# Symantec Web Filter - Admin Guide

2011-07-14

Michael Spence

**Audience:**

Currently this documentation is for the Network Administrator for APEagers. This document may be useful for Field Support and Helpdesk in analysing issues relating to the Symantec Web Filter. It is assumed that the user of this guide has knowledge of proxies.

**Preamble:**

This document describes the installation and configuration of the Client Side Proxy.

This document describes the installation and configuration of the Schemus Synchronisation Tool.

This document describes how to perform an on the spot synchronisation.

This document lists the Active Directory Security groups used.

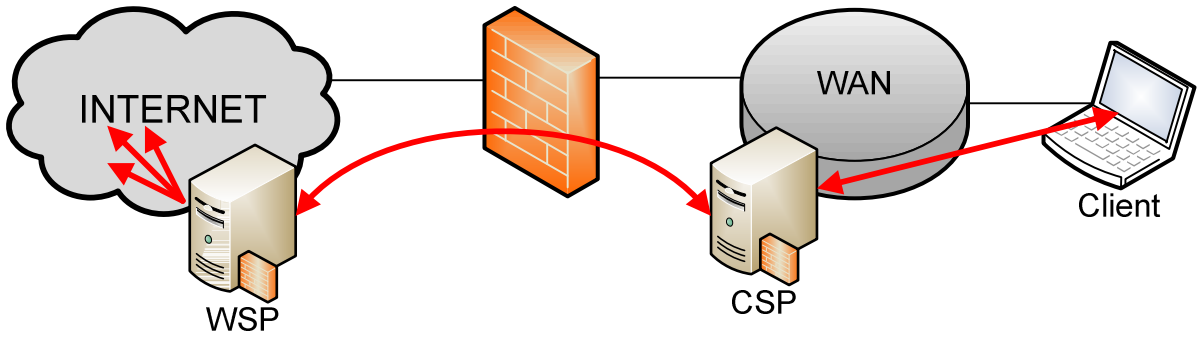
This document describes the use of the Symantec Online Portal for use with configuring rules.

**Topics of Discussion:**

**Topics in Detail**

## 1. General Overview

The Symantec Web Filter is a proxy for web browsers although not in the same manner as typical Microsoft ISA proxy servers. The system consists of a Client Side Proxy (CSP) and a Web Side Proxy (WSP). The CSP has access to the internal network and using this connectivity can gather information about the users, such as security groups. This information is synchronised with the WSP. As users attempt to access websites, their username is added by the CSP to their request and passed to the WSP. The WSP then filters the request based on the information it has about the user and the requested website.




## 2. CSP Setup

The CSP is essentially a squid proxy server with additional features to capture the AD user names of clients. This information is essential in identifying the user at the WSP.

### 2.a Installation

The installation files for the CSP can be downloaded from the Symantec.cloud Online Portal. Navigate to "Configuration" -> "Web Security Services" -> "Tools". From here download the "Client Side Proxy".

These downloads have been performed and at the time of this document the installation file could be found at:

```
\\gabbafs\it.data\Services\Symantec\CSP\csp_setup.exe
```

The installation is straight forward.

### 2.b Configuration

Some of the default configuration values installed with the CSP must be altered. The configuration files can be found at C:\ClientSideProxy\etc on the machine where installed.

The primary configuration file "squid.conf" contains the values which must be edited for an APEagers installation to work.

First configure the destination WSP. There are a number of commented "cache_peer" options at the top of the file. Uncomment the appropriate line, which pertains to the Asia-Pacific area (as this is the closest). This is the entry from the squid.conf file:

```
cache_peer proxy1.ap.webscanningservice.com parent 3128 0000 default
      no-query no-digest
```

Finally configure the internal Network. Near the middle of the file there are a number access list controls, denoted by "acl". An entry for the internal networks for the APEagers WAN must exist here to allow traffic to pass through. The entry added is:

```
acl our_networks src 10.0.0.0/8
```

Note the following rule which appears below the access lists, which denies traffic from any other source.

```
http_access deny !our_networks
```

### 3. Schemus Setup

The Schemus Tool is a program which interrogates the APEagers domain and based on configurable rules allows the upload of valid users of the CSP to the WSP system.

#### 3.a Installation

From the Symantec.cloud Online Portal the Schemus Tool can also be downloaded. This is entitled "Group Synchronization".

This download has been performed previously and the installation files can be found at:

```
\\gabbafs\it.data\Services\Symantec\Schemus\Schemus_windows_jre.exe
```

The installation of the tool is straight forward.

#### 3.b Configuration

To perform the Synchronisations with the WSP, the Schemus must be configured on how to interrogate the domain. These "rules" will need to be created.

Firstly start the Schemus Tool. If this is a new setup, create a configuration by pressing the "New" button at the top right of the screen. Give this configuration a meaningful name. Select the configuration and a summary of settings page will be presented.

The summary of settings is broken into two tabs; "Groups" and "Users".

#### 3.b.i Groups

To configure the security groups from AD which will be used to verify internet access, select the "Groups" tab and press "Modify". A "Schemus Groups configuration" window will be presented. Press "Next" to begin configuration.

Data sources are the locations where the Schemus Tool will pull information from. Multiple sources are allowed by ticking the "Multiple Sources" tick box. From the Source drop down list, choose "<add another source>" and select the source type "Microsoft Active Directory" from the source type drop down. Press "Next"

Enter details for an AD source on the next page. For the APEagers domain the following credentials have been supplied:

| | |
|---|---|
| Host Name: | `qld-dc1.apeagers.com.au` |
| Port Number: | `389` |
| Authentication: | `Simple & Plain` |
| User: | `apeagers\msadmin` |
| Password: | `***********` |

Configure the LDAP search to find groups within the domain. This location can be the root of the domain, but is simpler if it is configured to search the exact OU where the Internet Control Groups are located. The following is configured for the APEagers domain:

| | |
|---|---|
| Search base: | `OU=Computer Department,DC=apeagers,DC=com,DC=au` |
| Search scope: | `sub-tree` |
| Search filter: | `(objectCategory=group)` |
| Name: | `%DC[-1]%\\%sAMAccountName%` |

A Test search can be performed in the next step. This can help verify that you are searching the correct location for Control Groups in the domain.

