check box.

8. Click **Save**.

9. If you are ready to distribute and implement the changes in your system devices, click ![icon].

11 Configuring the Log Server

A lone Log Server always resides on the Policy Server machine.

Log Relays resident on each device receive the following types information, which is then collected from the relays by the Log Server, and routed to appropriate locations: Web transaction information from the Scanner, system message information from the System log, and Audit message information.

By default, the Log Server sends this information to the Log file and the Reports file, both of which are internal files. However, depending on the Logging Policy definition, the Log Server can also:

*   send Scanner, System log and/or Audit information to the Syslog file

*   send Scanner information to an Archive (zip) file.

11.1 Configuring Log Server Settings

This task consists of the following procedures:

*   To configure the Log Server:

*   To configure Log Relays and their schedules:

*   To have log messages sent to the Syslog:

*   To configure Scanner Messages sent to a Syslog:

*   To have Web Log messages sent to Archive:

*   To enable and configure log retention:

To configure the Log Server:

1. Select **Administration** | **System Settings** | **Trustwave Devices**.

2. In the Device tree, under the device that contains the Log Server, select **Log Server** | **Log Properties**.

    The main window displays the Log Server Properties screen. This screen displays the **Enable Log** field and the following tabs: **Collect Logs From**, **Syslog Targets**, **Syslog Fields**, **Log Archiving**, and **Web Log Retention**.

3. Click **Edit**.

4. Do either of the following:

    *   To configure the Log Server, fill in the relevant tabs in sequence, as described below:

        *   If your site has multiple scanners, configure their Log Relays and their schedules in the **Collect Logs From** tab. For instructions, see To configure Log Relays and their schedules:.
        *   To have log messages sent to the Syslog, configure the target Syslog files in the **Syslog Target** tab. For instructions, see To have log messages sent to the Syslog:.

- If you are sending Scanning Server messages to a Syslog, define the configuration options for those messages in the **Syslog Fields** tab. For instructions, see To configure Scanner Messages sent to a Syslog:.
- To have Scanner Web Log messages sent to the Archive, define the Archiving configuration in the **Log Archiving** tab. For instructions, see To have Web Log messages sent to Archive:.
- To enable log retention and configure how many weeks logs should be retained, define the configuration in the **Web Log Retention** tab. For instructions, see To enable and configure log retention:.

- To disable the Log server, clear the **Enable Log** check box. Then click **Save**. If you are ready to distribute and implement the changes in your system devices, click ⟱.

To configure Log Relays and their schedules:

This procedure is relevant only if your site is using multiple scanning servers.

By default, the Log server collects the information from each Log Relay every few seconds. However you can limit the collection times to specific time frames that you can define for each Log Relay.

These 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.

In the **Collect Logs From** tab of the Log Properties screen, do the following:

1. To stop the passage of logs from a particular Log Relay, clear the **Active** check box.

2. To define a time frame during which the Log Server will collect logs from the Log Relay:

   a. Click the ⊞ icon in the **Scheduling** column.

   b. In the displayed time frame definition area, specify a **From** time and **To** time. To define multiple ranges click the ➕ icon.

3. If the connection to a Log Relay should be secure, click **Secured**.

4. To have log messages sent to the Syslog, continue with To have log messages sent to the Syslog:. Otherwise, do either of the following:

   - To have log messages sent to Archive, continue with To have Web Log messages sent to Archive:.
   - If you have completed Log Configuration, click **Save**, and then if you are ready to distribute and implement the changes in your system devices, click ⟱.

To have log messages sent to the Syslog:

In the **Syslog Target** tab of the Log Properties screen, do the following for each message type, System Log, Scanner, and/or Audit, that you plan to send to a Syslog:

1. In the top set of entry fields, on a Facility line, beginning with Facility1, define a facility, as follows:

a. In the **Facility Mode** field, select a mode label — use this label to differentiate Trustwave logs from each other and from other platforms' logs on the remote Syslog server.

b. In the **Primary IP** field, specify the Primary Syslog Server target address.

c. In the **Primary Port** field, specify the Primary port to which the Syslogs will be sent.

d. Optionally, specify the Secondary Syslog Server target address and secondary port, in the **Secondary IP** field and **Secondary Port** field, respectively.

2. In the bottom set of entry fields, for each message type to be sent to the Syslog, select its check box, and select the facility that you defined for it.

3. Continue with To configure Scanner Messages sent to a Syslog:.

To configure Scanner Messages sent to a Syslog:

> This procedure is relevant and mandatory only if you are sending Scanner messages to the Syslog.
>
> Also, ensure that the **Send To: Syslog** check box is selected in the Logging Policy rules for logging information to be sent to Syslog, and that logging policy is assigned to users. If a rule's **Syslog** check box is not selected, its logging information will not be sent to Syslog.
>
> To verify that **Send To: Syslog** is selected, see To define a rule in a Logging policy.

In the **Syslog Fields** tab of the Log Properties screen, do the following:

1. In the Syslog format, select the 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. 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.

2. Select the syslog transaction fields that should be logged.

3. Do either of the following:

    *   To have log messages sent to Archive, continue with To have Web Log messages sent to Archive:.
    *   If you have completed Log Configuration, click **Save**, and then if you are ready to distribute and implement the changes in your system devices, click ⋙.

To have Web Log messages sent to Archive:

Ensure that the **Send To: Archive** check box is selected in the Logging Policy rules for logging information to be sent to Archive, and that logging policy is assigned to users. If a rule's **Archive** check box is not selected, its logging information will not be sent to archive.

To verify that **Send To: Archive** is selected, see To define a rule in a Logging policy.

An additional archiving option is to integrate SWG to Security Reporter (SR). For more information on integrating SWG with SR, see To connect SWG to Security Reporter via archiving:.

In the **Log Archiving** tab of the Log Properties screen, do the following:

1. Specify the Log Archiving Locations as follows. Repeat these steps for each Archive location:

   a. Click the ✚ icon.

   b. If archiving should be enabled to this Archive, select the **Enable** check box.

   c. In the **Connection Method** field, select the method that the Log Server uses to connect to the Archive location:
      - **FTP** — connect using regular File Transfer Protocol.
      - **FTP Passive** — connect using File Transfer Protocol. This is where 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.

   d. Specify the Archive file Location, the User Name, and the Password. The format of these values that you specify depends on the connection method:

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.

Connection Method	Archive Location Format, User Name and Password
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.

2. 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 details on each format, see the Management Console Reference Guide.

3. To have the Archive location tested when you save the definition, select the **Test Archive Location on Save** check box. Otherwise, ensure that the check box is cleared.

4. In the **Log Archive Schedule** area, specify when archiving should be performed. You can specify a daily time or an interval between archive processing.

5. o either of the following:

- To have log messages sent to Archive, continue with To enable and configure log retention:.

- If you have completed Log Configuration, click **Save**, and then if you are ready to distribute and implement the changes in your system devices, click .

To connect SWG to Security Reporter via archiving:

In addition to the SWG Internal Reporting Tool, Trustwave provides support for integration with the Security Reporter. The Security Reporter (SR) is an advanced external reporter offering organizational, security, and productivity reports.

1. Select **Administration** | **System Settings**| **Trustwave Devices**.

2. In the tree, under **Devices**, select **Management Devices Group**, then the default IP node, then **Log Server**, and then **Log Properties**.

3. Click **Edit**. The main window is opened for editing.

4. Click the **Log Archiving** tab.

5. In the **Log Archiving Location** area click to add a new entry row.

6. Complete the SR details in the new row.

7. In the **Archive format** list click **Extended Format**.

8. Click **Save**.

9. If you are ready to distribute and implement the changes in your system devices, click .

To enable and configure log retention:

To enable log retention, do the following in the **Log Retention** tab of the Log Properties screen:

1. Select the **Enable Log Retention** check box.

2. In the Retention Period field, specify the number of weeks that logs should be retained.

3. When you have completed Log Configuration, click **Save**.

4. If you are ready to distribute and implement the changes in your system devices, click .

12 Configuring Alerts

Through the Alerts mechanism, SWG can notify you of system events, application events, update events, and security events. SWG can send alerts through two different communication channels, besides System Log messages: Email messages, and SNMP notification.

If alerts notification will go through SNMP, you must configure SNMP settings.

> Administrators can view Alerts sent via SNMP in the Dashboard, accessed by clicking the icon. For more information, see the Management Console Reference Guide

You can also enable and configure alert notifications if certain security thresholds are passed by incoming or outgoing traffic.

The task of configuring Alerts consists of the following procedures:

- Assigning Alert Channels to Event Types

- Configuring SNMP Settings

- Setting Thresholds For Security Alert Notification

Assigning Alert Channels to Event Types

To Assign Alert Channels to Event Types:

1. Select **Administration** / **Alerts** / **Alert Settings**.

   The Alert Settings window is displayed.

2. Click **Edit**.

3. For each type of Event, check the type of alert notification, either **SNMP** or **Email**, that should be sent.

4. For each event type for which you requested email alerts, specify the target email address. To specify more than one email address for an event type, click the icon, and select **Add Row**.

   > For Email alerts to be sent, you must configure the Mail Server, including selecting the **Enable Sending Email** check box. For instructions, see Configuring the Mail Server.
   >
   > For SNMP alerts to be sent, you must configure SNMP settings, including selecting the **Enable Trap Sending** check box. For instructions, see Configuring SNMP Settings in this chapter.

5. Click **Save**.

6. To distribute and implement the changes in your system devices, click .

12.1 Configuring SNMP Settings

If you are sending SNMP alerts, you must configure SNMP settings.

To configure SNMP settings:

1. Select **Administration | Alerts | SNMP Settings**.

   The **General** tab of the SNMP Settings window is displayed.

   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.

2. Click **Edit**.

3. To enable SWG to perform MIB monitoring:

   a. Ensure that the **Enable MIB** monitoring check box is selected.

   b. In the **Listening Port (input)** field, specify the port against which SWG should perform SNMP queries. The default port is 161.

4. To enable SWG to send traps:

   a. Ensure that the **Enable Trap Sending** check box is selected.

   b. In the **Trap Port (output)** field, specify the corresponding Trap Port. The default port is 162.

5. If the Policy server should be the Trap Destination Server, select the **Set Policy server as Trap Destination Servers** check box.

6. In the three entry fields to the right of associated check boxes, optionally specify up to three possible 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.

7. Select the **SNMP Version** tab. In this tab, you select with which version of SNMP the system will work, and define any needed parameters.

8. Choose the SNMP version, and do one of the following as appropriate:

   • If you chose SNMPv2.c, in the **Community** field define the group to which the devices and management stations running SNMP belong. The default string: "**finjan**". Then skip to Step 10.

   • If you chose SNPMv3, do the following:

   a. Define the SNMP MIB Monitoring parameters, as follows.

   > The Monitoring parameters define the security protocol and encryption methods used to obtain information from the SNMP agent on the machine. The information retrieved is part of a MIB.

i.   In the **Security Name** field, specify the SNMP user name.

ii.   In the **Security Level** field, select whether the messages should be sent **unauthenticated (None)**, **authenticated**, or **authenticated and encrypted**.

iii.   If you specified that the messages should be sent unauthenticated, that is, you specified **None**, skip to Step b below; otherwise, fill in the remaining parameters in the SNMP MIB Monitoring area as instructed in the following substeps.

iv.   In the **Authentication Protocol** field, select the Authentication Protocol — either verification checksums **MD5** or **SHA**.

v.   In the **Authentication Key** field, specify the user's authentication key, which signs the message being sent. There is a minimum 8 character requirement.

vi.   In the **Encryption Key** field, specify the user's encryption key, which encrypts the data portion of the message being sent. There is a minimum 8 character requirement.

> The encryption mode or privacy protocol used is DES encryption algorithm.

b.   Define the SNMP Traps parameters, by doing either of the following:

> SNMPv3 mandates that trap messages are rejected unless the SNMPv3 user sending the trap already exists in the user database. The user database in a SNMPv3 application is referenced by a combination of the user's name or Security Name, and an automatically supplied identifier for the given SNMP application or engineID.

•   To supply the same Security parameters (name, level, etc.) for SNMP Traps that you used for MIB Monitoring, select the **Use SNMP MIB Monitoring Information** check box.

•   Otherwise, fill in a **Security name**, S**ecurity level**, **Authentication Protocol**, **Authentication key** and **Encryption key** for SNMP Traps. The same as MIB Monitoring in Step 8a.

9.   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 with the SNMP name, IP and SWG Software Version.

10. Click **Save**.

11. If you are ready to distribute and implement the changes in your system devices, click .

12.2 Setting Thresholds For Security Alert Notification

You can have administrators alerted when blocked incoming events such as Malicious Activities, Viruses, Scripts, Binary Content, and/or blocked outgoing events such as URL Categorization, URL Lists, Blocked Files according to file types, reach certain thresholds.

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.

To set security thresholds for Alert Notification

1. Select **Administration / Alerts / Security Settings**.

2. In the Security Settings screen, click **Edit**.

3. Select the **Enable Security Alerts When** check box.

4. To enable alerts based on incoming traffic, select the check box dealing with **incoming** traffic notification and specify the following blocked incoming traffic figures:

   • **alert-triggering percentage** — amount of blocked incoming traffic, as a percentage of total incoming traffic, that will trigger an alert.

   • **minutes** — number of minutes over which the percentages should be measured.

   • **alert-clearing percentage** — amount of blocked incoming traffic, as a percentage of total incoming traffic, below which the alert will be cleared and it must be lower that the alert-triggering percentage.

5. To enable alerts based on outgoing traffic, select the check box dealing with **outgoing** traffic notification and specify the following blocked outgoing traffic figures:

   • **alert-triggering percentage** — amount of blocked **outgoing** traffic, as a percentage of total **outgoing** traffic, that will trigger an alert.

   • **minutes** — number of minutes over which the percentages should be measured.

   • **alert-clearing percentage** — amount of blocked **outgoing** traffic, as a percentage of total **outgoing** traffic, below which the alert will be cleared, and it must be lower that the alert-triggering percentage.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

PART 5: Performing Monitoring And Maintenance

This part contains the following chapters and procedures:

13 Viewing Security and Component Statuses

The Dashboard enables you to view security status information at a glance in the Dashboard. In addition, the configuration screens for some components allow you to view certain dynamic information about the components.

