Secure Web Gateway

Version 11.0

Quick Start Guide

Legal Notice

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

Table 1: Revision history

Version	Date	Changes
1.0	September 2012	First document version
2.0	December 2012	SWG Version 11.0 update

About This Guide

This document is a quick start guide to help users installing the SWG for the first time. It describes the basic tasks required to get the proxy up and running, and how to add users and modify policies for first-time use. It also introduces some basic troubleshooting techniques needed to overcome the issues typically encountered in a new installation.

This guide assumes a simple SWG architecture which you would typically encounter in a POC environment. It is ***not*** meant as an all-encompassing guide for day-to-day use. For more information, refer to the *Secure Web Gateway User Guide*.

Formatting Conventions

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

Table 2: Formatting conventions

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in `Lucinda Console 9 pt` indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, or to introduce a new term.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Warnings

i	**Note**: This symbol indicates information that applies to the task at hand.
✓	**Tip**: This symbol denotes a suggestion for a better or more productive way to use the product.
!	**Caution**: This symbol highlights a warning against using the software in an unintended manner.
?	**Question:** This symbol indicates a question that the reader should consider.

Table of Contents

1 Installing Secure Web Gateway

Install the SWG appliance as described in the *SWG Setup Guide*. You can access the Guide online by clicking the following link:

SWG 11.0 Setup Guide

Completion of the initial configuration as outlined in the above Guide is considered a prerequisite for this document.

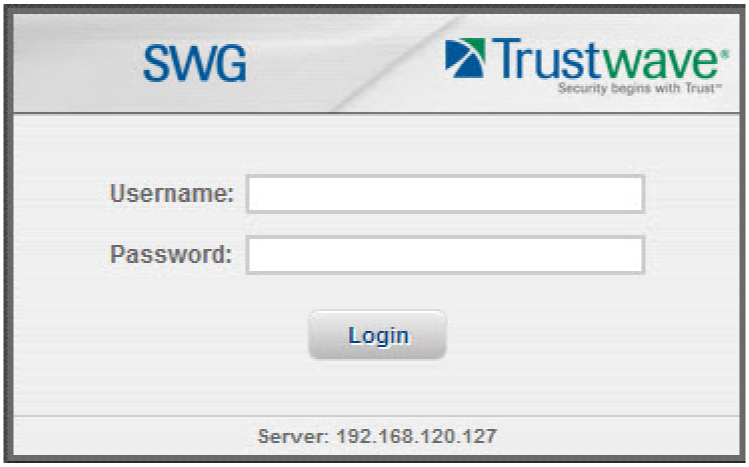
2 Connecting to the GUI

Connect to the GUI with a browser – point to the IP address using HTTPS:

https://<ip address>

Ignore any certificate warnings at this time.

The SWG Login screen opens. When logging in for the first time you will need to change the password from the default.



The default credentials are:

Username: admin
Password: finjan

To log back to the Console directly, use the updated password.

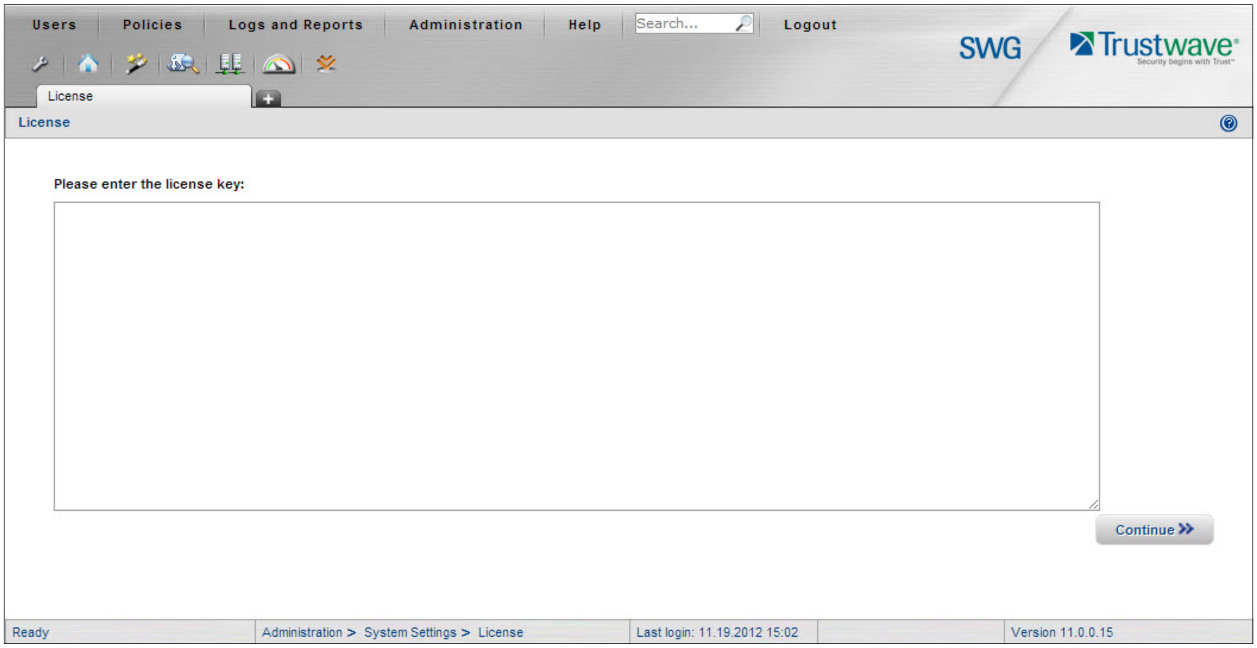
3 Licensing the SWG

You must have an SWG license to proceed. This can be a trial or full license. Be sure to plan ahead and have the license ready on the day of installation.

Licensing for the SWG is modular, so you need to decide in advance which Anti-Virus component, URL Database etc. to use:

- Anti-Virus: Choose from Sophos, McAfee, or Kaspersky
- URL: Choose from Trustwave, Websense, IBM (the default is Trustwave unless selected otherwise)
- Other Modules: Caching, HTTPS

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



Please enter the license key:

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

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

If you wish to participate in the Customer Feedback feature run by Trustwave SpiderLabs Research, ensure that the **Enable sending customer feedback information** check box is selected.

You can disable this feature at any time; Go to **Administration | System Settings | Administrative Settings** and deselect the check box. For more information, see https://www.trustwave.com/support/customer-feedback-module.asp

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

4 Introducing the SWG Interface

4.1 Welcome Screen

On first use, SWG opens at the 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.

4.2 Home Page

The Home Page serves as the entry point to the application Management Console UI, and includes links to frequently used tasks, commonly used reports and charts, information on pending updates and system log information.

Note that the Home Page is a limited view; data shown is dependent on the permissions of the current user.

The Home page is always accessible by clicking the Home icon 🏠 on the Management Console toolbar.

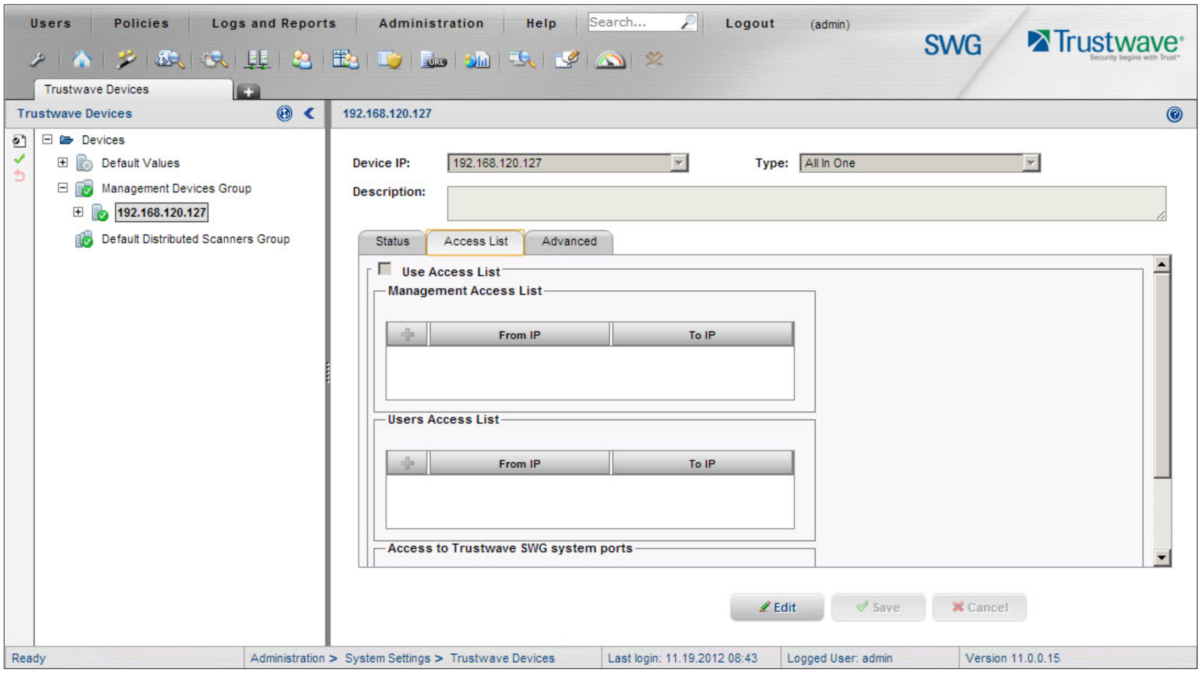
This page can:

- Provide quick links to recent and frequently used activities in the Management Console.
- Display notification of pending system updates and changes, both automatic and those requiring user action.
- Display a selection of logs and reports.

You can arrange the Home page to suit your needs. For more information, see Customizing the Home Page in the *Management Console Reference Guide*.

