



**Symantec Web Security**

# Web Security support guide

Version 1.0



## Contents

<b>1 Antivirus and Antispam setup guide .....</b>	<b>2</b>
Checking Symantec IP's.....	2
Checking the network address - What's my IP? .....	2
Setting the proxy in your browser to point directly to Symantec .....	2
Testing the Antivirus and Antispyware services.....	2
<b>2 URL Only Non-granular setup guide.....</b>	<b>2</b>
Checking Symantec IP's.....	3
Checking the Network Address .....	3
Setting the proxy in your browser to point to Symantec.....	3
Setting the URL Rules and Alerts .....	3
<b>3 URL Only Granular .....</b>	<b>3</b>
Checking Symantec IP's.....	3
Checking the Network Address .....	4
Requesting the Schemus tool.....	4
Installing and configuring the client site proxy .....	4
Proxy using a CSP on a different machine .....	4
Setting the proxy in internet explorer using a CSP on the same machine .....	4
Setting the URL Rules and Alerts .....	4
<b>4 Symantec Proxy Web Scanning .....</b>	<b>5</b>
Web Filtering without client side proxy .....	5
Client Site Proxy (CSP – Granular Filtering).....	5
Main Points.....	6
Squid Configuration file .....	6
Smart Connect Agent .....	7
<b>5 How to configure Web Filtering.....</b>	<b>7</b>
URL Filtering.....	7
Reporting.....	8
Web Routes.....	9
Roaming .....	9
HTTPS Inspection .....	10

# Setup

## 1 Antivirus and Antispam setup guide

### Checking Symantec IP's

Set the firewall rules using the IP's given by Symantec. Next test the firewall rules using Pings and a Telnet Session.

Please note, if you are not able to bring up a command window and perform a ping or Telnet session, you would need to visit Microsoft to search for instructions on how to fix this.

[Click here to view the tutorial](#)

### Checking the network address - What's my IP?

If the external IP of your network is not registered with the service, then the service will reject any traffic from that IP source. We can show you how to check your external IP by using [www.whatismyip.com](http://www.whatismyip.com) if necessary.

[Click here to view the tutorial](#)

### Setting the proxy in your browser to point directly to Symantec

The proxy settings of a test machine will be configured so that the web traffic from the machine is forwarded to the Symantec Infrastructure to be processed. The reason for performing the implementation on a test machine is to ensure that the rest of the machines on the network will not be affected.

[Click here to view the tutorial](#)

### Testing the Antivirus and Antispyware services

This test is to check the AntiVirus and Anti-Spyware services that you have bought which is part of the URL filtering. This will involve downloading a HTTP Anti-Malware test file. It is specifically for testing purposes. However, if for some reason the services fail to pick up the virus, then the file can be easily removed using standard network Anti-Virus software.

You do not have to perform this test if you do not wish to, Claranet SOHO is not responsible for any situation that might occur if you are not able to remove this file.

[Click here to view the tutorial](#)

## 2 URL Only Non-granular setup guide

## Checking Symantec IP's

Set the firewall rules using the IP's given by Symantec. Next test the firewall rules using Pings and a Telnet Session.

Please note that if you are not able to bring up a command window and perform a ping or Telnet session then you would need to visit Microsoft to search for instructions on how to fix this.

[Click to view the tutorial](#)

## Checking the Network Address

If the external IP of your network is not registered with the service, then the service will reject any traffic from that IP source. We can show you how to check your external IP by using [www.whatismyip.com](http://www.whatismyip.com) if you do not know it already.

[Click here to view the tutorial](#)

## Setting the proxy in your browser to point to Symantec

The proxy settings of a test machine will be configured so that the web traffic from the machine is forwarded to the Symantec Infrastructure to be processed. The reason for performing the implementation on a test machine is to ensure that the rest of the machines on the network will not be affected.

[Click here to view the tutorial](#)

## Setting the URL Rules and Alerts

This video will take you through the following:

1. URL Filtering
2. Alerts when a rule is triggered
3. Checking URL Categorisation

[Click here to view the tutorial](#)

## 3 URL Only Granular

### Checking Symantec IP's

Set the firewall rules using the IP's given by Symantec. Next test the firewall rules using Pings and a Telnet Session.

Please note that if you are not able to bring up a command window and perform a ping or Telnet session, you would need to visit Microsoft to search for instructions on how to fix this.

[Click here to view the tutorial](#)

## Checking the Network Address

If the external IP of your network is not registered with the service, then the service will reject any traffic from that IP source. We can show you how to check your external IP by using [www.whatismyip.com](http://www.whatismyip.com) if necessary.