This chapter contains the following topics:

- Viewing Security Status Information (Dashboard)
- Viewing Dynamic Component Information

13.1 Viewing Security Status Information (Dashboard)

To view Security Status Information at a glance:

1. Click ![icon] in the Management Console toolbar to display the Dashboard.

   > If the **Updates Available** icon is enabled, there are Security or other updates for your system. You should download them from **Administration | Updates | Updates Management**. For more information, see Viewing and Installing Updates.

2. In the title bar of the **Performance** area, select the device and time period for which you want to display the information. The values you select affect the other graphs displayed in the window.

3. Alternatively, you can adjust the time period by moving the period slider that appears in a number of graphs. The time period can range from as far back as the last 12 months, or as recently as the last 12 hours.

4. To display details about the threat level, click the **Threat Level** link under the threat level gauge.

5. To display additional utilization details for a device, click the device in the **Device Utilization** area. Note: The button is red if alert messages are available for the device; otherwise, the button is green.

For information about the gauges and graphs in the Dashboard, see the *SWG Management Console Reference Guide*.

13.2 Viewing Dynamic Component Information

The following table lists the components for which you can view dynamic information, what information is displayed, and where and how to access it. For descriptions of the displayed information, see the *SWG Management Console Reference Guide*.

Table 1: Dynamic Component Information

Component	Information Displayed	How to Access
Device — status	Sync status, Connection Status, Committing Status, Last connection time, and Device Role and Activity Status	Select **Administration	System Settings	Trustwave Devices**. In the configuration tree, click the device. Information is displayed in the **Status** tab.
Logs —Web, System and Audit	See Viewing Logs	See Viewing Logs.
Scanning Engine **URL Filtering (Trustwave, IBM, Websense)**	Version, DAT version	Select **Administration	System Settings	Scanning	Scanning Engines**. In the Scanning Engine tree, click the engine.
List of Available Updates	Status, type, release date and time, description	Select **Administration	Updates	Updates Management**. For more instructions, see Viewing and Installing Updates.
System Info: **General**	Appliance MAC, Licensed seats, Licensed virtual cores, license expiration	Select **Administration	System Info**.
Licensed Modules	List of modules	
Installed components	Component List, Version, Release Date, Install date	

14 Viewing Logs

There are three types of logs:

- **Web Logs** — record Web-surfing transactions of users in your network, according to your logging policy.

- **System Logs** — record 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** — record all changes made or actions taken from the Management Console, including tracking the creation of and changes to, policies, as well as system configuration.

When viewing a log, you can perform a search for relevant IDs.

You can also create filters, and create, edit, and manage log profiles, for each log type.

This chapter contains the following topics:

- Viewing Logs

- Creating, Editing, and Managing Log Profiles

- Viewing Transaction Details (Web Log only)

14.1 Viewing Logs

To view a log:

1. Choose **Logs and Reports | *<logtype>***.

   The log is displayed with the default profile. The information displayed in each column for the log entries is generally self-explanatory. For a detailed description of the data, see the *SWG Management Console Reference Guide.*

2. Optionally, choose a different profile, which will adjust the columns displayed and the filtering of the display.

3. To edit the current profile, click Edit Profile ; to create a new profile, click Manage Profiles . Then see Creating, Editing, and Managing Log Profiles for instructions.

4. To find a specific log entry, enter the ID in the **Find *<type>* ID** field and click Search . For System and Audit logs, specify a Log ID; for Web logs, specify a transaction ID.

5. To re-display the full display, click Clear .

6. **For Web Logs only**:

   a. To display the logs of a different Admin Group, select the Admin Group. Note that you must have permissions to see the logs of the group.

b. To limit the Web log display to a specific time frame, either select a time frame value in the drop down list, or select a date range. Then click **Apply**.

c. To delete all current log entries in the Log table, click ❌ **Log Cleanup** .

> **Note**: You cannot stop or reverse Log cleanup once you request it.

d. To add a URL that appears in a Web log entry to the URL list, right-click the 📋 icon for the particular entry, and choose **Add to URL List.** This will enable it to be blocked or allowed in the User policy.

7. To display the details of a Web Log only transaction, see Viewing Transaction Details (Web Log only).

14.2 Creating, Editing, and Managing Log Profiles

A Profile is a definition that defines which columns to display in the Log view, and filtering specifications for each log entry. Each log type Web, System, and Audit, comes with a default profile and several have other profiles pre-supplied with the SWG application, but you can define additional profiles.

To create or edit a log profile:

1. Select **Logs and Reports | Log Profiles View |** *<logtype>* **Profiles**.

> If you are displaying a log, to create a profile, click **Manage Profiles**, and continue with the next step. To edit the profile being used in the log display, click **Edit Profile** and skip the next step.

2. Do either of the following:

    • To create a profile, right-click the **Profiles** root in the tree and choose **Add Profile**.

    • To edit an existing profile, select the profile in the tree, and in the main panel, click **Edit**.

3. Fill in a name for the profile, and optionally add a description. It is recommended to add a description.

    The Profile definition screen contains two tabs:

    • **General** — determines which data columns will be displayed.

    • **Filter** — sets filtering criteria for the data

4. In the **General** tab, define which data will be displayed as follows:

    a. Set the refresh interval in seconds.

    b. Set the number of entries to display. The maximum number of entries is 100.

    c. Select the check boxes of the data columns that you want displayed.

> The list of data columns varies with the type of log who profile you are defining.

5. In the **Filter** tab, define filtering criteria as follows:

At the bottom of the Filter tab is a toggle button **Switch To Advanced Mode | Switch To Simple Mode**.

- **Simple Mode**, which is the default mode, is useful when you define either a single filter, or when you define multiple filters that all have an AND relationship. This mode:
  - allows only AND relational operators; it does not allow OR operators.
  - does not display parentheses columns for defining complex relationships.
  - displays a Delete icon to the left of the Filter definition.
- **Advanced Mode** is useful when you are defining multiple filters having at least one OR relationship. This mode:
  - allows specification of AND and OR operators.
  - displays parentheses columns for defining complex relationships.

The procedures for defining filters for Logs and for Reports are very similar.

a. To add a new row, click ⊕. If a popup menu appears, select **Add Filter**.

b. In the **Field** drop down list, select the required filter type.

c. In the **Operator** drop down list that appears, select the relevant parameter (for example, Equals). Note that the **Operator** drop down list varies according to the selected filter type.

d. Depending on your selections, the **Value** field displays either a drop down list or a blank field.

e. Select or specify a value in the **Value** field to complete your initial filter selection.

f. To define multiple filter criteria:

   i. If an **Or** relationship is needed between any of the filters, click **Switch to Advanced Mode**.

   ii. Repeat steps Step a through Step e for each filter. If you are in Advanced mode, be sure to select the appropriate relationship operators, and add any needed parentheses.

A filter with parentheses cannot be switched back to Simple mode.

g. To delete a filtering row, click the 🗙 icon if it is displayed. Otherwise, right-click the 📄» icon of the row, and choose **Delete Filter.**

6. Click **Save**.

To delete a profile:

1. If the Profiles tree is not displayed, display it by selecting **Logs and Reports | Log Profiles View | *<logtype>* Profiles**.

2. Right-click the profile and choose **Delete Profile**. Then confirm the deletion.

14.3 Viewing Transaction Details (Web Log only)

You can view the transaction details of any displayed Web Log entry.

To view the transaction details of an entry in the Web log:

1. In the Web Logs display, click the ≡» icon or double-click on the selected transaction for the particular entry, and choose **Details** or **Open in a new window**.

    The Transaction Entry Details window is displayed.

    The Transaction Entry details window contains a number of tabs, transaction, user, policy, and so on, that displays information related to the transaction.

    For an explanation of the information displayed in the tabs, see the *SWG Management Console Reference Guide*.

    The transaction is automatically scanned for Request and response details, and if found, the types request and/or response are displayed in the tree under the Detail root.

2. To display the details of a request or response, click the Request or Response entry that is in the tree.

3. If you opened the Details display in the same window as the Web log, to return to the log click **Back**.

15 Viewing and Working With 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.

This chapter contains the following topics:

- Running and Viewing Reports

- Creating or Modifying Report Definitions

- Managing Reports

15.1 Running and Viewing Reports

You can run reports on demand — that is, at any time, as needed. You can also define regular schedules for running reports. For details, see Defining Report Schedules.

To run a report on demand:

1. Select **Logs and Reports | Reporting Tool | Reports**.

2. Expand the tree of report types as needed and display the report name in the tree; if you previously added it to your **Favorites** folder in the tree, you can find it there. For instructions on adding a report to the **Favorites** folder, see Adding Report Shortcuts to the Favorites Folder.

3. Right-click the report in the tree or **Favorites** folder, and choose **Run Report.**

4. In the main window, modify any parameters as needed. Pay special attention to the following:

5. In the **General** tab:

   a. Make any desired changes to the report format in the **View As** field, name and description.

   b. To save the report run results in the report's History, ensure that the **Run in Background** check box is selected. If this check box is not selected, the results are not automatically saved.

6. To change which columns are displayed in the report, and/or the report filtering criteria, make the changes in the appropriate tabs. For instructions, see Creating or Modifying Report Definitions.

7. Click the **Run Report** button at the bottom of the main window.

   - If the **Run in Background** check box was NOT selected, the results of the report run are displayed in a report window. To print or export the report, right-click the report and choose the desired action.

   - If the **Run in Background** check box was selected, to view the report you must access the Report History. For instructions, see Viewing a Report's History.

15.2 Creating or Modifying Report Definitions

SWG comes with a number of predefined reports, listed by category in the Report tree.

You can, of course, run a report as is. But you also can edit the definition of any report before running it, or duplicate a report and edit the definition of the duplicate, enabling you to define as many versions of the report as will be useful.

To create a report or modify an existing report:

1. Select **Logs and Reports | Reporting Tool | Reports**.

    The reports tree displays the list of report categories. Under each category are the currently existing report of that type.

2. Do either of the following:

    *   To edit the attributes of an existing report in the tree, select the report in the tree and when its attributes are displayed in the main window, click **Edit**.

    *   To create a report, right-click a similar report and select **Duplicate Report**.

    The Report definition details appear in the main window. The definition consists of three tabs: **General**, **Columns**, and **Filters**.

3. In the **General** tab, define the general details about the report: name, description, and format in the **View As** field.

4. In the **Columns** tab, select the data columns that should be displayed in the report.

5. In the **Filter** tab, define filtering criteria as follows:

    > At the bottom of the Filter tab is a toggle button **Switch To Advanced Mode | Switch To Simple Mode.**
    >
    > *   **Simple Mode**, which is the default mode, is useful when you define either a single filter, or when you define multiple filters that all have an AND relationship. This mode:
    >   *   allows only AND relational operators; it does not allow OR operators.
    >   *   does not display parentheses columns for defining complex relationships.
    >   *   displays a **Delete** icon to the left of the Filter definition.
    > *   **Advanced Mode** is useful when you are defining multiple filters having at least on OR relationship. This mode:
    >   *   allows specification of AND and OR operators.
    >   *   display parentheses columns for defining complex relationships.
    >
    > The procedures for defining filters for Logs and for Reports are very similar.

    a. To add a new row, click . If a popup menu appears, select **Add Filter**.

    b. In the **Field** drop down list, select the required filter type.

    c. In the **Operator** drop down list that appears, select the relevant parameter (for example, Equals). Note that the **Operator** drop down list varies according to the selected filter type.

d. Depending on your selections, the **Value** field displays either a drop down list or a blank field.

e. Select or specify a value in the **Value** field to complete your initial filter selection.

f. To define multiple filter criteria:

i. If an **Or** relationship is needed between any of the filters, click **Switch to Advanced Mode**.

ii. Repeat steps Step a through Step e for each filter. If you are in Advanced mode, be sure to select the appropriate relationship operators, and add any needed parentheses.

A filter with parentheses cannot be switched back to Simple mode.

g. To delete a filtering row, click the ✖ icon if it is displayed. Otherwise, right-click the ≣» icon of the row, and choose **Delete Filter.**

6. Click **Save**.

15.3 Managing Reports

This topic include procedures for the following:

- Defining Report Schedules

- Adding Report Shortcuts to the Favorites Folder

- Viewing a Report's History

- Exporting Reports

15.3.1 Defining Report Schedules

You can define multiple schedules for any report. When you define the schedule, you can also modify which columns are displayed and the filtering criteria, as part of the schedule.

When you define a schedule for a report, it appears in the tree under the report name.

To define a schedule for a report:

1. Do either of the following:

- To define a new schedule, right-click the report name and choose **Add New Schedule**.

- To modify an existing schedule, click the schedule name under the report name in the tree, and in the main window, click **Edit**.

The Scheduling dialog box is displayed. It contains the following tabs: **Report Schedule**, **Report Target, Columns**, and **Report Parameters**.

2. Specify a name for the report schedule in the **Schedule Name** field. Specifying a name is mandatory.

3. To activate the report schedule you are defining, select the **Enable Scheduling** check box at the top of the screen. To suspend the automatic report scheduling for any reason, clear the check box.

4. In the **Report Schedule** tab, define the actual schedule. You can specify any combination of the following scheduling criteria, though you must specify at least one set of criteria:

   - run the report once at a specified date and time

   - run the report daily, weekly, and/or monthly, at the specified times.

5. In the **Report Target** tab, which allows you to send the report to one or more targets, specify the following target information:

   a. If the report should be stored on the appliance and appear in the Available Reports screen, select the **Enable Available Reports** check box. Note that there is a space limitation of 1 GB for locally saved reports and that older reports will be erased once this limit is reached.

   b. If the report should be exported to the network location defined in Exported Reports Location, select the **Export report** check box.

   c. To email the report to specific addresses, select the Email to check box, and for each address, click the ⊞ icon, and specify the email address.

   > The ⊞ icon is inactive, and emails cannot be sent, until mail server configuration is complete. You can navigate to **Administration | System Settings| Mail Server** to complete the configuration.