4.3 Working with the SWG Interface

Here are some quick pointers about the SWG Interface:



Device IP: 192.168.120.127

Type: All In One

Description:

Last login: 11.19.2012 08:43

Logged User: admin

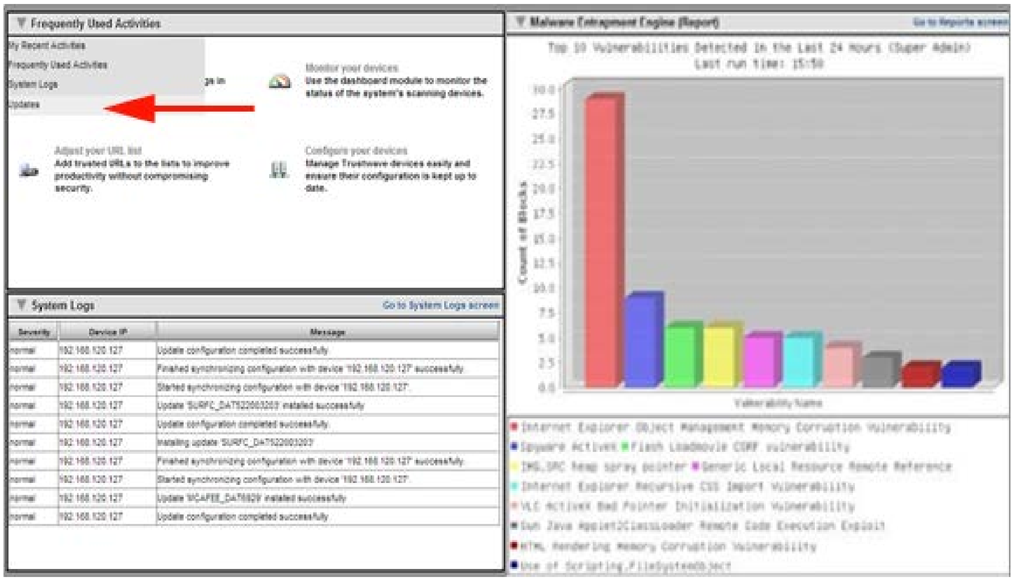
Version 11.0.0.15

- **Right Pane** and **Left Pane:** Most sections of the SWG GUI display a Right Pane containing detailed information about the item selected in the Left Pane. You may need to manually refresh the GUI to see current information. The **Refresh** button is located at the top of the pane.
- **Tabs:** Using tabs can save time when switching back and forth between commonly used areas of the GUI.
- **Toolbar:** Click the toolbar icons to save time accessing commonly used functions. You can customize which icons are displayed by clicking the **Edit Toolbar Buttons** icon .
- **Context Sensitive Help:** Click the **Help** button (or press **F1**) for help relating to the currently displayed GUI section. Note that Help content is online – you will need Internet connectivity to view it.
- **Commit Changes:** Changes to settings, policies, and so on are not applied to the system devices until you commit them by clicking **the Commit Changes** button . If there are no changes to make, this icon is disabled.
- **Right Mouse Click:** The GUI supports right-clicking, and much functionality is accessed in this way.
- **Quick-access icons:** Many tree panes have action icons to the left of the tree entries. You can select an entry in the tree, and then click the appropriate action icon. Pop-up tooltips provide a description of each icon.

4.3.1 Confirming Updates Work Correctly

If the SWG does not receive updates it will not work correctly. It needs URL updates to apply any rules based on URL Filtering. Anti-Virus updates are also needed for obvious reasons. Although the product, strictly speaking, doesn't require updates to perform its behavioral analysis, its security engines will need intermittent security updates to work at their best.

To ensure that the system is up to date, open the **Home** page. If the Updates pane is not open, click the down arrow ▼ in one of the panes and select **Updates** from the drop down menu.


Frequently Used Activities
My Recent Activities
Frequently Used Activities
System Logs
Updates
Monitor your devices
Adjust your URL list
Configure your devices
System Logs
Go to System Logs screen
Malware Entrapment Engine (Report)
Go to Reports screen
Top 10 Vulnerabilities Detected in the Last 24 Hours (Super Admin)
Last run time: 15:50
Count of Blocks
30.0
27.5
25.0
22.5
20.0
17.5
15.0
12.5
10.0
7.5
5.0
2.5
0.0
Vulnerability Name
Internet Explorer Object Management Memory Corruption Vulnerability
Spyware ActiveX
Flash LoadMovie CSRF vulnerability
IMG.SRC heap spray pointer
Generic Local Resource Remote Reference
Internet Explorer Recursive CSS Import Vulnerability
VLC ActiveX Bad Pointer Initialization Vulnerability
Sun Java Applet2ClassLoader Remote Code Execution Exploit
HTML Rendering Memory Corruption Vulnerability
Use of Scripting.FileSystemObject

Use the dashboard module to monitor the status of the system's scanning devices.

Add trusted URLs to the lists to improve productivity without compromising security.

Manage Trustwave devices easily and ensure their configuration is kept up to date.

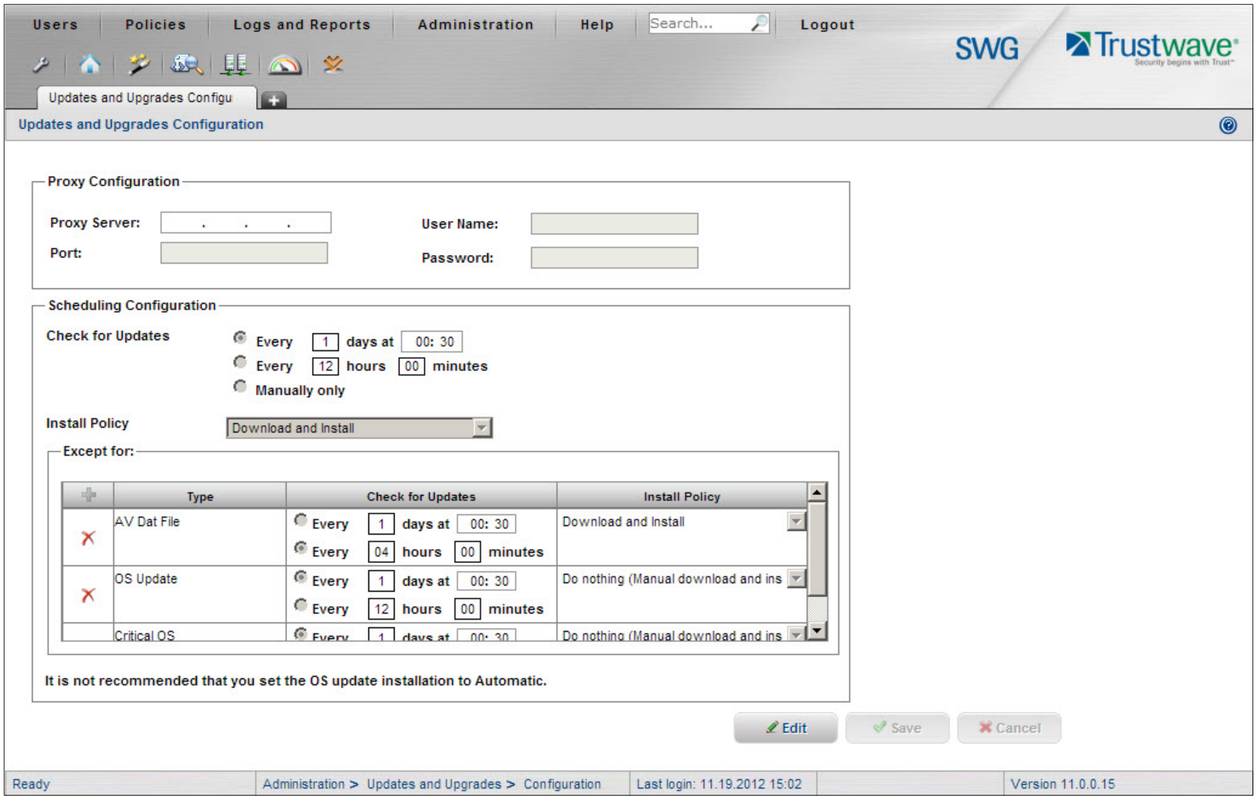
Severity	Device IP	Message
normal	192.168.120.127	Update configuration completed successfully
normal	192.168.120.127	Finished synchronizing configuration with device '192.168.120.127' successfully
normal	192.168.120.127	Started synchronizing configuration with device '192.168.120.127'.
normal	192.168.120.127	Update 'SURFC_DAT522003203' installed successfully
normal	192.168.120.127	Update configuration completed successfully
normal	192.168.120.127	Installing update 'SURFC_DAT522003203'
normal	192.168.120.127	Finished synchronizing configuration with device '192.168.120.127' successfully
normal	192.168.120.127	Started synchronizing configuration with device '192.168.120.127'.
normal	192.168.120.127	Update 'MCAFEE_DAT6929' installed successfully
normal	192.168.120.127	Update configuration completed successfully

Note the tabs in the **Updates and Upgrades Management** screen:

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

If neither the Available Updates nor Installed Updates tabs have any line entries, then no updates are being downloaded. There may be a problem with internet access, or you may need to configure access via a proxy.

To do this, go to **Administration | Updates and Upgrades | Configuration**.


Users
Policies
Logs and Reports
Administration
Help
Search...
Logout
SWG
Trustwave
Security begins with Trust
Updates and Upgrades Configu
Edit
Save
Cancel
Ready
Administration > Updates and Upgrades > Configuration
Last login: 11.19.2012 15:02
Version 11.0.0.15

Updates and Upgrades Configuration

Proxy Configuration

Proxy Server: . . .

Port:

User Name:

Password:

Scheduling Configuration

Check for Updates
● Every 1 days at 00: 30
○ Every 12 hours 00 minutes
○ Manually only

Install Policy: Download and Install

Except for:

	Type	Check for Updates	Install Policy
✗	AV Dat File	○ Every 1 days at 00: 30 ● Every 04 hours 00 minutes	Download and Install
✗	OS Update	● Every 1 days at 00: 30 ○ Every 12 hours 00 minutes	Do nothing (Manual download and ins
	Critical OS	● Every 1 days at 00: 30	Do nothing (Manual download and ins

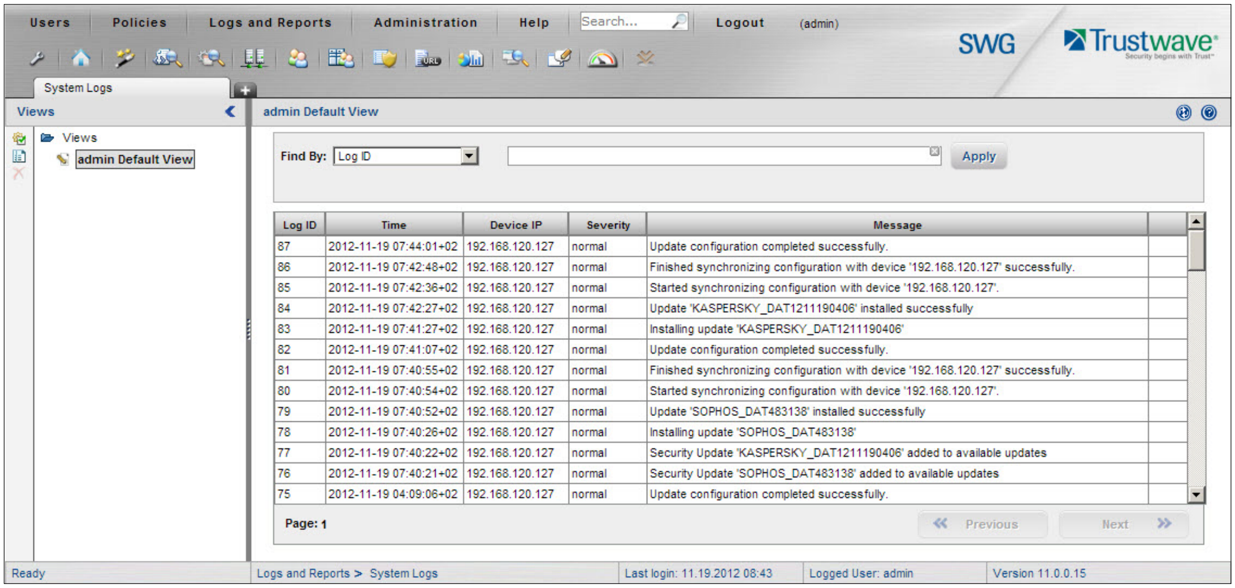
It is not recommended that you set the OS update installation to Automatic.