[Click to view the tutorial](#)

## Requesting the Schemus tool

The Schemus tool is used to synchronise the Users and the Groups from the customer's Active Directory with the Symantec portal. The tool is free to download and is mainly used by customers who would like to apply specific rules to groups of users that they have setup in their Active Directory.

[Click here to view the tutorial](#)

## Installing and configuring the client site proxy

This video can be used as a guide to downloading, installing and configuring the Client Site Proxy tool. For the tool to work, the machine that the Client Site Proxy is installed onto will need access to a domain controller. It is recommended that the tool is installed onto a test PC first to ensure that it is compatible to work on the network.

[Click here to view the tutorial](#)

## Proxy using a CSP on a different machine

The web browser settings of a computer on the network will not need to point to the machine where the Client Site Proxy is installed. This traffic will then be passed on to Symantec to be processed via the proxy.

[Click here to view the tutorial](#)

## Setting the proxy in internet explorer using a CSP on the same machine

The browser settings for the machine that the Client Site Proxy is installed onto, will not be configured so that the traffic will be pointed to the proxy which we have just installed onto the machine.

This traffic will then be passed onto Symantec to be processed. The reason for performing the implementation on a test machine is to ensure that the rest of the machines on the network will not be affected.

[Click here to view the tutorial](#)

## Setting the URL Rules and Alerts

This video will take you through the following:

1. URL Filtering
2. Alerts when a rule is triggered
3. Checking URL Categorisation

[Click here to view the tutorial](#)

## 4 Symantec Proxy Web Scanning

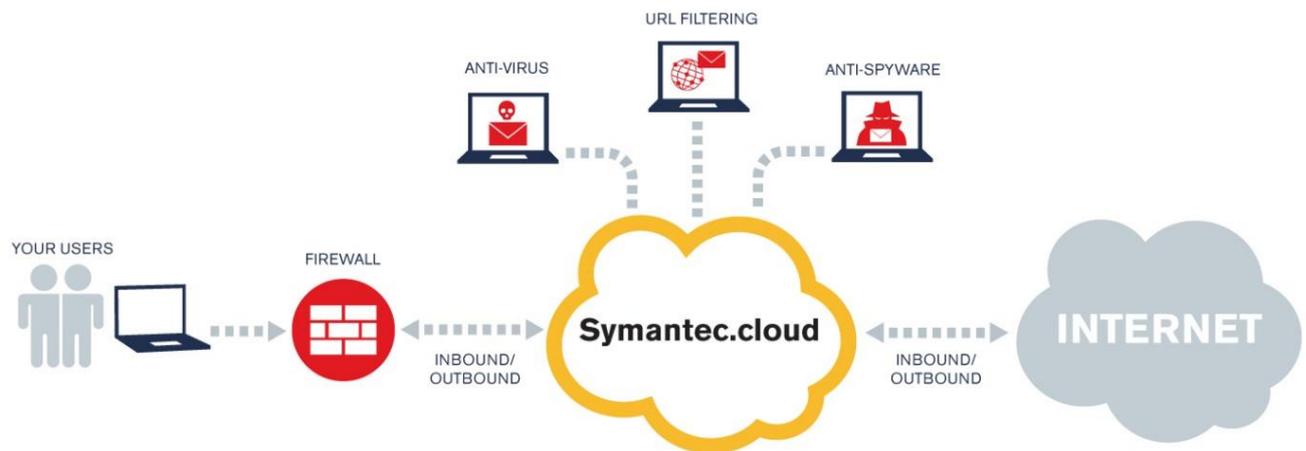
### Web Filtering without client side proxy

For Symantec to scan traffic, the firewall needs to be configured to accept any traffic through on port 3128 (web filtering traffic).

Users point their web traffic direct to the Symantec Cloud web proxy. Typically they would use the proxy address **proxy1.uk.webscanningservice.com over port 3128 (this is set in the users' internet browser)**.

Once it reaches the Symantec Cloud platform and the request is completed, it will then proceed to check against any current policies in place and will be scanned with Anti-Virus and Anti-Spyware to make sure the website is not malicious

The image below shows you the flow of the traffic that the devices take to get filtered.



### Client Site Proxy (CSP – Granular Filtering)

You are probably wondering if they can apply this to their browser, then what's the point of using a client side proxy? The truth is, using this is a big plus because they will be able to apply URL filtering rules to specific people or groups on their active directory.