6. In the **Columns** tab, ensure that only the data items that should be in the report are selected.

7. In the **Report Parameters** tab, define the filtering criteria as follows. Note that this tab is very similar to the Filters tab in the Report definition, and works essentially the same:

   > At the bottom of the Filter tab is a toggle button **Switch To Advanced Mode | Switch To Simple Mode.**
   > - **Simple Mode**, which is the default mode, is useful when you define either a single filter, or when you define multiple filters that all have an AND relationship. This mode:
   >   - allows only AND relational operators; it does not allow OR operators.
   >   - does not display parentheses columns for defining complex relationships.
   >   - displays a **Delete** icon to the left of the Filter definition.
   > - **Advanced Mode** is useful when you are defining multiple filters having at least on OR relationship. This mode:
   >   - allows specification of AND and OR operators.
   >   - display parentheses columns for defining complex relationships.
   >
   > The procedures for defining filters for Logs and for Reports are very similar.

   a. To add a new row, click ⊞. If a popup menu appears, select **Add Filter**.

   b. In the **Field** drop down list, select the required filter type.

   c. In the **Operator** drop down list that appears, select the relevant parameter (for example, Equals). The **Operator** drop down list varies according to the selected filter type.

    d. Depending on your selections, the **Value** field displays either a drop down list or a blank field.

    e. Select or specify a value in the **Value** field to complete your initial filter selection.

    f. To define multiple filter criteria:

        i. If an **Or** relationship is needed between any of the filters, click **Switch to Advanced Mode**.

        ii. Repeat steps Step a through Step e for each filter. If you are in Advanced mode, be sure to select the appropriate relationship operators, and add any needed parentheses.

        A filter with parentheses cannot be switched back to Simple mode.

    g. To delete a filtering row, click the ✖ icon if it is displayed. Otherwise, right-click the ▤» icon of the row, and choose **Delete Filter.**

8. Click **Save**.

15.3.2 Adding Report Shortcuts to the Favorites Folder

The **Favorites** folder serves as a repository for a selected group of reports created per Policy Server. It is designed to enable the administrator to view, schedule, or delete frequently used reports without scrolling through all Report Categories.

To add a report shortcut to the Favorites folder

1. If you are not already there, navigate to **Logs and Reports | Reporting Tool | Reports**.

2. Find the report in its category, and then right-click the report and choose **Add to Favorites**.

3. Clicking the report link in the **Favorites** folder will open the report editing screen, which provides all the same functionality used to configure original reports such as; Filters, Columns, and General report information.

4. To remove a report from the **Favorites** folder, find the report in the **Favorites** folder, and click **Remove from Favorites**.

15.3.3 Viewing a Report's History

The history of scheduled report runs is automatically saved.

You can also save the history of a report that you run on demand by running the report as a background process.

You can then view the report's history and any report saved in that history. The History screen provides the following report run details: Name, Recurrence, Status, Date, Time, and Format.

To view a report's history:

1. If it is not already selected, select **Logs and Reports | Reporting Tool | Reports**.

2. Do either of the following:

- To display the full report history, right-click the report either in the tree or in the **Favorites** folder, and choose **History**.

- To display the list of reports generated from a particular schedule of the report, right-click the schedule and choose **History**.

The History window provides report details such as Name, Recurrence, Status, etc.

3. To view an actual report run from the history, right-click the ▶ icon for the particular run, and choose **Show Report**. The report opens in a new window.

15.3.4 Exporting Reports

You can manually export reports that are currently open in a Report window. This applies to reports that were run on demand, and to report that you opened from the History file.

You can also define that scheduled reports be automatically exported. As part of this definition process, you must first define the Exported Reports Location. This requires that you choose a connection method. The chosen connection method, in turn, determines the content used to define your **Report Location**, **User to connect with** and **Password** fields

This section contains the following procedures:

- To manually export a currently-opened HTML report

- To define automatic export of a scheduled report:

- To define the Exported Reports Location:

To manually export a currently-opened HTML report

1. Place the cursor in the report area. A toolbar providing additional options is displayed.

2. Click 💾. A standard Windows Explorer window opens.

3. Save the file as needed.

To define automatic export of a scheduled report:

1. In the **General** tab of the report's schedule, select the **Export report** check box, and save and commit the change.

2. Define the Exported Reports Location, as described below in To define the Exported Reports Location::

To define the Exported Reports Location:

1. Navigate to **Logs and Reports** | **Reporting Tool** | **Exported Reports Location**. The Exported Scheduled Reports Location window is displayed.

2. In the main window, click **Edit**.

3. In the main window, click **Edit**.

4. In the **Connection Method** field, select the connection method. Possible values:

- **FTP** — connect using regular File Transfer Protocol.

- **FTP Passive** — connect using File Transfer Protocol where 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.

5. Specify the Report file location, User name and Password. The format of these values depends on the connection method:

<p style="text-align:center">Table 1:</p>

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/dir). **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.

6. Click the **Test** button to verify the connection.

7. If it works, click **Save**.

8. If you are ready to distribute and implement the changes in your system devices, click ⬇.

16 Maintaining Your System

This section contains the following topics and procedures:

- Performing Manual Backup and Restore

- Viewing and Installing Updates

- Importing From and Exporting Policy Databases

16.1 Performing Manual Backup and Restore

This section contains the following procedures:

- To manually backup your system:

- To restore a System backup:

- To manually backup your Reports database:

- To restore a Reports database backup:

To manually backup your system:

> Before performing backup, ensure that the backup settings have been configured. For instructions, see Configuring Backup Settings.

1. Select **Administration | Policy Server DB Backup | Backup Now**.

2. In the Backup Now window, specify a name or description for the backup file.

3. Click **Backup**.

To restore a System backup:

> If you have implemented the High Availability Policy Server feature, you must disable it before performing Rollback.

1. Select **Administration | Policy Server DB Backup | Backup Restore**.

2. In the Restore window, click **Edit**.

3. Click the icon adjacent to the backup that should be restored, and select Restore from the drop down menu.

4. Confirm that you want to perform the restore.

To manually backup your Reports database:

1. Select **Administration | Reports DB Backup | Backup Settings**.

2. Ensure that the backup configuration parameters are set. For instructions, see Configuring Backup Settings.

3. Click **Backup Now**.

To restore a Reports database backup:

1. Select **Administration | Reports DB Backup | Backup Restore**.

2. In the Restore window, click **Edit**.

3. Click the icon adjacent to the backup that should be restored, and select **Restore** from the drop down menu.

   A confirmation prompt withe the following message will appear: "Clicking restore will overwrite any pre-existing partition. Are you sure you want to restore this partition?"

4. Click **OK** in response to the Confirmation prompt.

   The Reports data will be restored to the system.

5. To verify that the operation was successful, check the System log.

16.2 Viewing and Installing Updates

In the Updates Management window, you can:

- 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.

   For more information on Offline Updates, contact your Trustwave representative and/or refer to the Offline Updates Technical Brief.

This task contains the following procedures:

- To upload and/or install an update:

- To view the list of installed updates:

- To generate a download key:

To upload and/or install an update:

1. Select **Administration | Updates | Updates Management**.

   The Updates Management window displays the list of available updates in the **Available Updates** tab.

The following icons in the **Status** column indicates the retrieval status of the available updates:

⚙ — indicates that an available update has been retrieved successfully.

⌛ — indicates that an available update is in the process of being uploaded/installed.

✖ — indicates that an upload/install has failed.

2. To upload an update, do either of the following as appropriate:

- If you are working remotely, click the **Retrieve Updates** button. It might take some time for the updates to be retrieved.

- To upload local updates, do the following:

   i. Click **Import Updates**.

   ii. In the displayed Import Local Update dialog box click **Browse** and browse to the local location containing the updates provided by Trustwave.

   iii. Click **Import**.

3. To view relevant details about an update, click the ⊞ icon next to the update.

4. To install an update, click 📋 next to the update, and select **Install Now**.

   The **Status** icon for the update will change as the install progresses. Once the update is installed, it is removed from the **Available Updates** tab and is displayed in the **Installed Updates** tab.

To view the list of installed updates:

1. Select **Administration | Updates | Updates Management**.

2. Display the **Installed Updates** tab. The tab lists both automatically installed and manually installed updates.

3. To view relevant details about an update, click the ⊞ icon next to the update.

To generate a download key:

1. Select **Administration | Updates | Updates Management**.

2. Select the **Update Key** tab.

3. Click **Generate Key**.

   The key is generated and appears in the tab. This feature requires that you have a special license to use the Offline Update application.

   ℹ️ If you are using Internet Explorer, you can copy the key to the clipboard. Firefox users do not have this option.

16.3 Importing From and Exporting Policy Databases

Administrators can export Security, HTTPS, Identification and Logging policy databases on a Policy Server to a file. They can then import policies, rules, conditions, and condition options from the exported database file into another Policy server. This only refers to administrator-created Policies, Rules and Conditions, not to Trustwave default Policies, Rules and Conditions.

When exporting, the exported files are encrypted and saved to a location specified by the administrator such as the local disk or network drive.

> Items for which the administrator does not have write permissions will not be exported.

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 task contains the following procedures:

- To export a policy database to a file:

- To import policies, rules, and conditions from an exported database file:

- To import condition options from an exported database file:

To export a policy database to a file:

1. Select **Administration | Export/Import | Export**.

   The File Download message appears.

2. Click **Save** and choose the location to save this file.

To import policies, rules, and conditions from an exported database file:

1. Select **Administration | Export/Import | Import**.

   The Import window is displayed.

2. Select the exported database file, as follows:

   a. In the tree pane, right-click the **Database Files** (root) entry, and choose **Import Policies**. Alternatively, you can click the 🗎 icon to the left of the **Database Files** entry.

   b. In the Import Policy screen, click **Browse** and select the file to be imported.

   c. Click **Import**. The nodes for import appear in the **Import Policies** tree.

3. Select and import the policy as follows:

   a. Expand the tree pane, and right-click the policy that you want to import and choose Import.

   The policy import window is displayed.

   b. 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.

c. For individual conditions that are displayed in the Conditions table, select the desired actions where the same actions available for the policy in Step b are available for conditions.

d. If you chose to rename conditions, specify their new names in the **New Component Name** column.

e. Click **OK**.

After importing any policy, be sure to check that it reflects the new licensed engine.

4. If you are ready to distribute and implement the changes in your system devices, click .

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, right-click the condition that you want to import and choose **Import**.

   The component 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 ⚡.

When importing a Condition from one Policy Server to another, if one of the components in the Condition does not exist on the target Policy Server, an error message is displayed. Depending on the cause, solve the problems as follows:

- If Trustwave added a new component to a Trustwave predefined list, make sure that you have the latest Security Update Version installed on the target Policy Server, and repeat the Import process.

If a customer-defined list has an added component, save the list in the source Policy Server under a different name.

PART 6: Performing Advanced Configuration

This part contains the following chapters and procedures:

- Chapter 17: Defining Administrators

- Chapter 18: Performing Additional Configuration Tasks

- Chapter 20: Implementing Cloud Security

- Chapter 19: Enabling HTTPS Scanning

- Chapter 21: Implementing ICAP

17 Defining 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.

At least one administrator must be designated as a Super Administrator. A Super Administrator is authenticated locally in the system even when RADIUS authentication is enabled, and has maximum allowable permissions. Super Administrators must belong to a predefined Super Administrators group.

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.

This chapter contains the following sections:

- Creating/Editing an Administrator Group

- Creating/Editing an Administrator

- Setting Access Permissions

- Configuring RADIUS Server Authentication

17.1 Creating/Editing an Administrator Group

To create or edit an Administrator Group:

1. Select **Administration | Administrators**.

2. Do either of the following:

    - To create an Administrator Group: In the tree pane, select the **Default Permissions** (root) node, and click the ![plus] icon. Alternatively, you can right-click the **Default Permissions** node, and choose **Add Administrator Group**. The Administrator Group Details screen is displayed.

    - To edit an existing Administrator Group: In the tree pane, select the group, and then, in the Administrator Group Details screen, click **Edit**.

    The Administrator Group Details screen has three tabs. The current tab is **General**.

3. Specify a **Group Name**, and optionally add any useful notes about this group that you want.

4. Select the appropriate check boxes for any desired password requirements and for expiration, set the number of days.

Note that enforcing a secure password means that the password will have to satisfy at least 3 of the following criteria:

- contains at least one uppercase alphabetic character (A-Z)

- contains at least one lowercase alphabetic character (a-z)

- contains at least one numeric character (0-9)

- contains at least one of the following characters !@#$%^&*( )

5. Edit the **Permissions Definitions**. For instructions, see Setting Access Permissions.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ![icon].

17.2 Creating/Editing an Administrator

To create or edit an administrator:

If you plan to assign privileges higher than **View Only** to a new administrator who will be authenticated by a RADIUS server, it is recommended that you manually create that administrator in the appropriate Administrator group prior to the administrator's first login.

1. Select **Administration | Administrators**.

2. Do either of the following:

- To create an Administrator: In the tree pane, select the Administrator Group to which the Administrator should be added, and click the ![icon] icon. Alternatively, you can right-click the administrator group, and choose **Add Administrator**. The New Administrator definition screen is displayed.

- To edit an existing Administrator definition: In the tree pane, select the administrator, and then, in the administrator's definition screen, click **Edit**.

The Administrator definition screen has three tabs. The current tab is **General**.

3. Specify a name for the Administrator.

4. Fill in or edit any desired General details of this administrator. Note the following:

- Regarding Master Policy: You should not change the Use Default Settings value unless you have a Master Policy assigned to the site and you want the administrator to use a different policy.

- For new administrators, except RADIUS administrators, you must assign and confirm a password.

- For RADIUS administrators, the **Password** field has no meaning. The field becomes a protected field so that you cannot enter a value once the RADIUS server is activated, as instructed in Step 4 in Configuring RADIUS Server Authentication.

5. Edit the Permissions Definitions. For instructions, see Setting Access Permissions.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

17.3 Setting Access Permissions

You can assign access permissions using either the Categories View tab or the Grid View tab. The procedure is the same for both Administrator Group definitions and Administrator definitions.