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

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

To troubleshoot further, go to: **Logs and Reports | System Logs**.

The System Logs should record the success or failure for update retrieval and installation.



Find By: Log ID

Log ID	Time	Device IP	Severity	Message
87	2012-11-19 07:44:01+02	192.168.120.127	normal	Update configuration completed successfully.
86	2012-11-19 07:42:48+02	192.168.120.127	normal	Finished synchronizing configuration with device '192.168.120.127' successfully.
85	2012-11-19 07:42:36+02	192.168.120.127	normal	Started synchronizing configuration with device '192.168.120.127'.
84	2012-11-19 07:42:27+02	192.168.120.127	normal	Update 'KASPERSKY_DAT1211190406' installed successfully
83	2012-11-19 07:41:27+02	192.168.120.127	normal	Installing update 'KASPERSKY_DAT1211190406'
82	2012-11-19 07:41:07+02	192.168.120.127	normal	Update configuration completed successfully.
81	2012-11-19 07:40:55+02	192.168.120.127	normal	Finished synchronizing configuration with device '192.168.120.127' successfully.
80	2012-11-19 07:40:54+02	192.168.120.127	normal	Started synchronizing configuration with device '192.168.120.127'.
79	2012-11-19 07:40:52+02	192.168.120.127	normal	Update 'SOPHOS_DAT483138' installed successfully
78	2012-11-19 07:40:26+02	192.168.120.127	normal	Installing update 'SOPHOS_DAT483138'
77	2012-11-19 07:40:22+02	192.168.120.127	normal	Security Update 'KASPERSKY_DAT1211190406' added to available updates
76	2012-11-19 07:40:21+02	192.168.120.127	normal	Security Update 'SOPHOS_DAT483138' added to available updates
75	2012-11-19 04:09:06+02	192.168.120.127	normal	Update configuration completed successfully.

Page: 1

Logs and Reports > System Logs | Last login: 11.19.2012 08:43 | Logged User: admin | Version 11.0.0.15

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

5 Confirming Proxy Operation

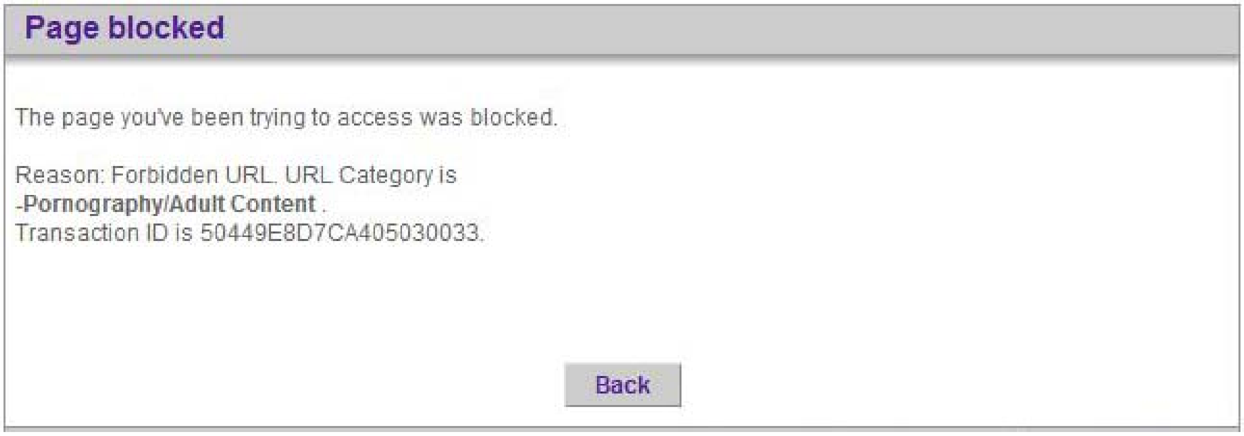
To confirm that the Proxy is handling web requests correctly, point a browser at the SWG. Note that the default listening ports for SWG are 8080 and 8443 for HTTP and HTTPS respectively.

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

Browse to some sites with this browser. There are some test sites that should trigger the default policies in the SWG:

- http://test.8e6.net ... Blocked as Adult if using the Trustwave URL DB (actual content is safe for work)
- http://www.eicar.org/85-0-Download.html ... Contains several forms of the harmless Eicar test virus. The HTTPS link can be used to confirm that HTTPS content scanning works correctly.

Is normal browsing working correctly? Are the above sites getting blocked as shown below?



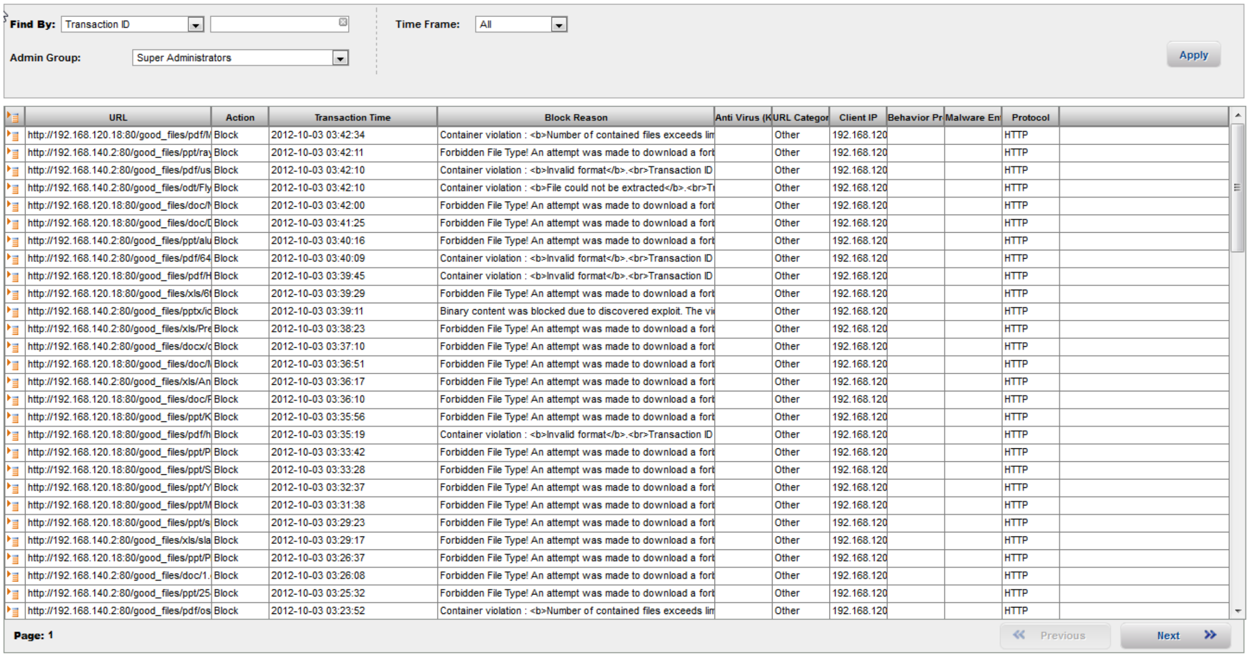
Page blocked

The page you've been trying to access was blocked.

Reason: Forbidden URL. URL Category is
-**Pornography/Adult Content** .
Transaction ID is 50449E8D7CA405030033.

Use the Web Logs to confirm normal operation or to troubleshoot abnormal proxy behavior.

Go to: **Logs and Reports | Web Logs**.



Find By: Transaction ID

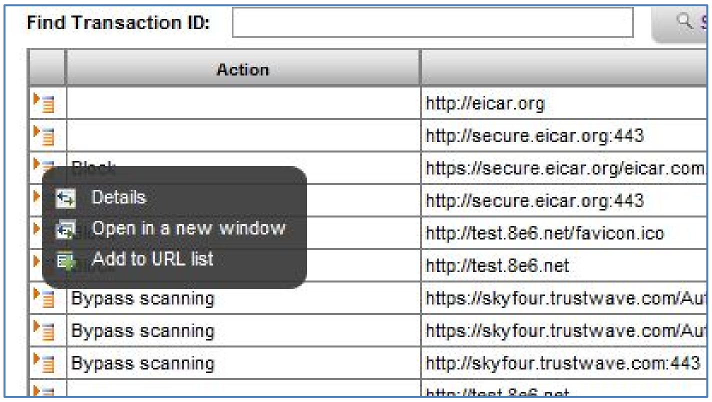
Time Frame: All

Admin Group: Super Administrators

URL	Action	Transaction Time	Block Reason	Anti Virus (K	URL Categor	Client IP	Behavior Pr	Malware En	Protocol
http://192.168.120.18:80/good_files/pdf/M	Block	2012-10-03 03:42:34	Container violation : <b>Number of contained files exceeds lim		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/ray	Block	2012-10-03 03:42:11	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/us	Block	2012-10-03 03:42:10	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/odt/Fly	Block	2012-10-03 03:42:10	Container violation : <b>File could not be extracted</b>. Tr		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/N	Block	2012-10-03 03:42:00	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/D	Block	2012-10-03 03:41:25	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/alu	Block	2012-10-03 03:40:16	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/64	Block	2012-10-03 03:40:09	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/pdf/H	Block	2012-10-03 03:39:45	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/xls/6t	Block	2012-10-03 03:39:29	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pptx/ic	Block	2012-10-03 03:39:11	Binary content was blocked due to discovered exploit. The vi		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/Pre	Block	2012-10-03 03:38:23	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/docx/c	Block	2012-10-03 03:37:10	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/N	Block	2012-10-03 03:36:51	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/An	Block	2012-10-03 03:36:17	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/F	Block	2012-10-03 03:36:10	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/K	Block	2012-10-03 03:35:56	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/pdf/h	Block	2012-10-03 03:35:19	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/P	Block	2012-10-03 03:33:42	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/S	Block	2012-10-03 03:33:28	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/Y	Block	2012-10-03 03:32:37	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/M	Block	2012-10-03 03:31:38	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/s	Block	2012-10-03 03:29:23	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/sla	Block	2012-10-03 03:29:17	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/P	Block	2012-10-03 03:26:37	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/doc/1.	Block	2012-10-03 03:26:08	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/25	Block	2012-10-03 03:25:32	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/os	Block	2012-10-03 03:23:52	Container violation : <b>Number of contained files exceeds lim		Other	192.168.120			HTTP