They are also able to gain a detailed granular reporting which will show the web usage and who has accessed what and when. This can then be used with the company's policies about accessing non work related web sites.

Furthermore, they are able to use Schemus (Synchronization tool) which will require to be running a recent version of Java RunTime Environment for the device they intend to run this tool on.

This would be something the customer would need to configure themselves to allow it to connect to their active directory server; there is an admin guide in the help section of the Symantec portal which will guide them through the set up.

From the image below this shows the flow of traffic will take to get filtered, the web proxy will be some sort of device on their internal network that all the other computers will end up being directed through. This device can be

anything from an old laptop to a full server to run the proxy.

## Main Points

- You can install the CSP onto any local device and it doesn't need to be a server OS to be able run although it will need their Symantec log in and Active Directory Username and password with the correct permissions to query AD.
- The max number of users for this proxy is 300. This includes multiple sites so if there is other people logging on EX your network these will count towards the limit.
- There Configuration file for the CPS is called the squid.conf which is what contains the entire configuration of the CSP on their device.
- If they find that the Proxy isn't working due to a configuration error with the squid file, we can resend over a default Squid config file. If they ever require any assistance, we will require a copy of this to take to Symantec if need be.
- They will be able to download any of these tools from the Tools > Downloads section in their Symantec portal.
- They are able to set up URL filtering polices for the domain and they are able to install the Synchronisation tool (Schemus). This will allow them to connect to their Active Directory on their mail server, without the CSP it will then it would block across the whole network.

## Squid Configuration file

```
# WELCOME TO SQUID 2
#
# NETWORK OPTIONS
#
# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
#
# TAG: cache_peer
# cache_peer proxy1.ap.webscanningservice.com parent 1128 0000 default no-query no-digest
# cache_peer proxy1.eu.webscanningservice.com parent 1128 0000 default no-query no-digest
# cache_peer proxy1.us.webscanningservice.com parent 1128 0000 default no-query no-digest
# cache_peer proxy1.uk.webscanningservice.com parent 1128 0000 default no-query no-digest
# cache_peer proxy.us.webscanningservice.com parent 1128 0000 default no-query no-digest

# TAG: acl
# TAG: disable password on conf file
#cachemgr_passwd none config
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl ssl_ports port 443 563
acl safe_ports port 80 # http
acl safe_ports port 23 # ftp
acl safe_ports port 443 563 # https, snews
acl safe_ports port 70 # gopher
acl safe_ports port 210 # wais
acl safe_ports port 1025-65535 # unregistered ports
acl safe_ports port 280 # http-mgmt
acl safe_ports port 488 # gss-http
acl safe_ports port 591 # filemaker
acl safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl our_networks src 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 169.254.0.0/16
```

The upstream proxy the customer has enabled in the squid.conf (i.e proxy1.uk proxy1.eu etc)

Their LAN range(s) that are defined that the CSP will relay traffic for

N.B ACL = Access Control List they are used in many ways in the squid.conf

## Smart Connect Agent

Smarts connect is an additional service which is not free and the licenses are purchased per user which allows the users to connect to the Symantec Cloud while on or off the network.

Once this is downloaded and installed on the local machine, it will run the service and run the set up. You will find the license key for this in the downloads section where the agent was downloaded from.

### Smart Connect Agent ?



Web Security Smart Connect agent is a Microsoft Windows Service that dynamically discovers the endpoint machine's Internet connection environment. It then connects the user to the optimal Web Services infrastructure access point so that mobile users can safely browse the Internet.

Zip Version (Windows Server Group Policy Deployment)  
 Exe Version (interactive install/upgrade)

Licence key:  
Number of licences: 10

[Download](#)

This agent saves them from having to mess around by applying the proxy address and so when wanting to connect but off the network and it makes it much simpler. It will also just save the set up for when they next want to connect. Once installed, the agentconfigure.xml file (similar to squid.conf) needs to be configured.

The basic configuration would include entering the licence key for Smart Connect (available from the downloads section) and the upstream proxy servers to use. Here is what they will see when they first open up this config file.

```
<!--  
Licence Key  
  
Your licence key is available on ClientNet. Copy it and paste it  
here. Without a licence key, Smart Connect will not  
function.  
-->  
<license_key>00E3B3-E7BF-589F-9258B0-C162C8-79C54D</license_key>
```

## 5 How to configure Web Filtering

### URL Filtering

If you want to check over your web filtering rules you can do this all through the Symantec Portal, under the services tab you should see an option for Web Security and URL filtering from within there.