*   Assigning permissions using the Categories View tab:

*   Assigning permissions using the Grid View tab:

Assigning permissions using the Categories View tab:

> 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.

1. If the Administration Group or Administrator definition screen is not displayed:

    a. Select **Administration | Administrators**.

    b. In the tree pane, select the Administrator or Group for which you want to define access permissions.

    c. In the main window, click **Edit**.

2. Select the **Permissions - Categories View** tab.

3. In the **Category** drop down list, select the appropriate category.

4. In the **Sub-category** drop down list, select the appropriate sub-category.

    Depending on the selection, beneath the Category/Subcategory fields, the screen displays either:

    *   a table of object types/objects, or

    *   a set of two radio-button options. The first option keeps the default permissions; the second option lets you change the permissions.

5. If the set of radio button options is displayed, to change the permissions, select the second radio button and choose the desired permission.

6. If the a table of object types/objects is displayed:

    a. Adjust the permissions for any object types as necessary by selecting the needed permission in the drop down list to the right of the object type. Note that when **Default** is selected permission in the drop down list, the column its right displays what the default value translates to (for example, **= update**).

    b. If the object type has a icon next to it, click the icon to display the objects under it.

    c.   To assign an object a different permission than its object type, select the **Override** check box, and select the permission.

7.   Repeat as necessary.

> To allow Administrator Groups to view Web Logs for users belonging to other Administrator Groups, click **Override** and set **View** Access permission to the groups that should be granted permission, under Category: **Logs and Reports**, Sub Category: **Web Log Admin Group / Objects created by Other Groups**.

8.   Click **Save**.

9.   If you are ready to distribute and implement the changes in your system devices, click ⚠.

Assigning permissions using the Grid View tab:

> 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.

1.   If the Administration Group or Administrator definition screen is not displayed:

    a.   Select **Administration | Administrators**.

    b.   In the tree pane, select the Administrator or Group for which you want to define access permissions.

    c.   In the main window, click **Edit**.

2.   Select the **Permissions - Grid View** tab.

3.   Scroll to the desired class. If the Class has a ⊞ icon next to it, click the icon to display the details under it.

    The **Default** column displays the what the default permission value is at each data level.

4.   Where necessary, adjust the permission value, beginning with the highest data level, and then moving down data levels, by selecting the desired level in the **Access** column.

5.   Repeat as necessary.

> To allow Administrator Groups to view Web Logs for users belonging to other Administrator Groups, set **View Access** permission to those groups that should be granted permission, under the Class: **Web Log Admin Group** / Sub Class: **Others**.

6.   Click **Save**.

7.   If you are ready to distribute and implement the changes in your system devices, click ⚠.

17.4 Configuring RADIUS Server Authentication

You configure RADIUS Server Authentication on the Policy Server.

> To ensure that the process runs efficiently, it is highly recommended that your SWG use NTP synchronization. For more information refer to *Limited Shell command* in the *SWG Setup Guide*.

To configure the RADIUS Server connection and authentication

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device configuration tree, select **Management Devices Group** | *<device_ip>* | **Policy Server | RADIUS Authentication**.

3. In the RADIUS Authentication window, click **Edit**.

4. Select the **Active** check box.

5. According to your RADIUS server configuration, select the **Authentication Method** from the drop down menu.

6. In the **Primary Authentication Host** field, enter the host name, which is the server name or IP.

7. In the accompanying **Port** field, enter the RADIUS authentication port. This is the port on which the servers will communicate.

8. Optionally, enter Secondary Authentication host and port values.

9. In the **Shared Secret** field, enter a password to define a shared string to authenticate the client and the server.

10. Select a number from the **Retry Limit** drop down menu. For example, retry limit is 6 times.

11. Select a number from the **Retry Interval** drop down menu to define the interval, in seconds, between each attempt.

> If your browser, specifically in IE6, freezes during login, you should try solving the problem by reducing the number of seconds set in the **Retry Interval** field.

12. Click **Save**.

13. If you are ready to distribute and implement the changes in your system devices, click .

18 Performing Additional Configuration Tasks

This chapter includes the following configuration tasks and procedures:

- Adjusting Network Settings For a Device

- Configuring A Device To Use An NTP Server

- Configuring Administrative Settings

- Importing Digital Certificates

- Configuring Backup Settings

- Configuring Automatic Update Handling

- Defining and Customizing Device Logging Policy

    - Defining a Device Logging Policy

    - Defining a Rule in a Device Logging PolicyIf you are ready to distribute and implement the changes in your system devices, click .

- Configuring Default and Device-Specific Access Lists

- Configuring Transparent Proxy Mode

- If you are ready to distribute and implement the changes in your system devices, click .

- Scheduling Configuration And Security Updates for Scanning Server Device Groups

- Implementing High Availability

- Modifying LDAP Directory Advanced Settings

18.1 Adjusting Network Settings For a Device

This procedure explains how to use the **config_network** Limited Shell command to modify a device's network settings, such as IP addresses, routing information, DNS parameters.

> Once you have completed device setup in the Limited Shell, you should **NOT** use the `setup` Limited Shell command to make changes. Instead, you should use the `config_network` command, as instructed in this procedure.

To adjust network settings for a device:

1. Log in to the Limited Shell. You can connect using either SSH client, serial cable, connecting keyboard and monitor or, in case of VM, vSphere client.

   The Limited Shell works by prompting you to enter a value, often in response to displayed information. For example, it might display a numbered list and ask you enter the number of the item you want to choose; or it might request that you enter specific information.

2. At the prompt, enter the **config_network** command.

   The current network configuration is displayed. The following data is displayed:

   - interfaces, and the status **Enabled** or **Disabled** of each.

   - DNS cache status, DNS Search Domain, nameserver. A nameserver is a network server that provides a naming or directory service, and Hostname configuration.

   A prompt is asks if you would like to change the configuration.

3. Enter **y** to change the network configuration.

   The Limited Shell then displays several numbered options. The following table lists these options, and describes the edits that each option allows you to perform.

<p align="center">Table 1: Main options of config_network</p>

Option	Edits you can perform from this option:
1. View	none
2. Interface	Choose a particular interface, and then: • Change, Add, or Remove its IP Address • Add, Remove, or change its route. Format: *<ip_address>*/ [*<netmask>*|*<prefix>*] **via** *<prefix_ip>*. For example: 1.1.1.1/32 via 10.0.3. • Enable or Disable it.
3. Gateway	Set/change the default gateway IP address. Format: *<ip_address>*/ [*<netmask>*|*<prefix>*]. For example, 192.168.120.32/24. **Note:** A default gateway is mandatory, and its IP address must be a local IP address.
4. DNS	• Change DNS search domains • Add, or Remove DNS server. **Note:** There must be a DNS Server that has the ability to resolve external IP addresses.
5. Hostname	Configuring the device's hostname.
6. Hosts	Configuring the device's host file.

4. Depending on the action that you want to perform:

   a. Enter the number of the main configure_network option.

   b. At each successive prompt, enter the expected information, for example, item number or specific value.

   c. To move back to the previous prompt, press **Enter**. This will enable you to perform additional actions before leaving the Limited Shell.

5. When you are done, enter **q** to quit the Limited Shell.

18.2 Configuring A Device To Use An NTP Server

This procedure explains how to use the Limited Shell to configure the device to use an NTP server.

To configure a device to use an NTP Server:

1. Log in to the Limited Shell. You can connect using either SSH client, serial cable, connecting keyboard and monitor or, in case of VM, vSphere client.

2. Enter the **config_time** command.

   A prompt is displayed asking you if you would like to change the time configuration.

3. Enter **y** to change the time configuration. The screen displays a number of Time and Date configuration options.

4. Enter **3**, the option for NTP server.

5. At the prompt to type in the NTP server, type in the URL of the NTP server that you want to use, and press **Enter**. A message confirms that the NTP Server is configured to the specified URL.

   > If you wish, before exiting, you can make other changes to the Date and Time and/or Time Zone if needed, by entering the option number and then providing the details at the prompts.

6. Enter **q** to exit.

The device is configured to use the specified NTP server.

18.3 Configuring Administrative Settings

This procedure explains how the administrator can:

• Set the amount of idle time, in minutes, after which the current session times out and requires the user to re-log in.

• Force the administrator to provide a relevant comment to be sent to the Audit log whenever a configuration change is committed.

• Enable the automatic sending of blocked transaction and browsing habit data to the Trustwave Labs Malware team, according to a specified schedule.

• Determine which icons to show in the Management Console toolbar.

To configure Administrative Settings:

1. Select **Administration | System Settings | Administrative Settings**.

2. Click **Edit**.

3. In the Administrative Settings screen, ensure the **General** tab is displayed.

4. In the **Console Timeout** field, set the number of idle minutes that will result in the current session timing out.

5. If the administrator should be required to provide a relevant comment for the Audit Log whenever a configuration change is committed, select the **Mandatory Audit log note on commit changes** check box.

6. To enable the sending of customer feedback information, mainly blocked transaction and browse habit data, to the Trustwave Labs Malware team:

    a. Select the **Enable sending customer feedback information** check box.

    > This check box is also available in the License agreement screen.

    b. Set the schedule either a Daily time, or a weekly day and time, for the information to be forwarded.

7. To set which icons are displayed in the Management Console toolbar:

    a. Display the **Toolbar** tab.

    b. In the Toolbar Icon list, ensure that only the icons that should be displayed are selected.

8. Click **Save**.

9. If you are ready to distribute and implement the changes in your system devices, click .

18.4 Importing Digital Certificates

This section explains how to import digital certificates, how to edit their details, and how to check to what rules and policies the certificates are applied.

The Trustwave Certificate Store is used to maintain import digital certificates. Managing the Trustwave Certificate Store includes adding root CAs, adding Certificate Revocation Lists (CRL) adding untrusted CA and then apply them to specified rules.

To import and edit a digital certificate:

1. Select **Administration | System Settings | Digital Certificates**.

2. In the tree pane, right-click on the Digital Certificate, and select **Import Certificate** in the drop down menu. The Import Digital Certificate screen is displayed in the main window.

3. Browse to the required file location and then **Import** the file, making sure that the file has the correct PEM extension. The imported certificate appears in the Digital Certificate list.

4. To edit the details, click **Edit**, make the needed changes. Note the following about the details in the screen:

    • For root certification authorities or self-signed certificates, the **Issued By** and **Issued To** names are the same.

- **Friendly name** is the name of the certificate presented externally.

- The fields displayed for certificate revocation lists, **Customer Certificate Revocation List** and **Trustwave Certificate Revocation List**, differ from those displayed for certificate lists. For more information, see the Management Console Reference Guide.

5. Click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click ![icon].

18.5 Configuring Backup Settings

Two kinds of backups can be configured and run:

- **System backups** — these backups save, to an external location, all data that an administrator can customize in the Management Console including Policies, settings etc. System backups do not include information in the Log Server database, Report Server database and Updates.

- **Reports DB backups** — these backups save, to an external location, data in the Reports database.

As part of configuration, you can enable automatic backup. Once backup is configured, you can also run backups manually as the need arises (for example, before applying updates, or before performing major configuration or setting changes to your system).

To configure backup settings:

1. Do either of the following:

   - To configure System Backup, select **Administration | Rollback | Rollback Settings**.

   - To configure Reports DB Backup, select **Administration | Reports DB Backup | Backup Settings**.

2. In the main window, click **Edit**.

3. In the **Connection Method** field, select the method that SWG should use to connect to the Backup file storage location:

   - **FTP** — connect using regular File Transfer Protocol.

   - **FTP Passive** — connect using File Transfer Protocol where 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. This is available for System backups only.

4. Specify the Backup file location, User name and Password. The format of these values depends on the connection mode:

5. **For Reports DB backup only:** To enable the Reports DB to be automatically backed up according to a predefined SWG schedule, select the **Enable Automatic Backup** check box.

Table 2:

Connection Method	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.

6. **For System backup only:** To enable automatic scheduling and configure the schedule as follows:

7. Select the **Enable Scheduling** check box.

8. Set the interval in days between successive backups.

9. Set the time of day that the backup should be started.

10. To check the connection to the specified location, select the **Check connection** check box. The connection to the location will be verified after you Save the definition.

11. Click **Save**.

12. If you are ready to distribute and implement the changes in your system devices, click .

18.6 Configuring Automatic Update Handling

Using the Updates Configuration window, you can define:

• When and how often the updates should be downloaded

• Which types of updates should be automatically installed

Note that if the Internet connection is blocked for the SWG appliance, you can still receive updates by routing them through a proxy.

To configure automatic Update Handling:

1. Select **Administration | Updates | Updates Configuration**.

2. Click **Edit**.

3. To automatically install any of the following types of updates Security, Critical OS Update, OS Version Update, select the accompanying check boxes.

4. To route the update information through a proxy, useful if SWG is blocked from Internet connections, fill in the following details about the Next Proxy Server, in the **Proxy Configuration** area:

   • IP of the next proxy server

   • Port of the next proxy server

   • User Name and Password required to access that proxy server

5. To enable and schedule the download of updates, fill in the following details in the **Retrieve Updates Automatically** area:

   a. Select the **Retrieve Updates Automatically** check box.

   b. Specify the S**tart Date** and **Start Time** of the download.

   c. In the **Download Every** fields, specify the frequency in days, hours, and minutes, that download of updates should be performed.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

18.7 Defining and Customizing Device Logging Policy

Device Logging policy determines, at the device level, what types of transactions carried out by the Identification and Upstream Proxy Policies will be logged.

Trustwave provides a single, predefined Device Logging Policy having several rules.

You can set different device logging policies for different devices.

This task consists of the following procedures:

• Defining a Device Logging Policy

• Defining a Rule in a Device Logging PolicyIf you are ready to distribute and implement the changes in your system devices, click .

18.7.1 Defining a Device Logging Policy

> You cannot edit a pre-supplied Device Logging Policy. However, you can duplicate such a policy and edit the duplicate; you can also create a Device Logging policy from scratch.