Page: 1

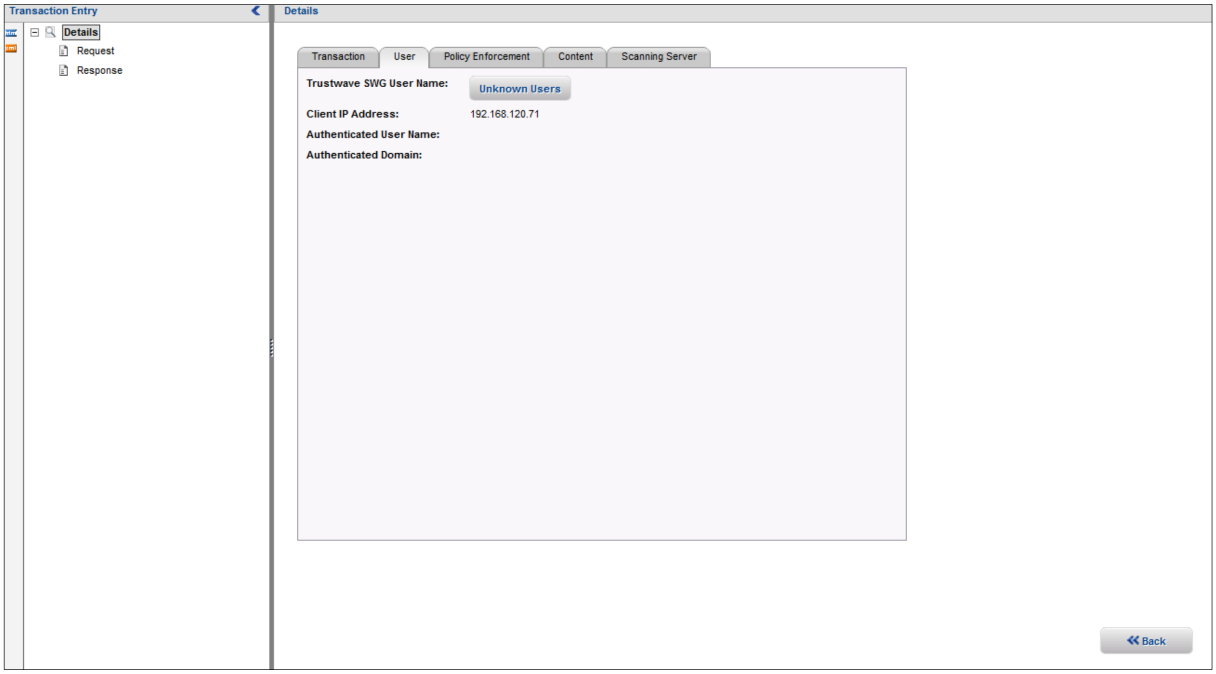
Note that, for each transaction entry, more details can be accessed by right-clicking on the leftmost column (with the little red triangle) and selecting **Open details in new window**.



Find Transaction ID:

Action	
	http://eicar.org
	http://secure.eicar.org:443
Block	https://secure.eicar.org/eicar.com
	http://secure.eicar.org:443
	http://test.8e6.net/favicon.ico
	http://test.8e6.net
Bypass scanning	https://skyfour.trustwave.com/Au
Bypass scanning	https://skyfour.trustwave.com/Au
Bypass scanning	http://skyfour.trustwave.com:443
	http://test.8e6.net

In the Details window, there are several Tabs with extra information about the transaction. Note in particular the User tab, which as shown below contains only the IP address of the User. This is because the Identification Policy for the SWG is not yet configured. The default is to identify by IP address only.



Trustwave SWG User Name: Unknown Users

Client IP Address: 192.168.120.71

Authenticated User Name:

Authenticated Domain:

No Web Logs Visible: If you can access the web via the proxy, but you see no Web Log entries, the first thing to confirm is that an appropriate logging Policy is enabled:

1. Go to **Policies | User Policies | Logging**.
2. Right-click **Log everything except Image files** and select **Set as Default**.

   During the initial setup and troubleshooting phase it is useful to log everything. Later, when everything is configured to your satisfaction, it may be advisable to revert to a Logging Policy that logs less information. This is both for performance reasons and to keep the Web Logs more usable by having fewer entries.
3. If you still can't see any Web Logs:
   a. Double-check that you are actually browsing via the SWG.
   b. Double-check your proxy settings in the browser.
   c. Confirm that the SWG is operating as a normal explicit proxy: Go to **Administration | System Settings | Trustwave Devices**. Then, in the Devices tree in the Left Pane, expand the IP address and Scanning Server nodes and go to **General | Transparent Proxy Mode**. Confirm that the Transparent Proxy Mode check box is <u>not enabled</u>.

6 Configuring Identification and Authentication

6.1 Configuring Identification Policy

You may want to configure the SWG to authenticate, or at least identify, all users browsing through the system. View the various default Logging Policies available under:

Policies | Device Policies | Identification

The two of primary interest will likely be:

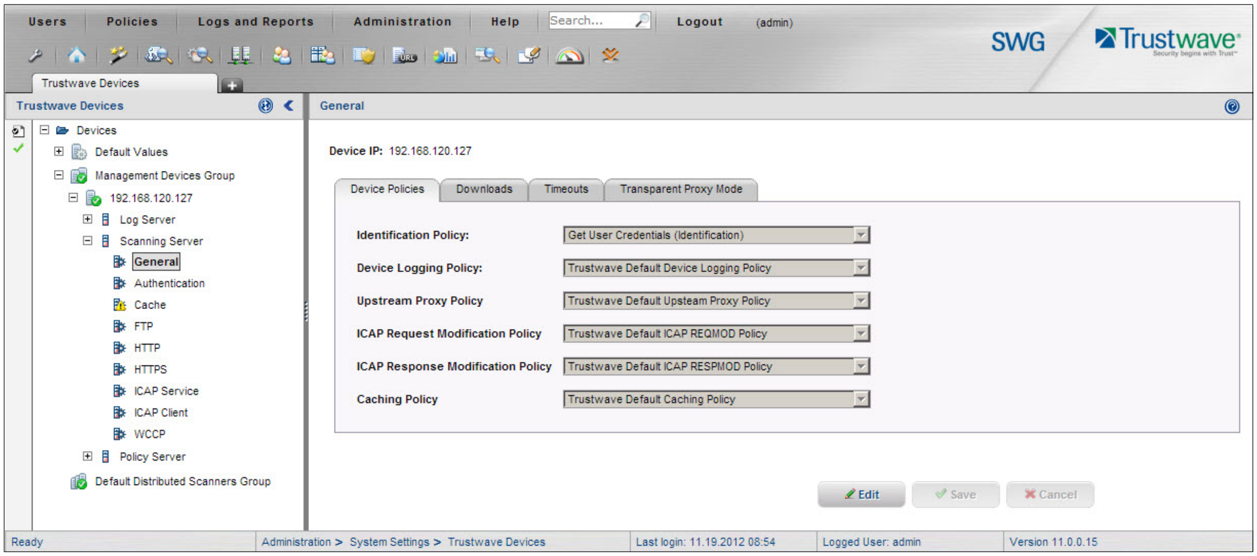
- Get User Credentials
- Authentication

The former uses NTLM to challenge the browser for user details, while the latter takes the additional step of checking the credentials against an Authentication Site (such as AD).

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

To use this policy:

1. Go **to Administration | System settings | Trustwave Devices**.
2. Expand the IP address and Scanning Server nodes and go to **General | Device Policies**.
3. Edit the Device Policies, and configure the Scanning Server to use the Identification Policy of **Get User Credentials**:



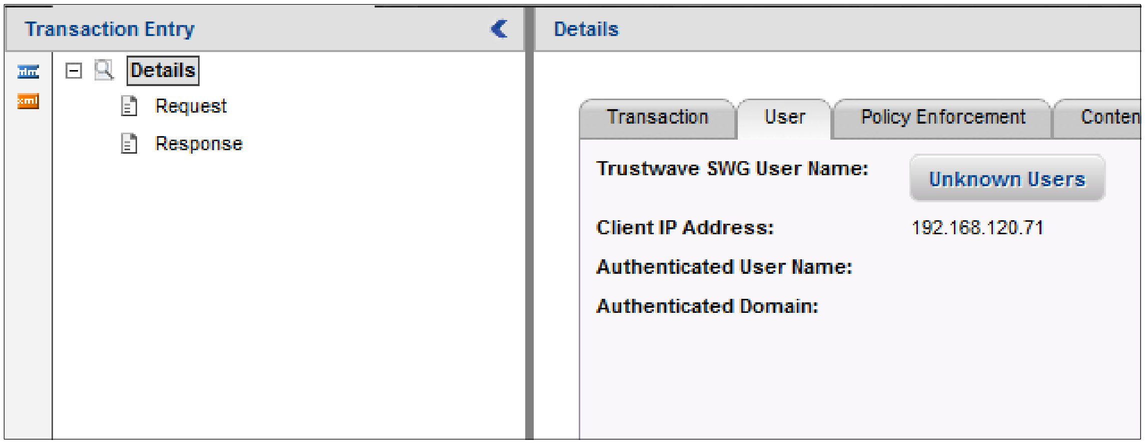
Device IP: 192.168.120.127

Identification Policy:	Get User Credentials (Identification)
Device Logging Policy:	Trustwave Default Device Logging Policy
Upstream Proxy Policy	Trustwave Default Upsteam Proxy Policy
ICAP Request Modification Policy	Trustwave Default ICAP REQMOD Policy
ICAP Response Modification Policy	Trustwave Default ICAP RESPMOD Policy
Caching Policy	Trustwave Default Caching Policy

Ready | Administration > System Settings > Trustwave Devices | Last login: 11.19.2012 08:54 | Logged User: admin | Version 11.0.0.15

4. Commit the changes.
5. Access some websites in your browser to generate new Web Logs. View the Details for these new transactions, and access the User Tab.