If you are unsure of what sort of category a website will be classed as (for example social media or news websites), you can use URL categorisation which will tell you exactly what the Symantec portal categorises that website as.

You are here: [Dashboard](#) > [Services](#) > [Web Security Services](#) > [Web URL Filtering](#) > [URL Categorization](#)

**URL Categorization**

The URL Categorization tool enables WSS administrators to enter a website address and obtain the list of categories based on the current URL database values. This tool is provided to assist with developing and understanding behaviour with respect to Web Services Policy Rules.

Please enter a website address below and click categorize to view the results:

**Categorize**

The URL belongs in the following category(ies):

**Category Name :** Dynamic

**Category Description :** Sites which have dynamically changing content with the possibility generating, displaying, or offering links to inappropriate material. Category includes search engines, directory services, hosting, portals. Sites which have dynamically changing content with the possibility generating, displaying, or offering links to inappropriate material. Category includes search engines, directory services, hosting, portals, and blogs

**Category Name :** Hosting Sites

**Category Description :** Sites which provide individuals or organizations with online systems for storing information, images, video, or any content accessible via the Web. Category includes free or paid hosting, virtual private server hosting, and online backup or file storage

If you believe this web site is not correctly categorized, please click the link below and submit a ticket to have the website reviewed.

**ReCategorize**

When you are in the URL filtering section, you can see the different rules that have been created and you can create, edit and delete all rules from here. One thing to make sure of if a rule doesn't seem to be working is in the far right column is that the rule is "Active" not "Inactive" otherwise the rule will do nothing.

You are here: [Dashboard](#) > [Services](#) > [Web Security Services](#) > [Web URL Filtering](#) > [Policy Rules](#)

**Policy Rules**

Create, edit or delete Web URL Filtering rules and determine the order in which rules are applied.

**New Rule**   **Delete Selected**   **Move To Position**      **Clear All Quotas**   **Clear Quotas for Selected**

Showing 1 - 3 of 3 policy rules

<< First | < Previous | Next > | Last >>

	Rule	Time	Groups	URLs	Content Types	Action	Change Priority	Rule Status
<input type="radio"/>	1 BBC Block	No	No	Yes	No	Block & Log	▲ ▼	Active
<input type="radio"/>	2 Website Allow	No	No	Yes	No	Allow & Log	▲ ▼	Inactive
<input type="radio"/>	3 Default Settings	No	No	Yes	No	Block & Log	▲ ▼	Inactive

<< First | < Previous | Next > | Last >>

## Reporting

From the reports section at the top, you are able to view what has been logged from the rules you have in place. For example, say a rule is set to block and log, if someone tries to access this website they won't be allowed access but there attempt to access this website will be logged in the reporting section for any admin users to view.

You are here: Dashboard > Reports > Report Requests

## Report requests

Refresh

[Request a new report](#)

Group by: [Activity](#) | [Privacy](#)

**Active report requests (1)** Collapse

Select: [Run Now](#) | [Delete](#) | [Clone](#) | [Rename](#) << < Previous Page **1** Next Page > >>

Next due	Repeat	Period	Format	Last modified by	Modified on	Recipients	Status
<input type="checkbox"/> <b>test</b> (Created by: Michael Prowse)	Once	06 Oct 2014 until 07 Oct 2014	PDF	Michael Prowse	17 May 2016	0	<span style="color: green;">●</span> <a href="#">Deactivate</a>
None	Once	06 Oct 2014 until 07 Oct 2014	PDF	Michael Prowse	17 May 2016	0	Expired

**Inactive report requests (0)** Collapse

Select: [Delete](#) | [Clone](#) | [Rename](#) << < Previous Page Next Page > >>

No report requests found. [Request a new report](#)

## Web Routes

Within the Web routes section this will show you IP addresses of the routes that have been registered with Symantec and that will get filtered. If you wish you purchase additional web routes here and view any change from the change log section.

You are here: Dashboard > Services > Web Security Services > Web Routes

**Web Routes**

**Web Routes**

The IP address range of each server used for web traffic must be registered

Status: ● At least one web route is registered

No new web routes can be added until additional capacity has been purchased.

**Registered Web Routes**

The web routes listed below are registered on the Symantec infrastructure. Web traffic sent via these routes will be filtered according to your Web Security Services configuration.