To define a Device Logging Policy:

1. Select **Policies | Device Logging**.

2. Do one of the following:

   - To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

   - To duplicate a Device Logging policy, right-click the policy in the tree that you want to duplicate, and choose **Duplicate Policy**.

   - To edit a Device Logging policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

   The Policy Definition is displayed in the main window.

3. Enter a name for the policy.

4. (Optional) Add or modify the policy description.

5. When done, click **Save**.

6. Continue with Defining a Rule in a Device Logging Policy.

18.7.2 Defining a Rule in a Device Logging Policy

If you duplicated a policy, it already has the same rules as were found in the original policy. You can edit these rules or create new rules from scratch.

> Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant.
>
> For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

To define a rule in a Device Logging policy

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining a Device Logging Policy.

2. Do any of the following:

   - To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

   - To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

   - To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**.

The main window displays the Rule Definition screen.

3. Enter a name for the rule.

4. (Optional) Provide a description of the rule.

5. If the rule has an **Enable Rule** check box, ensure that the check box is appropriately selected or cleared, depending on whether or not the rule should be enabled after being committed.

6. In the **Send To** area, check the locations to which the device logging data should be sent.

7. Click **Save**.

8. To make triggering of the rule conditional, continue with To define conditions in a Device Logging Rule:If you are ready to distribute and implement the changes in your system devices, click ..

9. To define additional rules in this policy, repeat this procedure.

10. If you are ready to distribute and implement the changes in your system devices, click ![icon].

To define conditions in a Device Logging Rule:

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define a Device Logging Policy:.

2. Do either of the following:

   - To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

   - To add a new condition to a rule:

   a. Right-click the rule and choose **Add Condition**.

   The main window displays the Condition Definition screen.

   b. In the **Condition Name field**, select the type of condition in the drop down list.

   For any selected condition type, the window displays an appropriate check box list.

   For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

3. If the window displays an **Applies To** area above the list, select whether the condition will apply to the items you check or to the items you do not check.

4. Select the appropriate check boxes in the list. If the window displays a **Select/Deselect All** check box, you can use this if it will be useful.

5. If the condition has any other special fields or requirements to fill in, fill them in appropriately.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ![icon].

18.8 Configuring Default and Device-Specific Access Lists

The Access List feature enables you to limit access to an SWG device. The following Access List definitions provides three access limitation options:

- **Management Access List** — Used to specify 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 enabled, that is, 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 to control 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 to control which device IPs have access to the SWG system.

It is recommended that you use the procedure to modify default settings, and after adding devices, to configure settings for specific devices.

To limit IP access by defining Access Lists:

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device tree that is displayed in the left pane, do either of the following:

   - To define or alter the default Access Lists, select **Devices | Default Values | Device General Settings | Access Lists**. Values you define here will apply to all new devices that you create. You can then modify the values for specific devices, as described in the next bullet.

   - To define different Access Lists, that is, to override default Scanning Server values defined in the previous bullet for a particular device, select *<device_ip>*, and then in the main window, click the **Access List** tab. This is relevant only if you added additional devices. For instructions on adding additional devices, see Adding Devices and Device Groups.

3. Click **Edit**.

4. Select the **Use Access List** check box.

5. In the appropriate area, depending on whether you are defining IP Access Lists for Management, Users, and/or Trustwave SWG system ports, do the following:

   a. Click the ![plus icon] icon.

   b. Fill in the IP range **From IP** and **To IP**.

   c. Repeat for each IP range.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click ![distribute icon].

18.9 Configuring Transparent Proxy Mode

By default, Explicit Proxy Mode is used. However, to enable FTP, HTTPS, and HTTP requests to be intercepted, you should enable and configure Transparent Proxy Mode. Working in transparent mode requires a network environment that can support transparent mode, for example an external switch/router redirects the traffic to SWG or setting SWG in bridge mode or as a default gateway.

To configure Transparent Proxy Mode

1. Select **Administration** | S**ystem Settings** | **Trustwave Devices**.

2. In the Device configuration tree, do either of the following:

   - To configure Default settings, select **Devices | Default Values** | **Device Settings** | **General**. Values you define here will apply to all new devices that you create.

   - To configure the settings for a specific Scanning Server, select *<device_group>* | *<device_ip>* | **Scanning Server** | **General**.

3. In the main window, click **Edit**.

4. Select the **Transparent Proxy Mode** tab.

5. Select the **Enable Transparent Proxy Mode** check box.

   > Selecting **Enable Transparent Proxy Mode** sets, or changes, the Authentication Retention Method to IP Caching, which authenticates only the first transaction from the IP address and treats the remaining transactions from that address as already authenticated. For more information, see Configuring Default and Scanning Server Authentication.

6. Specify the FTP, HTTPS, and HTTP ports ranges. Note the following points:

   - To add a new port or range, click the ![plus] icon.

   - For HTTPS, if the hostname should be extracted from the certificate, select the check box at the bottom of the HTTPS port range area.

7. To ensure the blocking of services that were not enabled, that is, services whose **Enable** *<service>* check box is not selected in modules under the Scanning server, click the **Block Disabled Services** check box.

8. Click **Save**.

9. If you are ready to distribute and implement the changes in your system devices, click ![icon].

18.10 Scheduling Configuration And Security Updates for Scanning Server Device Groups

You can define schedules to apply configuration and security updates to the devices in Scanning Server Device Groups.

> The schedules that you define go according to the time of the Policy Server, not the local client time.

To define configuration and security update schedules for the devices in a Scanning Server Device Group:

1. Select **Administration** | **System Settings** | **Trustwave Devices**.

2. In the Device tree that is displayed in the left pane, select a Scanning server devices group, **Default Devices Group** or a user-defined Devices Group.

3. In the main window, click **Edit**.

4. In the **Commit Scheduling** tab, define the schedule by which configuration changes will be committed and applied to the devices in the group.

   You can choose between:

   • Immediately upon commit.

   • Specific interval in number of days, at a specified time.

   • Specific days of the week at a specified time.

   • Specific day of the month at a specified time.

5. In the **Update Scheduling** tab, define the schedule by which security updates will be committed and applied to the devices in the group.

   You can choose between:

   • Immediate upon commit.

   • At a specified time. In this case, you also specify the window of opportunity in minutes by which the update must begin; if the update does not begin within that time, it will be attempted again the next day.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

18.11 Implementing High Availability

You can implement Policy Server High Availability by dedicating an additional device as a secondary Passive Policy Server.

Implementation of High Availability requires that:

- Your Active primary and secondary Policy Server be on its own device, NOT on an All-In-one device.

- The device that will house the secondary Passive Policy Server is accessible and that you know its IP address.

To be able to use a virtual IP address which will automatically route to the Active Policy Server see Step 5, both Policy Servers must be on the same network.

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 the change using the Limited Shell command **failover**. For more information on Limited Shell commands, see the *Management Console Reference Guide*.

To implement High Availability

1. Select **Administration | System Settings | Trustwave Devices**.

2. In the Device tree that is displayed in the left pane, right-click the **Management Devices Group** node and choose **Add HA Device**.

3. In the main window, fill in the mandatory Device IP, and optionally fill in a description. Note that the device type is automatically set to Passive Policy Server.

4. Click **Save**.

5. Optionally, specify a virtual device IP, which will automatically route to whichever Policy Server is active at any given time, as follows:

   a. In the tree pane, select **Management Devices Group**.

   b. In the main window, specify a virtual Device IP and click **Save**.

6. To complete implementation of High Availability, including synchronization of the database and configuration files, click .

The Management Console GUI does not work on the Passive Policy server device.

18.12 Modifying LDAP Directory Advanced Settings

To modify Advanced LDAP settings:

1. Select **Users** | **Authentication Directories |** LDAP.

2. In the tree, under the type of LDAP server, select the LDAP directory.

3. In the LDAP Directory definition screen, display the **Advanced** tab.

4. In the User Identifier Attribute field, specify the attribute that is used to indicate a user's unique identifier. The value of this attribute will be compared to the user name provided by the proxy authentication.

   If left blank, users will be identified by their DNs.

5. In the **Email Attribut**e, specify the attribute that is used to indicate a user's email.

6. In the **User Object Filter** field, define in LDAP query syntax the filter that can be optionally used to identify user objects.

7. In the **Group Identifier Attribute** field, specify the attribute that is used to indicate a group's unique identifier. The Management Console will use the value of this attribute when displaying group names and assigning policies.

   If left blank, users will be identified by their DNs.

8. In the **Group Object Filters** field, define in LDAP query syntax the filter that will be used to identify group objects.

9. In the **Connection Timeout** field, set the maximum number of seconds for an unanswered LDAP query, after which, users will not be imported. If set to 0, it will use the system default, which is 120 seconds.

10. In the **Group User Hierarchy Method** area, select how the group-user relationship is implemented in the LDAP directory. The attribute types are follows:

    • **memberOf Attribute** — Means that each user has zero or more memberOf attributes, each specifying a group to which the user belongs.

    • **member Attribute** — Means that each group has zero or more 'member' attributes, each specifying a user, or a group, belonging to this group.

11. If **Custom** directory type is used and **member Attribute** is used as the hierarchy method, there is an additional check box **Use "User Identifier" attribute value for group-user relationship**. Usually the **member attribute**s hold member DNs as a reference. In some LDAP directories, instead of holding the DN, they hold the value designated by the 'User Identifier' attribute. Selecting this check box enables handling such configurations.

12. To not check the connection to the server, select the **Do not check configuration settings on next save** check box at the bottom of the window.

13. When done, click **Save**.

14. If you already have some LDAP groups/users imported into the system and you have changed some of the above values except for Connection Timeout:

   a. Remove all LDAP groups that were already imported into the system.

   b. Right-click the LDAP directory node in the tree and select **Add Groups**.

   c. After the right pane page is displayed click **Import LDAP Groups**. The group LDAP list is displayed.

   d. From LDAP list select the LDAP groups.

   e. Import all LDAP users again.

15. After all the LDAP users are imported, and you are ready to distribute and implement the changes in your system devices, click .

19 Enabling HTTPS Scanning

If your site will be using HTTPS scanning, you must perform the following tasks:

- Defining an HTTPS Policy

  - Defining a Rule in an HTTPS Policy

  - Defining Conditions in an HTTPS Rule

- Configuring and Certifying HTTPS

HTTPS must be licensed at your site in order for you to enable HTTPS scanning.

19.1 Defining an HTTPS Policy

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

You can customize both a regular HTTPS policy and an HTTPS Emergency policy.

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

To define an HTTPS Policy:

1. Select **Policies | HTTPS**.

2. Do one of the following:

   - To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

   - To duplicate an HTTPS policy, right-click the policy in the tree that you want to duplicate, and choose **Duplicate Policy**.

   - To edit an HTTPS policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

   The Policy Definition is displayed in the main window.

3. Enter a name for the policy.

4. (Optional) Add or modify the policy description.

5. When done, click **Save**.

6. Continue with Defining a Rule in an HTTPS Policy.

19.1.1 Defining a Rule in an HTTPS Policy

If you duplicated a policy, it already has the same rules as were found in the original policy. You can edit these rules or create new rules from scratch.

You can specify if the rule should be applied to specific users and/or if specific users should be excluded. One method is by specifying User Lists to which the rule should or should not apply.

> If you will be using User Lists to identify users to which the rule should or should not apply, be sure to define those lists. For instructions, see Defining User Lists.

To define a rule in an HTTPS policy:

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining an HTTPS Policy.

2. Do any of the following:

> Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant. If no rules fire, the default action is to Inspect Content. For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

- To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

- To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

- To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**.

The main window displays the Rule Definition screen. The screen contains three tabs: **General**, **Applies**, and **Except**.

3. Fill in the **General** tab as follows.

   a. Enter a name for the rule.

   b. (Optional) Provide a description of the rule.

   c. If the rule has an **Enable Rule** check box, ensure that the check box is appropriately selected or cleared depending on whether or not the rule should be enabled after being committed.

   d. Choose the Rule Action, as follows, which depending on your selection, the fields in the rest of the rule display vary:
   - To block HTTPS sites, choose **Block HTTPS**.
   - If user approval is required to decrypt traffic for this site, choose **User Approval**. This will send an approval page to the end-user for each new HTTPS site that is accessed. If the end-user chooses not to approve the transaction, the connection is closed.
   - If no HTTPS or Security scanning is needed, choose **Bypass**.
     Note: The Bypass rule must be the first rule in the policy.
   - If scanning is needed, choose **Inspect Content**, and scanning will be performed first by HTTPS rules and then by Security rules. This is the default value.

e. If you chose **Block HTTPS** or **User Approval**, select the End User Message from the list.

f. **For Block HTTPS rule action only:** If the blocked page message should not be displayed to the end user, select the **Do Not Display End User Message** check box.

4. To apply the rule to specific users, select the **Applies** tab, and click the radio button for the category of users to which the rule should apply. Note the following:

- **All Users** is the default.

- **All Recognized Users** All users identified by the system.

- **All Unrecognized users** are Unknown users and/or Unassigned LDAP users. For more information, see the Management Console Reference Guide.

- If you chose Select User Lists, select the check boxes of the User Lists that contain the users to which the rule should apply.

5. To exclude specific users from application of the rule, select the **Except** tab, and select the check boxes of the User Lists which contain the users who should be excluded.

6. Click **Save**.

7. To make triggering of the rule conditional, continue with Defining Conditions in an HTTPS Rule.

8. To define additional rules in this policy, repeat this procedure.

9. If you are ready to distribute and implement the changes in your system devices, click .

19.1.2 Defining Conditions in an HTTPS Rule

To define conditions in an HTTPS Rule

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define an HTTPS Policy:.

2. Do either of the following:

- To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

- To add a new condition to a rule:

a. Right-click the rule and choose **Add Condition**.

The main window displays the Condition Definition screen.

b. In the **Condition Name field**, select the type of condition in the drop down list.

For any selected condition type, the window displays an appropriate check box list.

For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

3. If the window displays an **Applies To** area above the list select whether the condition will apply to the items you check or to the items you do not check, or use the **Exception** tab to define exceptions.

4. Select the appropriate check boxes in the list. If the window displays a **Select/Deselect** All check box, you can use this if it will be useful.