   Note that, as shown below, the User Name and Domain name are now listed correctly, but the SWG User Name remains as 'Unknown Users'. This is because the user is not yet a member of any Trustwave group or imported LDAP group (see next section)



Trustwave SWG User Name: Unknown Users

Client IP Address: 192.168.120.71

Authenticated User Name:

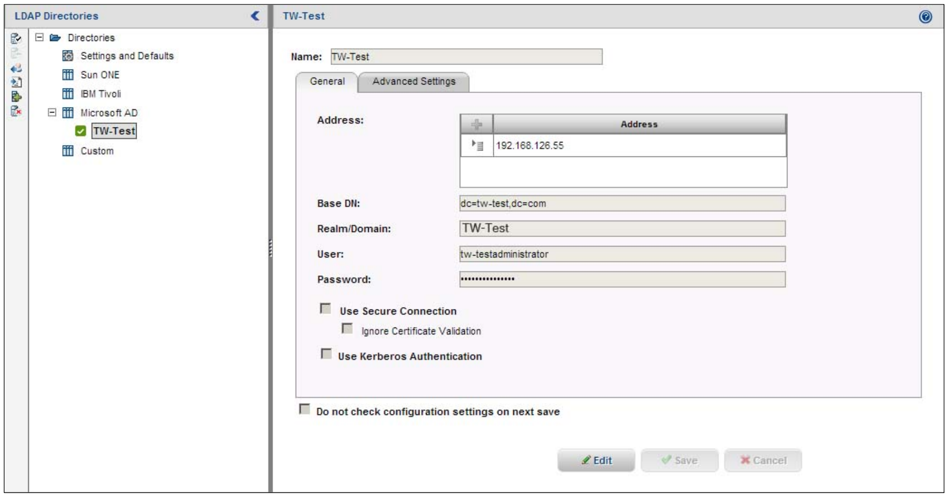
Authenticated Domain:

6.2 Importing LDAP Groups

To apply different policies or rule exceptions to end users, it is necessary to place users into groups. The easiest way to do this is by importing LDAP groups.

To do this, you need to configure a connection to an LDAP Server.

1. Go to **Users | Authentication Directories | LDAP**.
2. If connecting to AD, right-click **Microsoft AD** and select **Add Directory**. Use the context-sensitive Help if you need guidance in filling out the fields. See below for an example of a completed LDAP connection.



Name: TW-Test

Address: 192.168.126.55

Base DN: dc=tw-test,dc=com

Realm/Domain: TW-Test

User: tw-testadministrator

Password: •••••••••••••••

□ Use Secure Connection

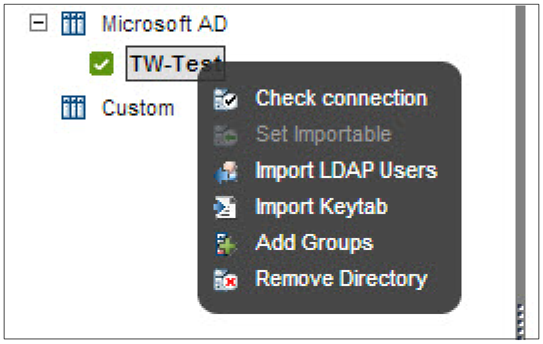
□ Ignore Certificate Validation

□ Use Kerberos Authentication

□ Do not check configuration settings on next save

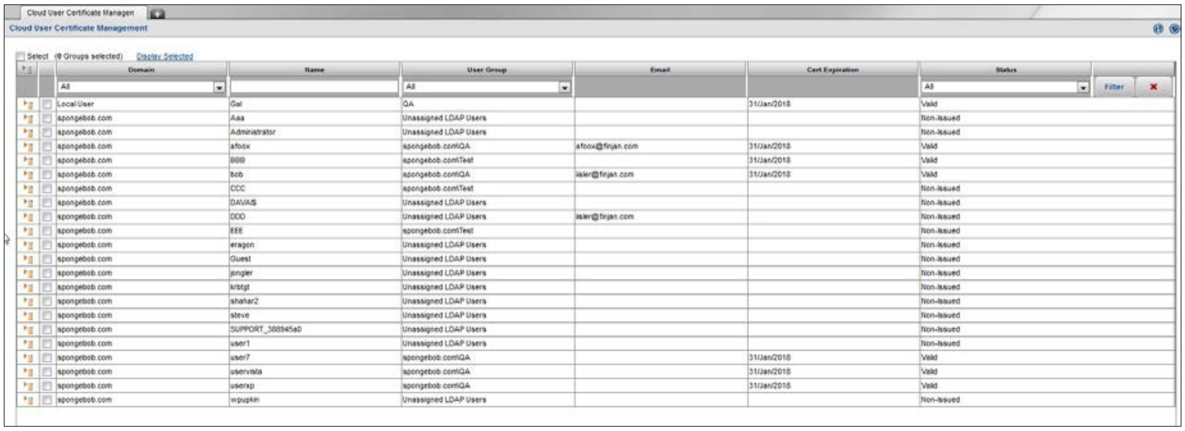
3. Right-click the newly-added LDAP connection, and choose **Add Groups**.
4. Select the LDAP Group(s) that you need to import.

   Note that the Search facility for Groups is case-sensitive.
5. Once you have selected your groups, right-click the LDAP connection again and choose **Import LDAP Users** – this makes the SWG connect to the LDAP server and actually imports the users.



There is no way to view LDAP group membership directly in the SWG. You can, however, see that users have been imported by viewing the Certificate Management page.

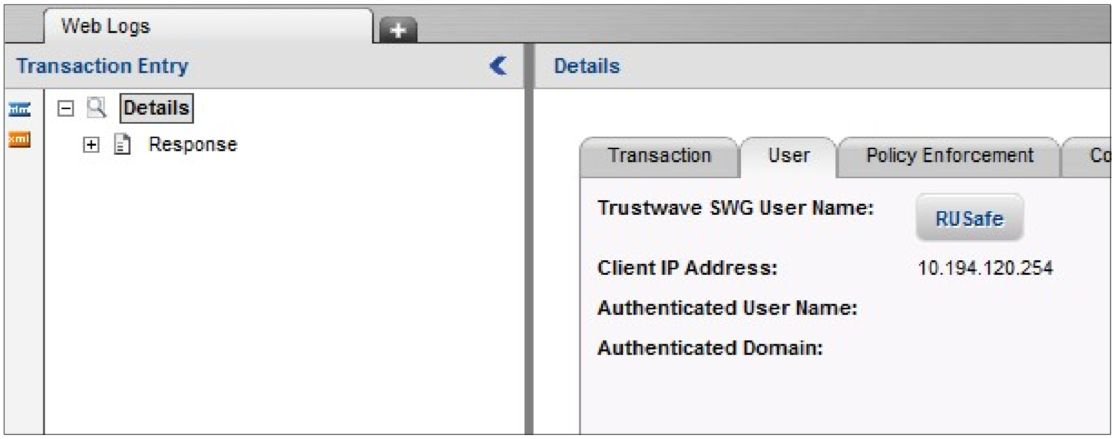
1. Go to **Users | Cloud User Certificate Management.**


Cloud User Certificate Managen
Cloud User Certificate Management
Select (0 Groups selected)
Display Selected
Filter

☐	Domain	Name	User Group	Email	Cert Expiration	Status
	All		All			All
☐	Local User	Gal	QA		31/Jan/2018	Valid
☐	spongebob.com	Aaa	Unassigned LDAP Users			Non-issued
☐	spongebob.com	Administrator	Unassigned LDAP Users			Non-issued
☐	spongebob.com	afoox	spongebob.com\QA	afoox@finjan.com	31/Jan/2018	Valid
☐	spongebob.com	BBB	spongebob.com\Test		31/Jan/2018	Valid
☐	spongebob.com	bob	spongebob.com\QA	isler@finjan.com	31/Jan/2018	Valid
☐	spongebob.com	CCC	spongebob.com\Test			Non-issued
☐	spongebob.com	DAVA$	Unassigned LDAP Users			Non-issued
☐	spongebob.com	DDD	Unassigned LDAP Users	isler@finjan.com		Non-issued
☐	spongebob.com	EEE	spongebob.com\Test			Non-issued
☐	spongebob.com	eragon	Unassigned LDAP Users			Non-issued
☐	spongebob.com	Guest	Unassigned LDAP Users			Non-issued
☐	spongebob.com	jongler	Unassigned LDAP Users			Non-issued
☐	spongebob.com	krbtgt	Unassigned LDAP Users			Non-issued
☐	spongebob.com	shahar2	Unassigned LDAP Users			Non-issued
☐	spongebob.com	steve	Unassigned LDAP Users			Non-issued
☐	spongebob.com	SUPPORT_388945a0	Unassigned LDAP Users			Non-issued
☐	spongebob.com	user1	Unassigned LDAP Users			Non-issued
☐	spongebob.com	user7	spongebob.com\QA		31/Jan/2018	Valid
☐	spongebob.com	uservista	spongebob.com\QA		31/Jan/2018	Valid
☐	spongebob.com	userxp	spongebob.com\QA		31/Jan/2018	Valid
☐	spongebob.com	wpupkin	Unassigned LDAP Users			Non-issued

2. Generate more web traffic as a user who is a member of an imported LDAP group.

In the Web Logs User tab, you should see group membership listed under the Trustwave SWG User Name.