IP Address From	IP Address To	Date Added	Delete IP
123.123.123.123	123.123.123.123	28 Jul 2008	<a href="#">Delete</a>
213.165.148.196	213.165.148.196	10 May 2016	<a href="#">Delete</a>
89.206.156.217	89.206.156.217	01 Dec 2014	<a href="#">Delete</a>

[Download](#) [Add New](#)

[+ Web Route Fees](#)

[+ Change Log](#)

## Roaming

Within the Roaming section you can find your list of users which are enabled from the remote connect using the proxy server service. You can also enable and disable the remote connect option from here.

You are here: Dashboard > Services > Web Security Services > Roaming

**Remote Connect Agent**

**Settings** **Users**

Edit Remote Connect settings. You can navigate between Remote Connect configuration tabs without losing settings before submitting.

**Note: These settings only apply to the Remote Connect roaming solution. You cannot activate/deactivate users for the Smart Connect roaming agent solution using these settings.**

Enable/Disable Remote Connect Service

Enable Remote Connect  Disable Remote Connect

Password Expiry

Select number of days after which passwords will expire. **Never** ▾

You can navigate between tabs without losing settings before submitting.

**Save and Exit** **Cancel**

You are here: Dashboard > Services > Web Security Services > Roaming

**Remote Connect Agent**

**Settings** **Users**

Select Users to which policy will be applied while roaming. You can navigate between Remote Connect configuration tabs without losing settings before submitting.

Enter Keyword  **Search**

**Activate Selected** **Deactivate Selected**

Entries per page **20** ▾

Showing 0 - 0 of 0 << First | < Previous | Next > | Last >>

<input type="checkbox"/>	User	Email Address	Password	Active
<< First   < Previous   Next >   Last >>				

You can navigate between tabs without losing settings before submitting.

**Save and Exit** **Cancel**

## HTTPS Inspection

This section will scan any of the website that is using the filtering services and checks SSL encrypted traffic for anything that may be considered harmful. This will work in conjunction with your URL filtering rules as well.

You can set this to ignore particular SSL encrypted web traffic for websites or IP addresses from this screen by adding it in to the table. You can also allow access to sites which have been getting certification errors which otherwise would have been blocked. This will NOT warn the end user if they go to website that has been flagged with a certification failure.

You are here: Dashboard > Services > Web Security Services > HTTPS

## HTTPS Inspection

Configure and manage the scanning of SSL encrypted web traffic for your Web Security services.



### Scanning of SSL encrypted web traffic is currently ● On

HTTPS inspection scans SSL encrypted web traffic for malware, and includes the traffic in your URL filtering rules. To configure the service, you decide whether to block access to sites with certificate errors and whether to exclude sites from HTTPS inspection.

#### Ignore SSL encrypted web traffic – by URL category (0)

Select the URL categories that you want to exclude from HTTPS inspection. Any SSL encrypted Web traffic for the selected categories is not scanned for malware and is not included in your URL filtering rules.

No categories selected.

[Edit URL Categories](#)

#### Ignore SSL encrypted web traffic – by website or IP address (0)

Enter the sites that you want to exclude from HTTPS inspection. Any SSL encrypted web traffic for these sites is not scanned for malware and is not included in your URL filtering rules. Wild cards (such as \*.symantec.com and \*symantec.com) are allowed.

Select [New](#) | [Delete](#)

|< < Previous Page Next Page > >| [View 10](#) ▾

<input type="checkbox"/>	Website/IP address	Description	Active	Last updated
--------------------------	--------------------	-------------	--------	--------------

There are currently no Website/IP addresses entered

#### Allow access to sites with certificate errors (5)

[Edit User Alert](#)

Enable site bypass list

Select the Enable site bypass list check box to add sites to the list below. Sites that are 'active' can be accessed by users. Note that users will not be warned if a certificate error is detected by our service.

Select [New](#) | [Delete](#)

Showing 1 – 5 of 5 |< < Previous Page 1 Next Page > >| [View 10](#) ▾

<input type="checkbox"/>	Website/IP address	Description	Active	Last updated
<input type="checkbox"/>	89.206.174.179		<span style="color: green;">●</span> On	01 Dec 2014 9:36 AM
<input type="checkbox"/>	google.com		<span style="color: green;">●</span> On	01 Dec 2014 9:23 AM
<input type="checkbox"/>	mail.google.com		<span style="color: green;">●</span> On	01 Dec 2014 9:17 AM
<input type="checkbox"/>	my.star.co.uk		<span style="color: green;">●</span> On	01 Dec 2014 9:23 AM
<input type="checkbox"/>	www.google.com		<span style="color: green;">●</span> On	01 Dec 2014 9:23 AM