5. If the condition has any other special fields or requirements to fill in, fill them in appropriately.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click [icon].

19.2 Configuring and Certifying HTTPS

Before HTTPS policy can be effective, you must:

- ensure that HTTPS is enabled in the HTTPS module, and

- obtain a certificate, and ensure that it is propagated to the scanners and users.

Scanning server devices have an HTTPS module with pre-configured settings. You should also make any desired adjustments to the settings in the HTTPS module.

It is recommended that you perform these HTTPS-related tasks for Device Default settings, and then propagate them to the HTTP modules in all Scanning servers

This section contains the following procedures:

- To configure device HTTPS settings

- To obtain and propagate an HTTPS certificates

To configure device HTTPS settings

1. Select **Administration** | S**ystem Settings** | **Trustwave Devices**.

2. Choose **Devices | Default Values | Device Settings | HTTPS**. To alter settings for a specific device, choose *<device_group>* **|** *<device_ip>* **| Scanning Server | HTTPS**.

3. In the main window, click **Edit**.

4. Select the **Enable HTTPS** check box.

5. If needed, modify the **Listening Port** value in the **HTTPS Service** tab.

6. If other configuration adjustments are needed in any of the tabs, perform them. For information on the fields in each tab, see the *Management Console Reference Guide*.

7. Click **Save**.

8. Continue with the procedure To obtain and propagate an HTTPS certificates.

To obtain and propagate an HTTPS certificates

1. If the device tree is not displayed, select **Administration** | **System Settings** | **Trustwave Devices**.

2. Depending on how you plan to obtain the needed certificate, do one of the following:

   - To use an Trustwave-generated certificate, do the following:

a. Right-click **Devices | Default Values | Device Settings | HTTPS** and choose **Generate Certificate**.

b. In the **Type** field, select **Self Signed. Self Signed** is the default.

c. In the **Common Name** field, specify a name for the CA. The name is **mandatory**.

d. In the remaining fields, fill in all relevant data as needed.

e. Click **OK**. Then continue with Step 3.

• To obtain a certificate by issuing a Certificate Signing Request (CSR) to an external CA, and then importing the certificate generated by the CA, do the following:

a. Right-click **Devices | Default Values | Device Settings | HTTPS** and choose **Generate Certificate**.

b. In the **Type** field, select **CSR**.

c. In the **Common Name** field, specify a name for the CA. The name is mandatory.

d. In the remaining fields, fill in all relevant data as needed.

e. Click **OK**.

f. Copy the entire certificate request, including the **BEGIN ...** and **END ...** lines, and provide them to the CA.

g. When the CA provides the certificate, copy the certificate details.

h. Right-click **Devices | Default Values | Device Settings | HTTPS** and choose **Import Certificate**.

i. In the **Certificate Type** field, select **CSR**.

j. In the **Certificate** field, paste the Certificate details.

k. Click **OK**. Then continue with Step 3.

• To import a Root CA certificate from an external CA without issuing a CSR, do the following:

a. Right-click **Devices | Default Values | Device Settings | HTTPS** and choose **Import Certificate**.

b. In the **Certificate Type** field, select **Root CA** The Root CA is the default.

c. In the **Certificate** field, paste the Certificate Public key.

d. In the **Private Key** field, paste the Private Key.

e. Fill in the **Password**.

f. Click **OK**. Then continue with Step 3.

3. Propagate the certificate and the defaults you set in To configure device HTTPS settings to the HTTPS module on all devices by right-clicking **Devices | Default Values | Device Settings | HTTPS** and choosing **Reset all HTTPS modules with default values**.

> To alter values for specific scanners, choose **<device_group> | <device_ip> | Scanning Server | HTTPS**, and then perform the steps in To configure device HTTPS settings and make the needed adjustments.

4. Export the certificate to a file so that it can be propagated to all users, by right-clicking **Devices | Default Values | Device Settings | HTTPS** and choosing **Export Certificates**. Then perform the export.

5. Ensure that IT propagates the exported certificate to all users.

6. If you are ready to distribute and implement the changes in your system devices, click .

20 Implementing Cloud Security

This chapter is relevant only if implementing a Hybrid SWG deployment.

Hybrid deployment is an SWG feature providing Web security for users when working off-site, for example, when connecting to the internet from hotels, airports, internet cafes, home or even working from remote offices.

An SWG Hybrid deployment combines normal SWG Scanning Servers to protect internal network users, SWG Cloud Scanners to protect roaming/mobile/remote users and Trustwave Mobile Security Client software. The client software directs Web traffic to the appropriate and optimal scanner, on-premise or cloud, depending on the user location and available scanners. The client also provides mutual certificate authentication between the user and the target Cloud Scanner. Multiple Cloud Scanners can be deployed to cover the geographic locations from which users work.

Cloud Scanners are virtualized SWG Scanning Servers configured to support connections only from user computers running the Trustwave Mobile Security Client, or specifically defined proxy servers, for example in remote offices. Cloud Scanners can be run on a number of different platforms and although the platform set-up varies, the Management Console configuration is the same for each server.

Setting up details for the different platforms are as follows:

Table 1: Cloud Scanner Platform Setup Procedures

Cloud Scanner Platform	Type	Setup Procedure
Trustwave Hardware Appliance	Private Cloud	This document
Trustwave Virtual Appliance	Private Cloud	This document
Trustwave Secure-Web Services-Hybrid	Trustwave managed platform	See Hybrid Deployment Guide
Amazon Web Services EC2	Infrastructure as a Service	See Hybrid Deployment Guide

When one or more Cloud Scanners are deployed in a customer's own data centre, or a business partners data centres using the Trustwave Hardware Appliance or Trustwave Virtual Appliance platform types, then this is termed a Private Cloud. Typically a Private Cloud is linked to the customer network by high bandwidth network connections.

For more information on Hybrid deployment scope and planning, see the *SWG Hybrid Deployment Guide*.

For more information on the client software, see the *MSC Administrator Guide*.

20.1 Implementing Cloud Security Outline

This is to be read in conjunction with the overall hybrid deployment process.

Outlining a Hybrid deployment requires the following:

- Deployment decisions

  - Certificate management method PKI Mode or Internal Mode?

  - Number of Cloud Scanners per region?

  - Client types to be used PC and/or Mac?

- Cloud Scanner Platform set-up

  - Private Cloud Scanner set-up

  - Other Cloud Scanner set-up

- SWG Policy Service Configuration

  - Configure Cloud Settings in Internal Mode, or

  - Configure Cloud Settings in PKI Mode

- Client Deployment

- Certification and Management of Hybrid Users

Cloud Scanning Servers can be implemented in either of two modes:

- **Internal Certification Mode** — In this mode, the policy server acts as the Certificate Authority for all certificate management creation and signing.

  In **Internal** mode, you designate which users are cloud users, and manage user 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.

- **Public Key Infrastructure (PKI) Mode** — In this mode, the policy server integrates Cloud configuration with an external Public Key Infrastructure.

  In **PKI** 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.

You can also define a private cloud scanner.

This chapter contains the following procedures:

- Configuring Cloud Settings in Internal Mode

- Configuring Cloud Settings in PKI Mode

- Certifying and Managing Cloud Users

- Defining a Private Cloud Scanner

20.2 Configuring Cloud Settings in Internal Mode

Before configuring cloud settings, ensure that you have:

- *added the needed cloud scanning servers. For instructions, see* Configuring/Adding Scanning Servers.

- c*onfigured the Mail Server. For instructions, see* Configuring the Mail Server.

You can also configure a provisioning Email Template. For more information, see the *Management Console Reference Guide*.

To configure Cloud Settings in Internal Mode:

1. Select **Administration | Cloud | Configuration**.

2. Click **Edit**.

3. If the **Cloud Configuration** title bar does **NOT** end with **(Internal Mode)**, change the mode as follows:

   If you change the Certificate Management mode, your existing Certificate Authority definitions will not be saved.

   a. Click the **Change Certification Management Mode** button.

   b. In the displayed Certification Management Mode window, choose the **Internal Certification** option.

   c. Click **Save**. Then confirm the change.

4. Configure Cloud Proxies in the **Proxies (Cloud)** tab, as follows:

   a. In the **Server Side** area, define the following details:

      i. In the **Cloud Proxy HTTP Port** field, specify the server-side HTTP port number on which <u>all</u> cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.

      ii. In the **Cloud Proxy HTTPS Port** field, specify the server-side HTTPS port number on which <u>all</u> cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.

   b. In the **Client Side** area, do the following:

      Be sure not to confuse the Local Client ports and Listening Server ports.

    i.   In the **Local Control Port** field, specify the port which the client uses to perform "control" activities, such as configuration updates.

It is recommended that you not change the port value from the default unless you use the default for a different application.

    ii.   In the **Client Side** table under the Local Control Port field, for each Cloud Scanner or Load Balancer that the client can use, define the identifying details, as follows:

        1.   Click the ✚ icon.

        2.   In the **Comment** field, specify an internal label for this scanner/load balancer, for example a suggested name could include the scanner type, and/or the scanner location.

        3.   In the **Address** field, specify the IP Address or Hostname of the scanner/load balancer.

        4.   In the **Local Client HTTP Port** field, specify the client-side port number used to uniquely identify a specific cloud proxy or cloud-based load balancer for HTTP.

        5.   In the **Local Client HTTPS Port** field, specify the client-side port number used to uniquely identify a specific cloud proxy or cloud-based load balancer for HTTPS.

5.   Configure On-premise Proxies and On-premise/Off-premise indicators in the **Proxies (On-premise)** tab, as follows:

    a.   In the **On-premise Proxy Details** area, for each explicit proxy server to which roaming users can connect while on premise, configure the details as follows:

        i.   Click the ✚ icon.

        ii.   In the **Address** field, specify the IP or Hostname of the on-premise proxy server.

        iii.   In the **Proxy HTTP Port** field, HTTP port to which roaming users will connect when on-premise.

        iv.   In the **Proxy HTTPS Port** field, HTTPS port to which roaming users will connect when on-premise.

    b.   In the **On-Premise.Off-Premise Indicator** area, do the following:

        i.   In the **Corporate Hostname** field, specify the 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, which is specified in the next sub-step. When the user is outside the corporate network, this name should not be resolvable to the Internal Hostname IP.

        ii.   In the **Internal Hostname IP** field, specify the IP of the corporate hostname, using either of the following methods:

      •   Click the **Resolve IP** button. The application will look up the IP address of the internal hostname and display the results in the Internal Hostname IP field.

- Manually specify the Internal Hostname IP.

Note the following points about the On-Premise Proxy:

- If the **Corporate Hostname** is resolvable, the PAC file will include instructions to use the local, on-premise proxy, since it recognizes you are within the local network.

- If the **Corporate Hostname** is not resolvable, it will use the nearest available Cloud proxy region.

The **On-premise Proxy Details** area can be left empty in a situation where the administrator determines for users which proxy to use.

6. Define the system Certificate Authority in the **CA Management** tab, using one of the following methods:

- Generate a self-signed certificate authority, as follows:

  i. Click the **Generate Self Signed CA** button. The window displays fields for defining the Certificate Authority.

  ii. In the **Common Name** field, specify a name for the CA. It is mandatory to specify a CA name.

  iii. Optionally, fill in relevant data in the other fields.

  iv. Click **OK**.

- Import a CSR-based CA as follows:

  i. Click the **Generate CSR** link that is under the **Import CSR-based CA** button. The window displays fields for defining the Certificate Authority.

  ii. In the **Common Name** field, specify a name for the CA. It is mandatory to specify a CA name.

  iii. Optionally, fill in relevant data in the other fields.

  iv. Click **OK**. A CA Certificate request is generated and displayed.

  v. Copy the Certificate request to provide to the trusted CA for signing.

  vi. Click **OK**.

  vii. Have the trusted CA sign the Certificate Request.

  viii. Click the **Import CSR-based CA** button.

  ix. In the displayed **Certificate** field, paste the signed Certificate and click **OK**.

- To import a CA

  i. Click the **Import CA** button.

  ii. Paste the certificate information into the appropriate entry fields in the window. Then click **OK**.

Regardless of the method you chose to define the system CA, the **CA Management** tab is re-displayed, and all information provided is displayed in the appropriate column and fields.

7. According to need, define **Non-Routable Network Bypass** and **Trusted URL Bypass** settings in the **Bypass** tab, as follows.

    a. For each network or domain to be bypassed while the Mobile Security Client agent is browsing in Cloud proxy or local proxy, add it to the bypass list, as follows:

        i. Click the ![icon] icon.

        ii. In the opened detail line, specify the Network IP and Network Mask.

        iii. To delete a network bypass, right-click the ![icon] icon and choose **Delete Row**.

    b. To enable security to bypass the URLs appearing in a particular type of URL list (for example, Customer Defined White List), select the URL type in the **Trusted URL's** drop down list.

8. Set Client Configuration in the **Client Configuration** tab, as follows:

    a. By default, users can only browse using an Trustwave agent and PAC file. To eliminate either or both of these restrictions, do the following:

        i. To allow the user to disable the client and browse using a non-Trustwave client, clear the **Prevent user from disabling client** check box.

    ![warning icon] Disabling the Mobile Security Client agent might contravene your site's Acceptable Use Policy. Therefore, consider carefully before clearing this check box, which gives users the ability to disable the agent. This can also be done as a group configuration affecting all clients in the group. For more information see Defining and Assigning Policies to User-Defined User Groups.

        ii. If a proprietary PAC file is used, clear the **Enforce PAC file usage via the Mobile Security Client** check box.

    b. To ensure that a warning is issued if a user tries to uninstall the client, ensure that the **Enable Client Uninstall Warning Text** check box is selected, and if desired, edit the message text in the accompanying text box.