Trustwave SWG User Name: RUSafe

Client IP Address: 10.194.120.254

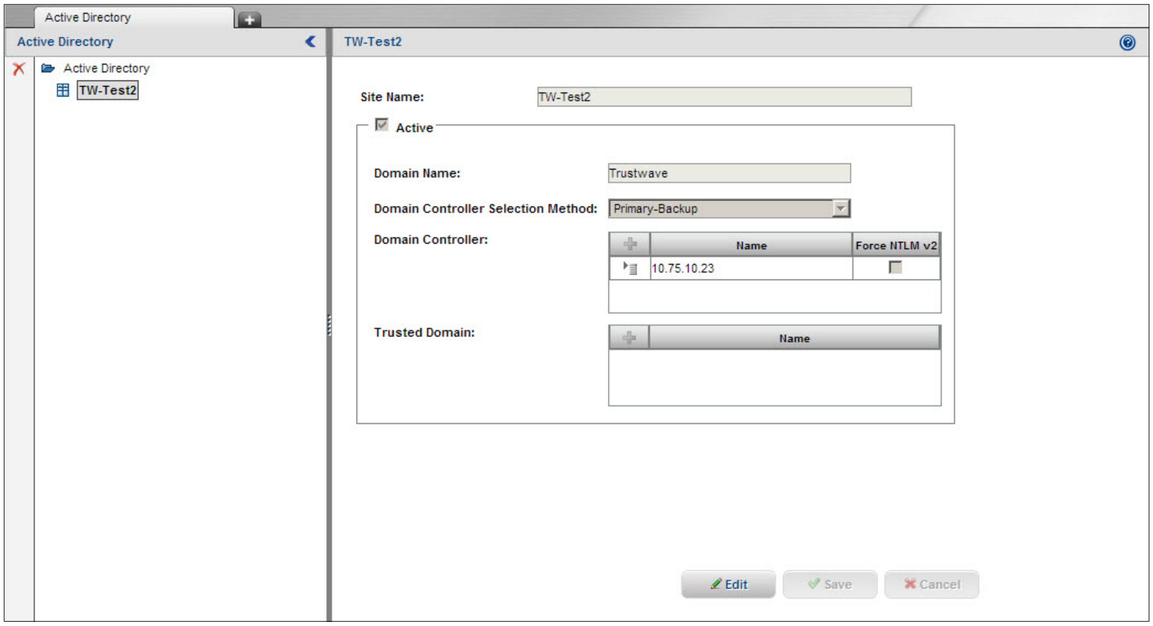
Authenticated User Name:

Authenticated Domain:

6.3 Configuring Full Authentication

To enable full authentication against AD, you must first configure the AD Site.

1. Go to **Users | Authentication Directories | Active Directory**.



Site Name: TW-Test2

☑ Active

Domain Name: Trustwave

Domain Controller Selection Method: Primary-Backup

Domain Controller:

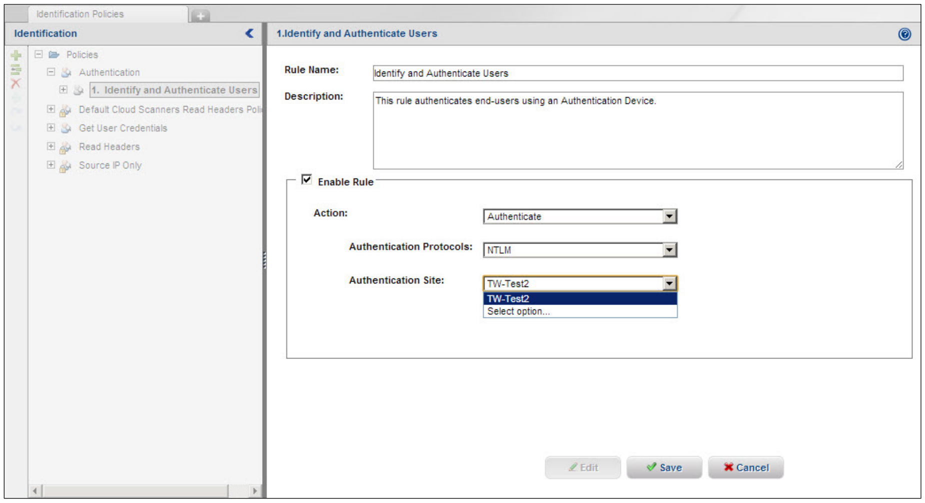
Name	Force NTLM v2
10.75.10.23	□

Trusted Domain:

Name

2. Add the details of a domain controller in your AD site.

3. Configure your Authentication Policy to use this new Site.



1.Identify and Authenticate Users

Rule Name: Identify and Authenticate Users

Description: This rule authenticates end-users using an Authentication Device.

☑ Enable Rule

Action: Authenticate

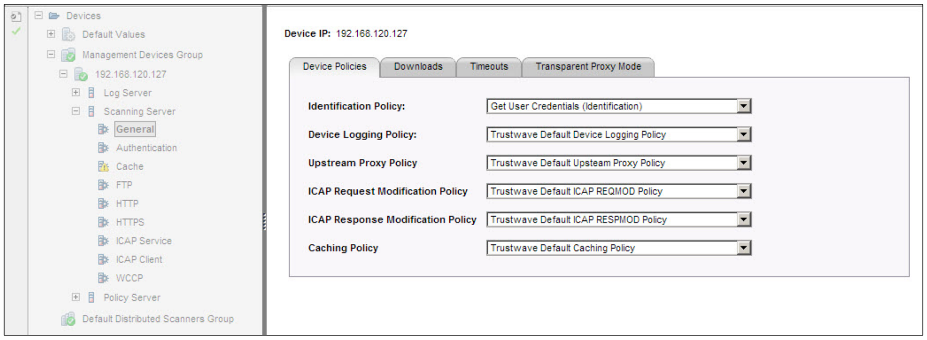
Authentication Protocols: NTLM

Authentication Site: TW-Test2

TW-Test2
Select option...

4. Configure the scanning server to use the Authentication Policy.
   a. Go to **Administration | System settings | Trustwave Devices.**
   b. In the Devices tree in the Left Pane, expand the IP address of the Scanning Server and go to **General | Device Policies.**

5. Edit the Device Policies, and configure the Scanning Server to use the Identification Policy of **Get User Credentials.**



Device IP: 192.168.120.127

Identification Policy: Get User Credentials (Identification)

Device Logging Policy: Trustwave Default Device Logging Policy

Upstream Proxy Policy Trustwave Default Upsteam Proxy Policy

ICAP Request Modification Policy Trustwave Default ICAP REQMOD Policy

ICAP Response Modification Policy Trustwave Default ICAP RESPMOD Policy

Caching Policy Trustwave Default Caching Policy

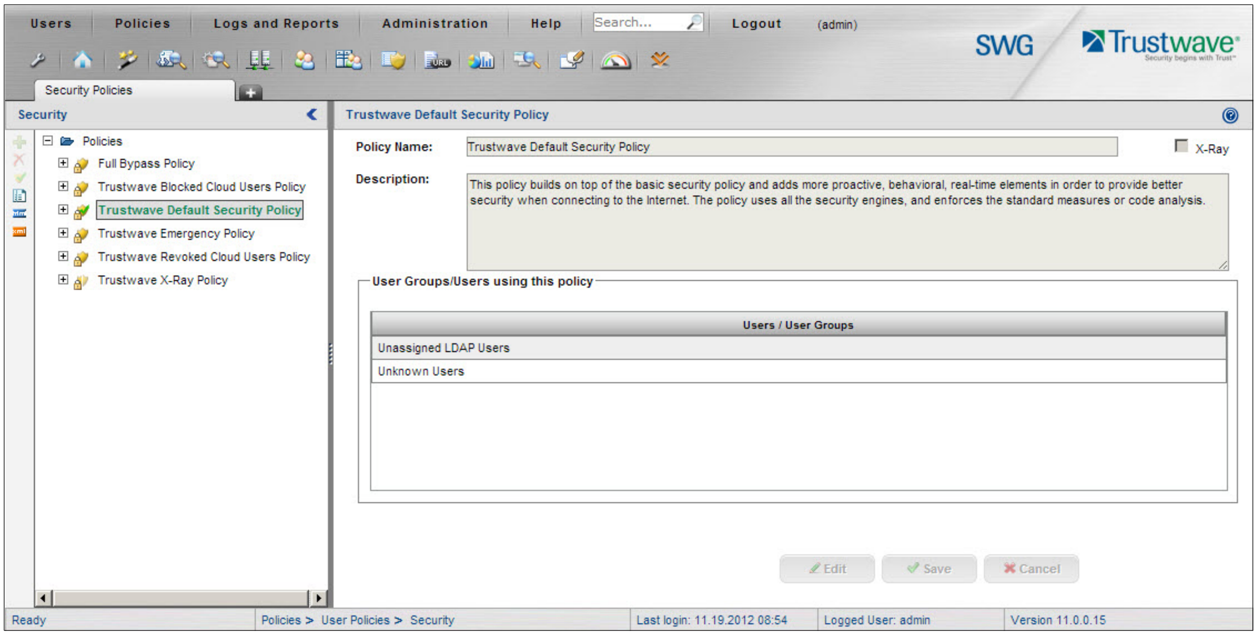
Note: There is a known issue with using Authentication against a Server 2008 R2 site. Refer to this KB article for more information:

HOTFIX: Authentication failure with MS AD 2008 R2 when using windows 7/vista Client.

7 Defining Security Policies

The SWG is shipped with a selection of Security Policies.

To view these, go to **Policies | User Policies | Security**.



- Policies
  - Full Bypass Policy
  - Trustwave Blocked Cloud Users Policy
  - Trustwave Default Security Policy
  - Trustwave Emergency Policy
  - Trustwave Revoked Cloud Users Policy
  - Trustwave X-Ray Policy

Trustwave Default Security Policy

Policy Name: Trustwave Default Security Policy

□ X-Ray

Description: This policy builds on top of the basic security policy and adds more proactive, behavioral, real-time elements in order to provide better security when connecting to the Internet. The policy uses all the security engines, and enforces the standard measures or code analysis.

User Groups/Users using this policy

Users / User Groups
Unassigned LDAP Users
Unknown Users

Ready | Policies > User Policies > Security | Last login: 11.19.2012 08:54 | Logged User: admin | Version 11.0.0.15

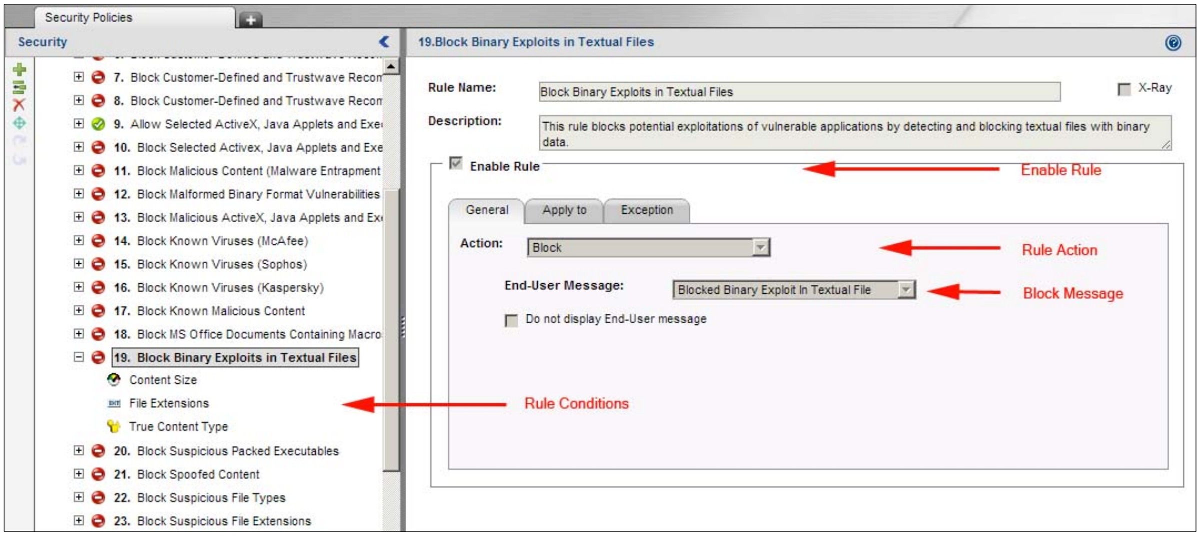
Note that all of the policies have a little padlock on the icon, indicating that each Policy is read-only.