Finally for the Data Source, select the appropriate Control Groups from the entire list of Groups found and move them across to the right list by pressing the ">" button. Ensure that "Include only member of included groups" is selected in the "Filter Users" drop down box.

The Data repository can be configured to use potentially other credentials, but should be automatically configured from the initial setup.

Notifications of the synchronisation can be sent via email to a user or distribution group if configured. McAfee anti-virus needs to be configured for the server to allow this program to send emails.

Ensure that the configurations have been saved.

### 3.b.ii Users

To configure the users from AD which will be able to use the CSP, select the "Users" tab and press "Modify". A "Schemus Users configuration" window will be presented. Press "Next" to begin configuration.

Similar to the Group configuration, create a Data Source for the Users to be configured.

Again the AD source must be configured, in the same way as for groups. However, be aware that due to the existence of sub-domains, this may cause a failure as the Schemus Tool traverses to the sub-domains, due to a difference in credentials. To stop this behaviour, click "Advanced" and change the Continuation References Action from "Follow" to "Ignore".

The LDAP search configurations should be set to the root of the domain, unless there is specific reason to select only a particular group within the domain. (Test groups were configured in this manner during the Beta testing of this product.)

Other options are straight forward and can essentially be ignored. Again ensure that the configurations made are saved.

### 3.c Syncronisation

The Schemus Tool is designed to Synchronise based on a predefined schedule. This schedule can be altered from the "Configuration->Schedule..." menu item.

The primary CSP "qld-csp" has been configured to update the WSP every 4 hours. During this period changes to users will not take effect.

A forced synchronisation can be performed up pressing the "Update" button on the left of the screen. A small window is presented which asks if groups or groups and users are to be updated. Select the appropriate option. Continuing from this, the tool will display the list of updated groups and users and will synchronise these with the WSP. (The "Test Update" button will simply display the groups and users that would be synchronised.)

Note: If the Schemus Tool is left open on the CSP then scheduled updates WILL NOT occur. The Schemus Tool should be close EVERY time you leave the server for an extended period of time.

## 4. Security Groups

The internet control groups created for use with the Symantec Web Filter are:

```
Internet L0 – No Access
Internet L1 – Manufacturer Only
Internet L2 – Whitelist Only
Internet L5 – Standard Access
Internet L7 – plus Social Networking
```

## 5. Online Portal

The Symantec.cloud online portal is the location that the WSP can be configured from. (It is also the area at which MessageLabs email filtering can be configured. Please avoid the MessageLabs area when dealing with the Web Filter.)

### 5.a Login

Navigate the online portal using the following address:

```
https://clients.messagelabs.com
```

The user name for this site is:

```
ape1248
```

and the security is currently set to Security Level 1.

From the dashboard, navigate to the "Configuration" -> "Web URL Filtering" section of the website.

### 5.b Rule Priority

Each of the rules is processed in order from the Top of the list to the bottom. If the groups and URL match for a request, the filtering stops at this rule and following rules are ignored. Using this feature, it is possible to create a layerd set of rules which can be matched to levels of access.

Rules can be moved up and down the list by using the arrow buttons on the right side of the table.

Also rules must be "Active" for them to take effect, by pressing the "Inactive" on the right of the rule definition, they become active.

### 5.c Rules by URL

The simplest of rules can be configured to act upon particular URLs. While editing a rule, click the "Specific URLs" tab. From the presented page, the list of currently configured URLs can be viewed. New URLs can be added here also. In most cases, it is the author's opinion that URLs are entered in the following format:

```
*.domainname
```

(For example *.holden.com.au NOT www.holden.com.au)

Ensure that specific URL filtering is enabled by selecting the "Use Specific URLs Below" radio button at the top of the page.

### 5.d Rules by Category

Symantec have attempted to categorise all websites on the internet. Be aware however that some of these categorisations are not immediately intuitive and a URL can be placed into more than one category.

Under the "URL categories" tab, select the categories which are to be acted upon.

Ensure that URL Category filtering is enabled by selecting the "Use URL Cateogries Below" radio button at the top of the page.

Also the portal provides a "URL Categorization" link, which will display the category(s) a URL is in.

### 5.e Rules by Groups

Bringing this back to the Schemus Tool, the rules can be configured to act upon groups of users. There are two types of groups "Custom Groups" (defined in the portal) and "Directory Groups" (uploaded by the Schemus Tool).

To apply a rule to a group, select the "Groups" tab. Under "Directory Groups", move the required groups from the "Available Groups" column to the "Assigned" column by pressing the "Add >>" button.

Ensure that Group filtering is enabled by selecting the "Use Groups Below" radio button at the top of the page.

## 6. Complications

By putting this system in place, a few complications have arisen. Primarily these issues are made evident due to the difference in methodology between the WSP and an internal web proxy (like ISA for example). With an internal proxy, the web request comes from the internal network. With the WSP the request is coming from the external proxy.

For the above reason sites which require our Public IP for validation, need to be updated with the IP of the Symantec proxy, or allowances on the firewall and the client browser need to be provisioned.

Also internal sites fail to function as they cannot for obvious reasons be routed to from the external WSP. Proxy exceptions for these sites must be added to the clients browsers.