9. Configure Provisioning parameters, and perform downloads, in the **Provisioning** tab, as follows:

    a. In the **Agent Installer URL** field specify the address chosen by the administrator where the Agent Installation Package is saved.

    b. If the Policy Server should automatically send emails with needed enabling instructions to new cloud users, select the **Automatically send an email with provision instructions to new cloud members** check box.

    c. If the Policy Server should automatically send emails to existing cloud users notifying them that configuration changes have been committed, select the **Send an email update upon configuration changes** check box.

d. In the **Mobile User Private Key Password** field, specify the password that the end user will use when installing the certificate. Specifying the password is mandatory.

e. Confirm the password.

f. Click **Save**.

g. Click .

h. Download the appropriate Agent Installer, for Windows or Mac, so that you can later distribute it for installation.

i. If you cleared the **Enforce PAC file usage via the Mobile security Client** check box in the **Client Configuration** tab, you can optionally download and modify the PAC file for later distribution.

Before you can download these files, you must ensure that you have saved and committed the mandatory information in the other tabs. Download buttons in the Provisioning tab are disabled until all mandatory information in the other tabs is saved and successfully committed. Warning icons and/or yellow field backgrounds in the other tabs indicate which fields are mandatory.

If you are using a third-party PAC file, ensure that the Enforce PAC file usage via the Mobile Security Client check box in the Client Configuration tab is cleared, and that the local host proxy within the PAC file belongs to Trustwave.

20.3 Configuring Cloud Settings in PKI Mode

Before configuring cloud settings, ensure that you have added the needed cloud scanning servers. For instructions, see Configuring/Adding Scanning Servers.

To configure Cloud Settings in PKI Mode:

1. Select **Administration | Cloud | Configuration**.

2. Click **Edit**.

3. If the **Cloud Configuration** title bar does NOT end with **(PKI Mode)**, change the mode as follows:

If you change the Certificate Management mode, your previous Certificate Authority definitions will not be saved.

a. Click the **Change Certification Management Mode** button.

b. In the displayed Certification Management Mode window, choose the **Enterprise PKI** option.

c. Click **Save**. Then confirm the change.

4. Configure Cloud Proxies in the **Proxies (Cloud)** tab, as follows:

a. In the **Server Side** area, define the following details:

   i. In the **Cloud Proxy HTTP Port** field, specify the server-side HTTP port number on which <u>all</u> cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.

   ii. In the **Cloud Proxy HTTPS Port** field, specify the server-side HTTPS port number on which <u>all</u> cloud proxies and cloud-based load balancers will listen, and to which all clients will connect.

b. In the **Client Side** area, do the following:

   > Be sure not to confuse the Local Client ports and Listening Server ports.

   i. In the **Local Control Port** field, specify the port to which the client uses to perform "control" activities, such as configuration updates. **Note**: It is recommended that you not change the port value from the default unless you use the default for a different application.

   ii. In the **Client Side** table under the Local Control Port field, for each Cloud Scanner or Load Balancer that the client can use, define the identifying details, as follows:

      1. Click the ➕ icon.

      2. In the **Comment** field, specify an internal label for this scanner/load balancer, for example a suggested name could include the scanner type, and/or the scanner's location.

      3. In the **Address** field, specify the IP Address or Hostname of the scanner/load balancer.

      4. In the **Local Client HTTP Port** field, specify the client-side port number used to uniquely identify a specific cloud proxy or cloud-based load balancer for HTTP.

      5. In the **Local Client HTTPS Port** field, specify the client-side port number used to uniquely identify a specific cloud proxy or cloud-based load balancer for HTTPS.

5. Configure On-premise Proxies and On-premise/Off-premise indicators in the **Proxies (On-premise)** tab, as follows:

   a. In the **On-premise Proxy Details** area, for each explicit proxy server to which roaming users can connect while on premise, configure the details as follows:

      i. Click the ➕ icon.

      ii. In the **Address** field, specify the IP or Hostname of the on-premise proxy server.

      iii. In the **Cloud Proxy HTTP Port** field, HTTP port to which roaming users will connect when on-premise.

      iv. In the **Cloud Proxy HTTPS Port** field, HTTPS port to which roaming users will connect when on-premise.

   b. In the **On-Premise.Off-Premise Indicator** area, do the following:

      i.   In the **Corporate Hostname** field specify the corporate address (for example, www.trust-wave.com). When the user is within the corporate network, this name must be resolvable to the Internal Hostname IP which is specified in the next sub-step. When the user is outside the corporate network, this name should not be resolvable to the Internal Hostname IP.

      ii.   In the **Internal Hostname IP** field specify the IP of the corporate hostname, using either of the following methods:

- Click the **Resolve IP** button. The application will look up the IP address of the internal hostname and display the results in the Internal Hostname IP field.
- Manually specify the Internal Hostname IP.

> Note the following points about the On-Premise Proxy:
> - If the **Corporate Hostname** is resolvable, the PAC file will include instructions to use the local, on-premise proxy, since it recognizes you are within the local network.
> - If the **Corporate Hostname** is not resolvable, it will use the nearest available Cloud proxy region.
>
> The On-premise Proxy Details area can be left empty in a situation where the administrator determines for users which proxy to use.

6. Import Certificates in the **Certificate Management** tab, as follows

   a.   Import the CA Certificate as follows:

      i.   Request a CA Certificate from the CA, and open the certificate in a text editor (for example, Notepad).

      ii.   Copy the public Certificate Key including the Begin Certificate and End Certificate lines.

      iii.   Click the **Import Enterprise CA Certificate** button,

      iv.   In the displayed **Certificate** field, paste the Certificate key and click **OK**.

The Certificate Management tab is re-displayed, and all information provided by the CA is displayed in the appropriate fields under the **CA Certificate** column. Note that only the **Common Name** field is mandatory, that is, that the CA must provide the information required for this field; other fields will be filled in or empty according to the information that is embedded within the certificate.

   b.   Import the Server Certificate in either of the following ways:

- To generate and import a CSR-Based Server Certificate:

      i.   Click the **Generate CSR** link that is under the Import CSR-based Server Certificate button. The window displays the Certificate field with a request for a Server certificate.

      ii.   Copy the Certificate request and provide it to the CA. The CA processes the request and generates a Server Certificate.

      iii.   Open the certificate in a text editor (for example, Notepad), and copy the certificate.

      iv.   Click the **Import CSR-based Server Certificate** button.

      v.   In the displayed **Certificate** field, paste the Certificate key and click **OK**.

- To import a Server Certificate:

    i. Request a CA Certificate from the CA, and open the certificate in a text editor (for example, Notepad).

    ii. Click the **Import Server Certificate** button.

    iii. The window displays entry fields for entering information from the Server certificate.

    iv. Copy the certificates information that is displayed in the editor and paste it in the appropriate entry fields in the window. Then click **OK**.

Regardless of the method you chose to import the Server certificate, the Certificate Management tab is re-displayed, and all information provided by the CA in the certificate is displayed in the appropriate fields under the **Server Certificate** column. Note that only the **Common Name** field is mandatory, that is, that the CA must provide the information required for this field; other fields will be filled in or empty according to the information that is embedded within the certificate.

7. According to need, define **Non-Routable Network Bypass** and **Trusted URL Bypass** settings in the **Bypass** tab, as follows.

  a. For each network or domain to be bypassed while the Mobile Security Client agent is browsing in Cloud proxy or local proxy, add it to the bypass list, as follows:

    i. Click the ➕ icon.

    ii. In the opened detail line, edit the Network Address and Network Mask.

    iii. To delete a network bypass, right-click the icon and choose **Delete Row**.

  b. To enable security to bypass the URLs appearing in a particular type of URL list (for example, Customer Defined White List), select the URL type in the **Trusted URL's** drop down list.

8. Set Client Configuration in the **Client Configuration** tab, as follows:

  a. By default, users can only browse using an Trustwave client and PAC file. To eliminate either or both of these restrictions, do the following:

    i. To allow the user to disable the client and browse using a non-Trustwave agent, clear the **Prevent user from disabling client** check box.

Disabling the Mobile Security Client agent might contravene your site's Acceptable Use Policy. Therefore, consider carefully before clearing this check box which gives users the ability to disable the agent.

    ii. If a proprietary PAC file is used, clear the **Enforce PAC file usage via the Mobile Security Client** check box.

  b. To ensure that a warning is issued if a user tries to uninstall the client, ensure that the **Enable Agent Uninstall Warning Text** check box is selected, and if desired, edit the message text in the accompanying text box.

  c. In the **EKU** field, specify the OID provided by the domain administrator.

9. Define Certificate Revocation List handling in the **CRL Handling** tab, as follows:

a. Specify the location of the Certificate Revocation List. To test the location, click **Test**.

b. In the Scheduling area, there is an option to define a time schedule for how often certificate revocation is performed against the list.

10. Click **Save**.

11. Click ⋙.

12. In the **Provisioning** tab:

a. Download the appropriate Client Installer, for Windows or Mac, so that you can later distribute it for installation.

b. If you cleared the **Enforce PAC file usage via the Mobile Security Client** check box in the **Client Configuration** tab, you can optionally download and modify the PAC file for later distribution.

> Before you can download these files, you must ensure that you have saved and committed the mandatory information in the other tabs. Download buttons in the Provisioning tab are disabled until all mandatory information in the other tabs is saved and successfully committed. Warning icons and/or yellow field backgrounds in the other tabs indicate which fields are mandatory.
>
> If you are using a third-party PAC file, ensure that the Enforce PAC file usage via the **Mobile Security Client** check box in the Client Configuration tab is cleared, and that the local host proxy within the PAC file belongs to Trustwave.

20.4 Certifying and Managing Cloud Users

> This section is relevant only when the cloud is configured to work in **Internal mode**. In **PKI mode**, cloud users are certified and managed externally.
>
> Furthermore, many of the options and features described in this section are non-operational if the cloud is not configured to work in Internal mode.

Cloud users must be properly certified.

When the cloud is configured to work in **Internal** mode, it is the administrator that must ensure the issuance of certificates to cloud users. They must also manage 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.

These actions are generally performed in the Cloud User Certificate Management screen, accessed under the **Users** main menu option.

To simplify certificate issuance, administrators can dedicate specific User Groups and LDAP Groups to cloud use, and configure those groups so that certificates are automatically issued to all new users added to the group. This eliminates the need to issue certificates individually to each new user in the group.

Such configuration, however, will not apply to any user who belonged to such a group before it was so configured. For these users, as an alternative to individual, manual requests for certification, you can make a group-level request to issue certificates to all non-provisioned users in the group.

You can also, at the group level, download all certificates issued to provisioned users, and request that needed instructions be sent by email to all users.

This section contains the following procedures:

- To certify and manage cloud users:

- To enable automatic certification of all new users in a group, and to prevent disabling of the Mobile Security Client:

- To manually issue or download certificates or emails at the Group level

To certify and manage cloud users:

The Cloud User Certificate Management screen is the main screen for manually handing the issuance and management of certificates for users.

1. Select **Users | Cloud User Certificate Management**.

2. Filter the display, as follows:

   - To leave the display unfiltered, that is, to display the complete list of cloud users, click the ✖ icon.

   - To filter the display:

   Select any desired filtering values in the filtering fields that appear in the same row as the **Filter** button.

   Note that the **Domain** filtering field contains the following selection values:

   - a domain value for each LDAP user.

   - the value **Local Users**, which includes all users belonging to User Groups.

   - the value **All**, which includes all users belonging to User Groups and LDAP groups.

   Note that **Pending** status displays cloud users who will get certificates after you click ⬇ as opposed to **Non-issued** status, which displays cloud users who have not been issued a certificate.

   a. Click the **Filter** button.

   The list of users, as filtered, is displayed below the filter row.

3. To manually issue a certificate to an uncertified user which makes the user a cloud user, click the ▶️ icon for the user and choose **Issue New Certificate**.

> ℹ️ This step is not necessary for new users added to a User Group or LDAP Group that automatically ensures issuance of certificates to new users. For more information, see To enable automatic certification of all new users in a group, and to prevent disabling of the Mobile Security Client:.
>
> This step is necessary, however, for users who belonged to the group before it was so configured, and for users in such a group whose certification has been revoked.

4. To manage the certificates of a particular user, click the ▶️ icon for the user and choose the action to perform. Note the following points about possible actions:

   • **Block certificate** temporarily blocks, but does not revoke a certificate. It is intended for use where a certificate is suspected of being compromised. If the certificate proves not to be compromised, you can unblock it via the **Allow certificate** option; if the certificate has been compromised, you can permanently revoke it via the **Revoke certificate** option.

   • **Revoke certificate** is permanent; it cannot be reversed. Instead a new certificate would have to be issued via the **Issue new certificate** option, as described in Step 3.

   • The **Send provisioning email** action re-sends previously issued certificate information. This option is useful if the initial certificate was lost.

   • You can export a user's certificate to an external file via the **Export Certificate** option.

5. To export all certificates for all users who have valid certificates, click the Export All Certificates button at the bottom of the display.

To enable automatic certification of all new users in a group, and to prevent disabling of the Mobile Security Client:

You can configure any User Group or LDAP Group so that all new users added to the group are automatically issued certificates. This is especially useful if you are dedicating the group to cloud users. You can also ensure the users in the group cannot disable the Mobile Security Client agent on their machines.

1. Display the list of user/LDAP groups as follows:

   • For a regular user group, select **Users | Users/User Groups**.

   • For an LDAP group, select **Users | Authentication Directories | LDAP**.

2. In the tree, select the group.

3. In the group definition screen, click **Edit**.

4. To ensure that each **new** user added to the group automatically becomes a cloud user, that is issued a certificate, select the **Issue Mobile Security Client Certificates to new group members** check box. To issue certificates to all users who were in this group before you performed this configuration, see To manually issue or download certificates or emails at the Group level.

5. To ensure that new users cannot disable the Mobile Security Client agent installed on their machines, ensure that the **Prevent user from disabling Mobile Security Client** check box is selected. The selected check box is the default.

> This option is only relevant if you selected the check box in Step 4.
>
> The **Prevent user from disabling Mobile Security Client** option is only relevant if the site supports a Cloud in **Internal** mode. For more information, see Configuring Cloud Settings in Internal Mode.

6. Click **Save**.

7. If you are ready to distribute and implement the changes in your system devices, click .

To manually issue or download certificates or emails at the Group level

You can use a single operation to perform any of the following operations:

- manually issue certificates to all unprovisioned users in a User Group/LDAP group.