If you need to create a customized Policy, you must duplicate an existing Policy.

To do so:

1. Right-click, say, the Trustwave Default Security Policy and select **Duplicate**.
2. Give the duplicate policy a suitable name and then save it.

3. Expand the custom Policy and view one of the Rules to see how it is constructed.



7. Block Customer-Defined and Trustwave Recon
8. Block Customer-Defined and Trustwave Recon
9. Allow Selected ActiveX, Java Applets and Exe
10. Block Selected Activex, Java Applets and Exe
11. Block Malicious Content (Malware Entrapment
12. Block Malformed Binary Format Vulnerabilities
13. Block Malicious ActiveX, Java Applets and Ex
14. Block Known Viruses (McAfee)
15. Block Known Viruses (Sophos)
16. Block Known Viruses (Kaspersky)
17. Block Known Malicious Content
18. Block MS Office Documents Containing Macro
19. Block Binary Exploits in Textual Files
    - Content Size
    - File Extensions
    - True Content Type
20. Block Suspicious Packed Executables
21. Block Spoofed Content
22. Block Suspicious File Types
23. Block Suspicious File Extensions

Rule Name: Block Binary Exploits in Textual Files

Description: This rule blocks potential exploitations of vulnerable applications by detecting and blocking textual files with binary data.

☑ Enable Rule

Action: Block

End-User Message: Blocked Binary Exploit In Textual File

□ Do not display End-User message

Enable Rule

Rule Action

Block Message

Rule Conditions

Note the following Rule Properties:

- **Rule Conditions:** The components that must match in order for the rule to trigger.
- **Rule Actions:** The action taken if the rule triggers; Block, Coach (warn user), or Bypass
- **Enable Rule:** Turns the Rule on or off
- **Block Message:** Controls the text of the message seen by the end user

  In case the default policy does not meet your needs, you can walk through the rules enabling and disabling rules and rule components as needed. Here are some key Rules to focus on:

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

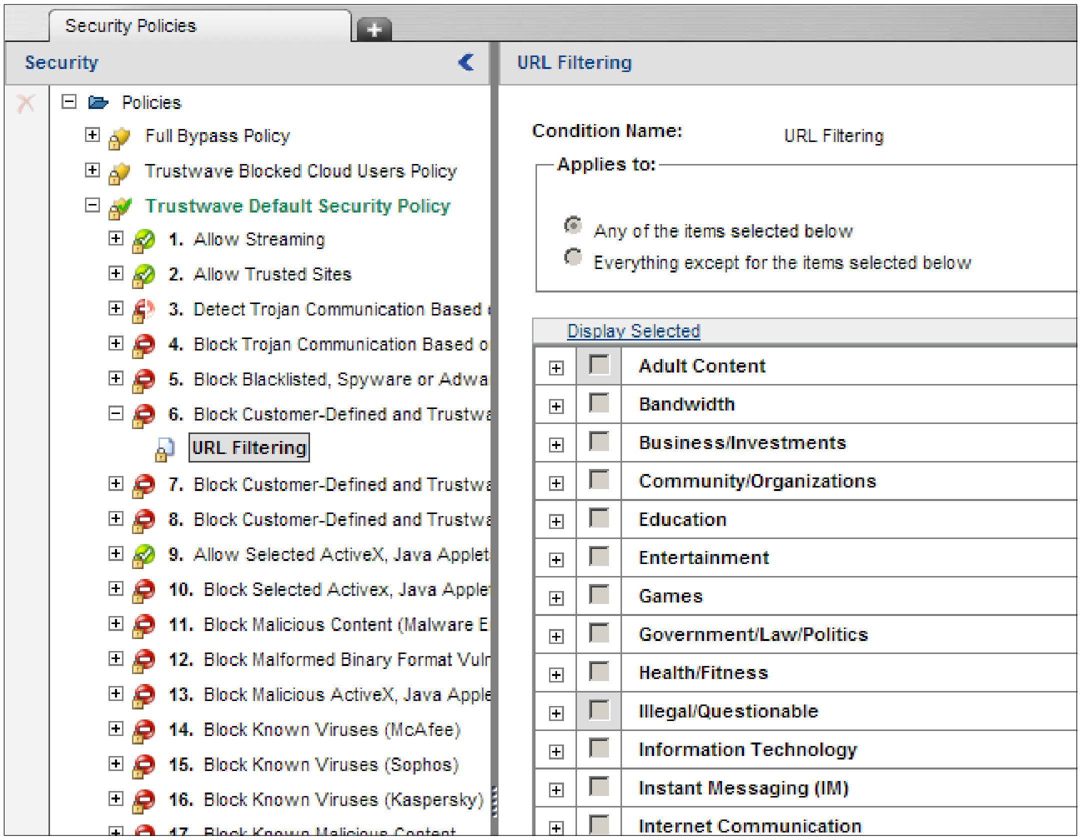
  Go to: **Policies | Condition Elements | URL Lists**

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

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

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

- **Block Customer-Defined and Trustwave Recommended Site Categories:** This rule will certainly require some consideration. This one rule takes care of blocking all your chosen URL categories.



Security Policies

Security

- Policies
  - Full Bypass Policy
  - Trustwave Blocked Cloud Users Policy
  - Trustwave Default Security Policy
    - 1. Allow Streaming
    - 2. Allow Trusted Sites
    - 3. Detect Trojan Communication Based
    - 4. Block Trojan Communication Based o
    - 5. Block Blacklisted, Spyware or Adwa
    - 6. Block Customer-Defined and Trustwa
      - URL Filtering
    - 7. Block Customer-Defined and Trustwa
    - 8. Block Customer-Defined and Trustwa
    - 9. Allow Selected ActiveX, Java Applet
    - 10. Block Selected Activex, Java Apple
    - 11. Block Malicious Content (Malware E
    - 12. Block Malformed Binary Format Vuln
    - 13. Block Malicious ActiveX, Java Apple
    - 14. Block Known Viruses (McAfee)
    - 15. Block Known Viruses (Sophos)
    - 16. Block Known Viruses (Kaspersky)
    - 17. Block Known Malicious Content

URL Filtering

Condition Name: URL Filtering

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

Display Selected

☐ Adult Content
☐ Bandwidth
☐ Business/Investments
☐ Community/Organizations
☐ Education
☐ Entertainment
☐ Games
☐ Government/Law/Politics
☐ Health/Fitness
☐ Illegal/Questionable
☐ Information Technology
☐ Instant Messaging (IM)
☐ Internet Communication

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

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

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

7.1 Rules Order

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

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

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

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

8 Enabling HTTPS Scanning

By default, the SWG performs HTTPS scanning on all HTTPS traffic it receives on port 8443. Below are some things to keep in mind if enabling HTTPS scanning for your users.

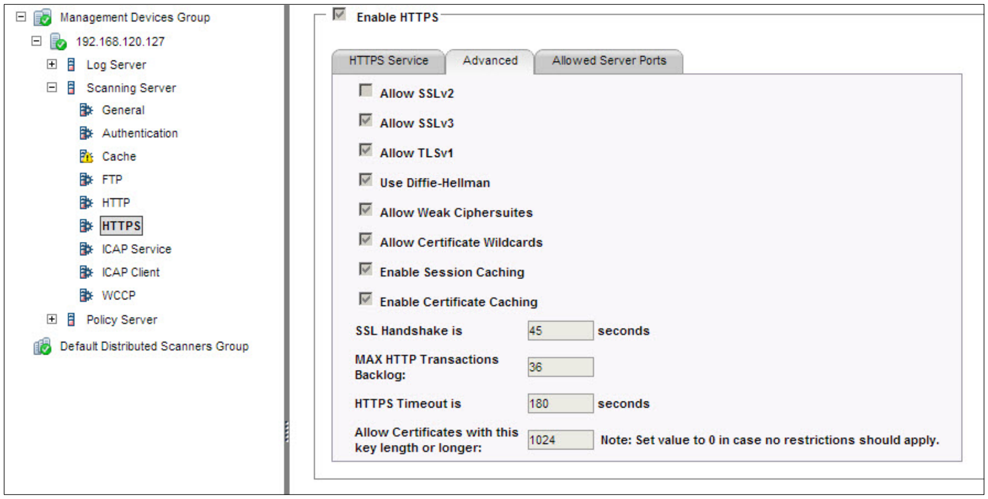
Certificate Roll Out
If you perform HTTPS scanning on web traffic, the end user will receive the certificate provided by the SWG. If this is not made known to their browsers in advance, end users will receive a certificate error. To avoid this problem, it is recommended that the certificate is pushed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

FAQ: How to automate the installation of the user certificate/agent on first login

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

1. Go to **Administration | System settings | Trustwave Devices**.
2. In the Devices tree in the Left Pane, expand the IP address of the Scanning Server and go to **Scanning Server | HTTPS | Advanced**.

3. Ensure that the **Allow Certificate Wildcards** check box is enabled.



☑ Enable HTTPS

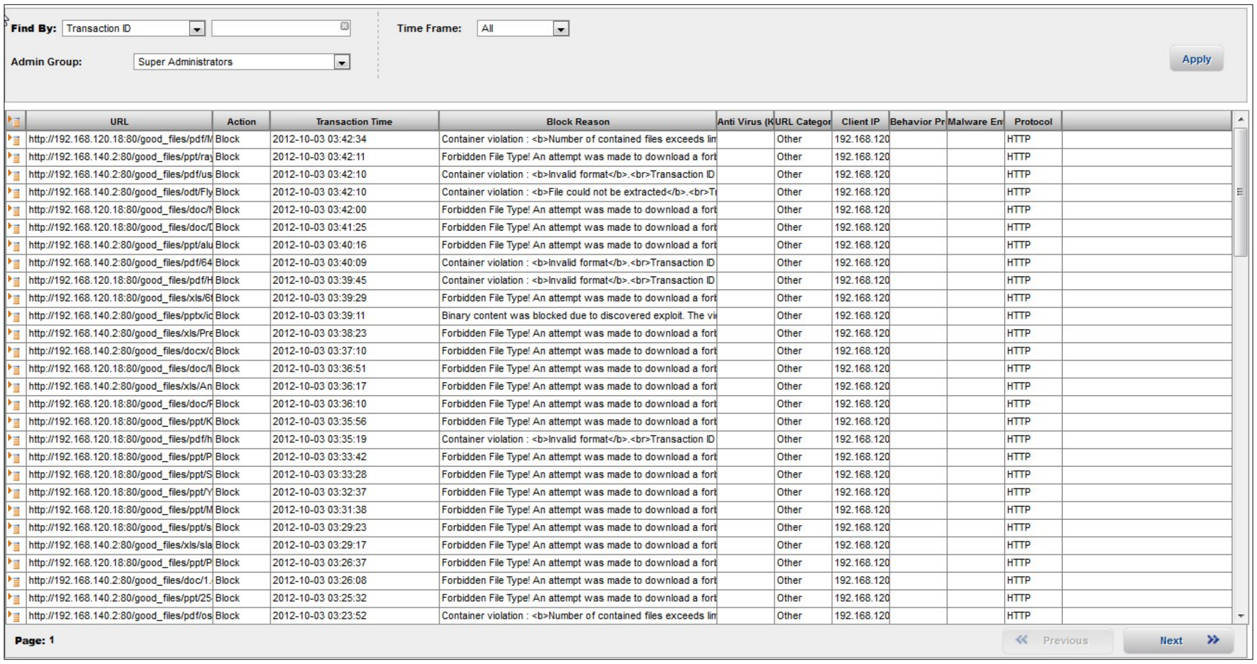
□ Allow SSLv2
☑ Allow SSLv3
☑ Allow TLSv1
☑ Use Diffie-Hellman
☑ Allow Weak Ciphersuites
☑ Allow Certificate Wildcards
☑ Enable Session Caching
☑ Enable Certificate Caching

SSL Handshake is 45 seconds
MAX HTTP Transactions Backlog: 36
HTTPS Timeout is 180 seconds
Allow Certificates with this key length or longer: 1024 Note: Set value to 0 in case no restrictions should apply.

HTTPS and Web Logs

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

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



Find By: Transaction ID
Time Frame: All
Admin Group: Super Administrators

URL	Action	Transaction Time	Block Reason	Anti Virus (K	URL Categor	Client IP	Behavior Pr	Malware En	Protocol
http://192.168.120.18:80/good_files/pdf/M	Block	2012-10-03 03:42:34	Container violation : <b>Number of contained files exceeds lim		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/ray	Block	2012-10-03 03:42:11	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/us	Block	2012-10-03 03:42:10	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/odt/Fly	Block	2012-10-03 03:42:10	Container violation : <b>File could not be extracted</b>. Tı		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/N	Block	2012-10-03 03:42:00	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/D	Block	2012-10-03 03:41:25	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/alu	Block	2012-10-03 03:40:16	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/64	Block	2012-10-03 03:40:09	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/pdf/H	Block	2012-10-03 03:39:45	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/xls/6t	Block	2012-10-03 03:39:29	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pptx/ic	Block	2012-10-03 03:39:11	Binary content was blocked due to discovered exploit. The vi		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/Pre	Block	2012-10-03 03:38:23	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/docx/c	Block	2012-10-03 03:37:10	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/N	Block	2012-10-03 03:36:51	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/An	Block	2012-10-03 03:36:17	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/doc/F	Block	2012-10-03 03:36:10	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/K	Block	2012-10-03 03:35:56	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/pdf/h	Block	2012-10-03 03:35:19	Container violation : <b>Invalid format</b>. Transaction ID		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/P	Block	2012-10-03 03:33:42	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/S	Block	2012-10-03 03:33:28	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/Y	Block	2012-10-03 03:32:37	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/M	Block	2012-10-03 03:31:38	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/s	Block	2012-10-03 03:29:23	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/xls/sla	Block	2012-10-03 03:29:17	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.120.18:80/good_files/ppt/P	Block	2012-10-03 03:26:37	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/doc/1.	Block	2012-10-03 03:26:08	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/ppt/25	Block	2012-10-03 03:25:32	Forbidden File Type! An attempt was made to download a fort		Other	192.168.120			HTTP
http://192.168.140.2:80/good_files/pdf/os	Block	2012-10-03 03:23:52	Container violation : <b>Number of contained files exceeds lim		Other	192.168.120			HTTP

Page: 1

9 Creating Custom HTTPS Policies

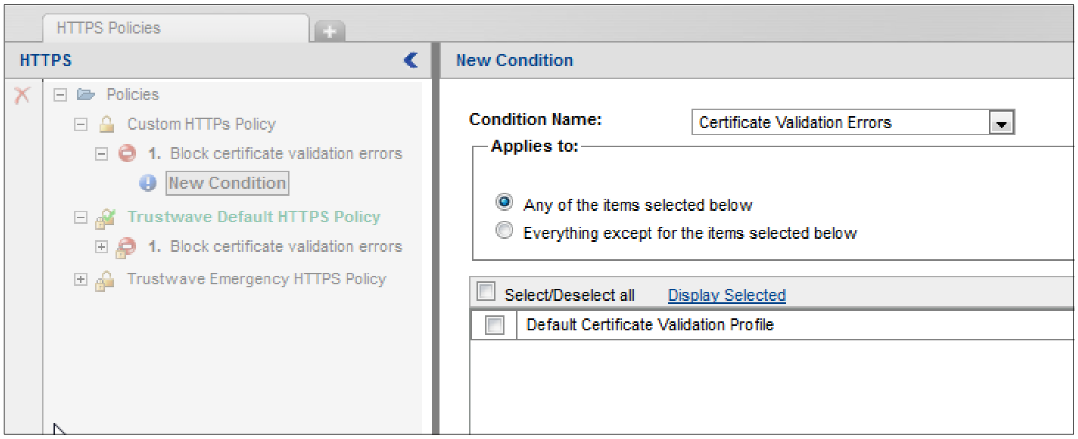
As with Security Policies, the SWG ships with some default, read-only HTTPS Policies. To create a custom HTTPS Policy, you need to duplicate and then edit an existing HTTPS policy.

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

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

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

As with the Default HTTPS Policy, the default Validation Profile is read-only, and if you wish to edit you must duplicate it. Don't forget; if you do this, you must configure your HTTPS Rule to use the new Profile:


HTTPS Policies
HTTPS
Policies
Custom HTTPs Policy
1. Block certificate validation errors
New Condition
Trustwave Default HTTPS Policy
1. Block certificate validation errors
Trustwave Emergency HTTPS Policy
New Condition

Condition Name: Certificate Validation Errors

Applies to:

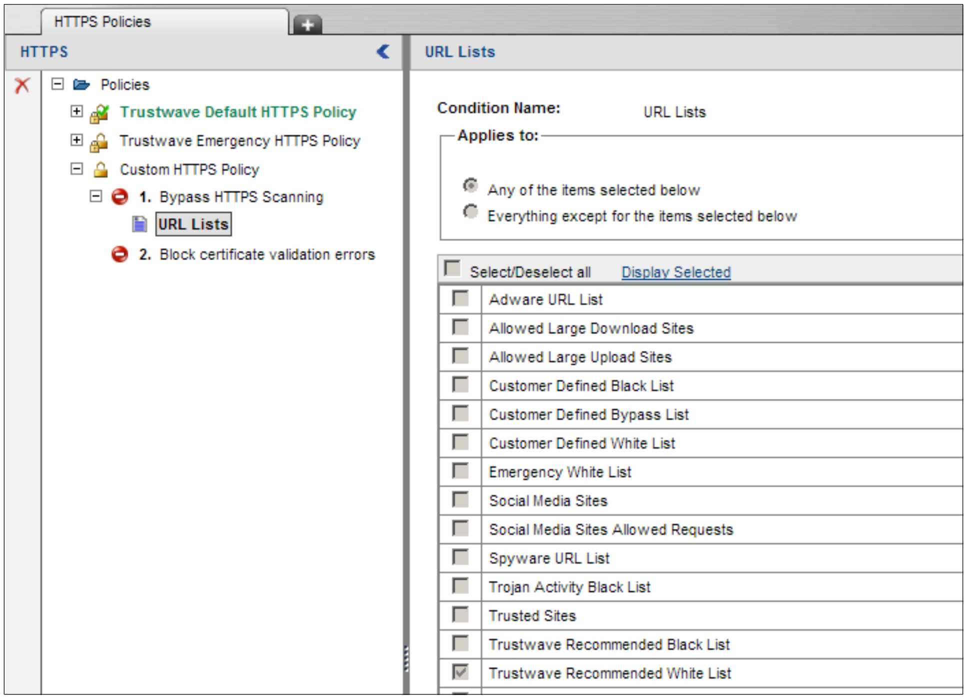
● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all Display Selected

□ Default Certificate Validation Profile

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

Add a URL List rule condition, and select your HTTPS Whitelist. The rule should look something similar to that shown below:


HTTPS Policies
+
HTTPS
Policies
Trustwave Default HTTPS Policy
Trustwave Emergency HTTPS Policy
Custom HTTPS Policy
1. Bypass HTTPS Scanning
URL Lists
2. Block certificate validation errors
URL Lists

Condition Name: URL Lists

Applies to:

● Any of the items selected below
○ Everything except for the items selected below

□ Select/Deselect all   Display Selected

□ Adware URL List
□ Allowed Large Download Sites
□ Allowed Large Upload Sites
□ Customer Defined Black List
□ Customer Defined Bypass List
□ Customer Defined White List
□ Emergency White List
□ Social Media Sites
□ Social Media Sites Allowed Requests
□ Spyware URL List
□ Trojan Activity Black List
□ Trusted Sites
□ Trustwave Recommended Black List
☑ Trustwave Recommended White List

<u>NOTE:</u> There are two important HTTPS Policy issues to be aware of:

1) If you configure a Bypass rule in your HTTPS Policy, it will bypass all Security Policies that might come after. As such, you can't, for example, exclude a URL from HTTPS inspection with a bypass, and then block it with a URL Filtering Security Rule. Thus a site that is deemed an adult or porn site will not get blocked by the Security Rules, if that site has triggered an HTTPS bypass rule.
2) All HTTPS traffic reaching the SWG HTTPS port is inspected by default. Effectively there is a hidden rule at the end of the HTTPS policy which says 'inspect all traffic'. If specific sites or categories need to be excluded from HTTPS inspection, you will need an explicit Bypass rule to do so.

About Trustwave®

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