- download the certificates for all provisioned users in a group

- issue instruction emails to all users in a User Group/ LDP Group via a single operation.

1. Display the list of user/LDAP groups as follows:

   - For a regular user group, select **Users | Users/User Groups**.

   - For an LDAP group, select **Users | Authentication Directories | LDAP**.

2. In the tree, do any of the following:

   - To issue certificates to unprovisioned users in a group, right-click the group in the tree and choose I**ssue Mobile Security Client cert to non-provisioned users**.

   - To download the certificates for all provisioned users in the group, which you can then distribute, right-click the group in the tree and choose **Download Group Users Certificates**.

   - To issue emails with instructions to provisioned users in a group, right-click the group in the tree and choose **Send emails to provisioned users**.

20.5 Defining a Private Cloud Scanner

> Before defining a private cloud scanner, ensure that you have added and setup the needed device.

To define a Private cloud scanner

1. Using the Limited Shell commands, define the device as a private cloud, as follows:

a. Log in to the Limited Shell on the device that will be used for the private cloud. The default user name and password for the shell command line are **admin** and **finjan** respectively.

b. Enter the **setup** command. The current configuration is displayed.

c. Enter the line command **config_cloud**.

d. When prompted whether to enable the cloud, enter **Y**.

You will then get a completed message.

2. If the device that you are defining as a private cloud scanner is already defined in the system as a cloud scanner, skip the remaining steps.

3. Select **Administration** | S**ystem Settings** | **Trustwave Devices**.

4. If the device that you are defining as a private cloud scanner is currently defined as a local scanner, delete the device from the Device list by right-clicking the device and choosing **Delete Device**.

5. Add the device to the device list and define it as a cloud scanner as follows:

a. In the Device tree that is displayed in the left pane, right-click the **Devices** root and choose **Add Device**. The New Device screen is displayed in the main window.

b. Specify the device IP.

c. Select **Cloud Scanning Server** as the Device type.

d. In the various tabs in the window, perform the rest of the device configuration. For instructions, see Adding Devices and Device Groups.

6. Click **Save**.

7. Configure the device's General settings. For instructions, see Configuring Device General Settings.

Instructions for configuring Authentication and Caching are described in this guide.

For information on configuring HTTP, ICAP, WCCP, FTP, and HTTPS settings, see the *Management Console Reference Guide*.

8. If you are ready to distribute and implement the changes in your system devices, click .

Implementing Cloud Security

21 Implementing ICAP

Beginning with SWG release 10.2.0, SWG can provide ICAP Services and can use external ICAP Services. Prior to this release, SWG could only provide ICAP Services.

This chapter contains the following main topics:

- Configuring SWG To Provide ICAP Services

- Configuring SWG To Use External ICAP Services

21.1 Configuring SWG To Provide ICAP Services

To enable SWG to provide ICAP Services, you need to configure the **ICAP Service** module, previously called just "ICAP", on the relevant scanning servers.

Cloud scanning servers do NOT have or need an ICAP Service module.

To configure the ICAP Service module:

1. Select **Administration** | **System Settings** | **Trustwave Devices**.

2. Do either of the following:

   - To configure ICAP Service module defaults, choose **Devices | Default Values | Device Settings | ICAP Service**.

   - To configure ICAP Service settings for a specific non cloud scanning server, choose *<device_group>* **|** *<device_ip>* **| Scanning Server | ICAP Service**.

   The **ICAP Service** module window contains five tabs, in addition to an **Enable ICAP Service** check box.

3. In the main window, click **Edit**.

4. To enable the ICAP Service, select the **Enable ICAP Service** check box.

5. In the **ICAP Service** tab, specify the following, as needed:

   - **Listening IP** — local IP on which the ICAP Service listens.

   - **Listening Port** — local port through which the ICAP Service listens.

6. In the **ICAP Clients** tab, define the details of each ICAP client that can request ICAP Services from SWG as follows:

   a. Click the ![plus icon] icon to add an ICAP Client detail line.

   b. Select the client type. Valid values:
      - **Blue Coat**

- **NetApp**
- **Generic**

c. Specify the **Source IP** — IP from which the ICAP client can use this scanner for the ICAP Services. Mandatory.

d. In the Weight field, specify the percentage of resources allowed to this client. The weighted range is 1 to 100.

> The sum of all weights specified for all clients must add up to 100. This is mandatory as the weighting is calculated as a percentage of 100.

7. Click **Save**.

8. If you are ready to distribute and implement the changes in your system devices, click ![icon].

21.2 Configuring SWG To Use External ICAP Services

To configure SWG to use external ICAP Services, that is, for SWG to act as an ICAP client, you must configure the ICAP Client module on the relevant scanning servers, and define ICAP Forward Policy. However, before you can define ICAP Forward Policy, you must define the ICAP Service Groups and their ICAP Services that will be identified in the ICAP Forward Policy rules.

This section contains the following topics:

- Configuring the ICAP Client

- Defining ICAP Service Groups

- Defining ICAP Services

- Defining an ICAP Forward Policy

21.2.1 Configuring the ICAP Client

To enable SWG to receive ICAP Services, you need to configure the **ICAP Client** module.

You can enable ICAP and configure ICAP Client parameters in the Default **ICAP Client** module, and/or the **ICAP Client** module for specific scanning server devices.

The **ICAP Client** module contains two tabs, in addition to the Enable check box.

To configure the ICAP Client module

1. Select **Administration** | S**ystem Settings** | **Trustwave Devices**.

2. Do either of the following:

- To configure ICAP Client module defaults, choose **Devices | Default Values | Device Settings | ICAP Client**.

- To configure ICAP Client settings for a specific scanning server, choose *<device_group>* | *<device_ip>* | **Scanning Server** | **ICAP Client**.

3. In the main window, click **Edit**.

4. To enable the ICAP client, select the **Enable ICAP Client** check box.

5. In the **TimeOuts** tab, adjust the following values, as needed:

   - **Connection Timeout** — Maximum number of second to wait for a connection to be established. Default: 60.

   - **I/O Timeout** — Maximum number of seconds to wait for completion of a message transmission. Default: 120.

   - **Connection Reuse Timeout** — Maximum number of seconds that the connection will be alive on idle after its previous use. Default: 300.

6. In the **Keep Alive** tab, specify the number of seconds between each health check of ICAP Services. The health check determines if the service is up and running. The default is 180 seconds.

7. Click **Save**.

8. If you are ready to distribute and implement the changes in your system devices, click .

21.2.2 Defining ICAP Service Groups

You must identify/define the ICAP Services that SWG as an ICAP client can request. However, each ICAP Service must belong to an ICAP Service Group; therefore, before you can define an ICAP Service, you must define the group to which it will belong.

To define an ICAP Service Group

1. Select **Policies | Condition Elements | ICAP Service Groups**.

2. Do either of the following:

   - To create 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.

   - To edit an existing group, select the group node, and in the main window click **Edit**.

   The ICAP Service Group window is displayed. This window contains two tabs:

   - **General** tab — for defining basic parameters of the group.

   - **Advanced** tab — for defining timeout parameters for the group.

3. Fill in the **General** tab, as follows:

   a. In the **Name** field, specify a name for the ICAP Service Group.

   b. In the **Method** field, select the mode in which the ICAP protocol works. **Note**: Currently, only one mode is supported.
      - **REQMOD** — Request Modification. 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 Request Modification is a Data Leakage Prevention (DLP) server that scans all outgoing requests and enforces the organizations DLP policy.

c. In the **Load Balancing Algorithm** field, select the type of algorithm that should be used for distributing the load. **Note**: Currently, only one algorithm is supported.

   • **Round Robin** — Distributes the load between servers sequentially in a circular pattern.

d. In the **Health Check URL** field, specify the URL to which the SWG scanner sends health check requests through the ICAP Service to ensure that the ICAP Service server is alive, or up and running.

   These requests are sent at the interval defined in the Keep Alive tab in the ICAP Client module.

e. Specify the In the Expected Return Code field, specify the return code expected from the Health Check URL. If this return code is received it is an indication that the ICAP Service is alive.

4. Fill in the **Advanced** tab, as follows:

a. In the **Connection Timeout** field, specify the maximum number of seconds to wait for a health check connection to be established. Default: 60.

b. In the **I/O Timeout** field, specify the maximum number of seconds to wait for completion of a health check transmission. Default: 30.

5. When done, click **Save**.

6. If you are ready to distribute and implement the changes in your system devices, click ⩗.

   You do NOT have to commit the ICAP Service Group before using it in an ICAP Forward policy rule.

21.2.2.1 Defining ICAP Services

To define an ICAP Service

1. Select **Policies | Condition Elements | ICAP Service Groups**.

1. Do either of the following:

   • To create an ICAP Service, right-click the node of the ICAP Service Group to which the ICAP service should be added, and choose **Add Service**. The main window for defining the ICAP Service is displayed.

   • To edit an existing ICAP Service, select the service node, and in the main window click **Edit**.

   The ICAP Service window is displayed.

2. Perform the following steps in the ICAP Service window.

a. Specify a name for the service.

b. To enable use of this external ICAP Service, ensure that the **Enable ICAP Service** check box is selected.

c. In the URL field, specify the URL of the ICAP Service and Server, as follows:

i. In the first entry field (**icap://**), specify the address of the server hosting the ICAP service.

ii. In the second entry field, following the "**:**", specify the port on which the ICAP Service is listening.

iii. In the third entry field, following the "**/**", specify the URL of the ICAP Service on the hosting server. For example: icap://10.10.10.10:1344/Finjan_REQMOD

3. To perform discovery of the ICAP Service's Connection Items through a particular scanner, do the following in the **Scanner** area. For more information on Discovery, see the Management Console Reference Guide:

a. In the **Scanner** field, select the scanner device through which discovery should be performed.

b. Click the **Discovery** button.

The remaining fields in the **Scanner** area display the returned Connection Option values:

• **Max Connections** — Maximum number of simultaneous connections to the Service.

• **Supports preview** — When checked, that is, indicating that the ICAP Service supports Preview, the ICAP Service will initially look at a portion of the request before determining if it has enough information to continue or if it needs to view the full request.

• **Preview Window** — number of bytes the ICAP Service will preview when supported. The default is 4096 bytes.

> • The values returned by discovery replace the current values, and if the returned values are different to the ones they replace, the field is marked with a green asterisk.
>
> • You can return the defaults by clicking 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.

21.2.3 Defining an ICAP Forward Policy

ICAP Forward Policy identifies the ICAP Service Groups from which SWG can request ICAP Services, and defines behavior in case of an error.

> You cannot edit the pre-supplied ICAP Forward policy or **Default ICAP Forward policy**. However, you can duplicate the policy and edit the duplicate; you can also create an ICAP Forward policy from scratch

To define an ICAP Forward Policy:

1. Select **Policies | ICAP Forward.**

2. Do one of the following:

- To create a policy from scratch, right-click the **Policies** root node in the tree, and choose **Add Policy**.

- To duplicate an ICAP Forward policy, right-click the policy to be duplicated, and choose **Duplicate Policy**.

- To edit an ICAP Forward policy that you previously created from scratch or created by duplicating, select the policy in the tree, and then in the main window, click the **Edit** button.

  The Policy Definition is displayed in the main window.

3. Enter a name for the policy.

4. (Optional) Add or modify the policy description.

5. When done, click **Save**.

6. Continue with Defining a Rule in an ICAP Forward Policy.

21.2.3.1 Defining a Rule in an ICAP Forward Policy

If you duplicated a policy, it already has the same rules as were found in the original policy. You can edit these rules or create new rules from scratch.

> Before defining a rule, 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 Defining ICAP Service Groups.

To define a rule in an ICAP Forward policy

1. In the Policy tree, expand the policy so that you display its existing rules. For instructions on displaying the Policy tree, see Step 1 in the procedure Defining an ICAP Forward Policy.

2. Do any of the following:

> Rules in a policy are checked sequentially from the top, and the first rule to be activated in a policy determines the handling of the content. Therefore, the sequential placement of rules in a policy is significant. The default action when no rule fires is to bypass ICAP service. For instructions on moving a rule within a policy, see Relocating an Item in a Tree.

- To edit an existing rule, click the rule in the tree, and then in the main pane, click **Edit**.

- To add a rule to a policy that has no rules, or to add a rule to the bottom of the rule list in the policy, right-click the policy and choose **Add Rule**.

- To add a rule directly above an existing rule, right-click the existing rule, and select **Insert Rule**.

  The main window displays the Rule Definition screen.

3. Enter a name for the rule.

4. (Optional) Provide a description of the rule.

5. Ensure that the check box is appropriately selected or cleared depending on whether or not the rule should be enabled after being committed.

6. Select the **ICAP Service Group** that will provide the ICAP Services.

7. Select the action that SWG should take in case of error. Possible actions:

    - **Fail open** — In case of TCP failure, continue as if nothing happened.

    - **Fail close** — In case of any ICAP conversation failure, fail the HTTP transaction.

8. Click **Save**.

9. To make rule triggering conditional, continue with Defining Conditions in an ICAP Forward Rule.

10. To define additional rules in this policy, repeat this procedure.

11. If you are ready to distribute and implement the changes in your system devices, click .

21.2.3.2 Defining Conditions in an ICAP Forward Rule

To define conditions in an ICAP Forward Rule

1. In the Policy tree, expand the relevant policy and rule. For instructions on displaying the Policy tree, see Step 1 in the procedure To define an ICAP Forward Policy:.

2. Do either of the following:

    - To edit an existing condition, click the condition in the tree, and in the main pane, click **Edit**.

    - To add a new condition to a rule:

    a. Right-click the rule and choose **Add Condition**.

    The main window displays the Condition Definition screen.

    b. In the **Condition Name field**, select the type of condition in the drop down list.

    For any selected condition type, the window displays an appropriate check box list.

    For detailed information on condition types and the particular items in a condition list, see the *Management Console Reference Guide*.

3. If the condition has any other special fields or requirements to fill in, fill them in appropriately.

4. Click **Save**.

5. If you are ready to distribute and implement the changes in your system devices, click .

About Trustwave®

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® 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.