

# WebDefender Enterprise

## Step by step Getting Started guide



### Step 1 - Plan your filtering structure

Call the intY Technical Support Team and decide how you want your end users to be allocated to filtering groups. We recommend using the primary OU's on your Active Directory as the group names.

Tick box when done



### Step 2 - Export your Active Directory

Export your Active Directory to a CSV file so intY Support can import all the users into WebDefender. Here's the procedure to export your Active Directory user list:

- Open a command prompt and cd to the system32 directory.
- Type the following line then press return.
- `csvde.exe -r "(objectClass=user)" -n -f ad_dump.csv`

This will dump the AD user list to a file called **ad\_dump.csv** in the system32 directory.

**Email this file to support@inty.net** along with your contract ID and we will import your users into WebDefender

Tick box when done



### Step 3 - Customise Active Directory (if reqd.)

If you chose to use your primary OU in Step 1 proceed to Step 4.

If this was **not** chosen for your filtering groups then you need to decide which users need to go in which groups.

Our Support team will have sent you back a simplified Active Directory user list. Amend this for each user by indicating which WDFe group should be assigned to. Send us the completed list.

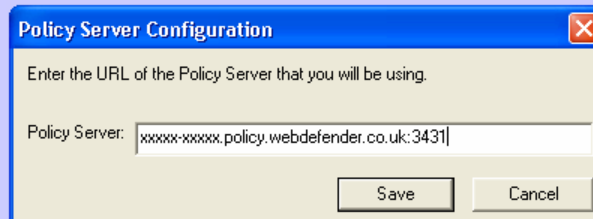
Tick box when done







## Step 4 - Test the installation and firewall access

Put the WDFe client on to a number of test PCs. Install the client manually on the PCs by double clicking on the WDFe client installer.

During the installation you will need to enter your unique policy server URL followed by “:3431”. Your unique policy server is included in your welcome email. See the screenshot below for details of how this will look during the installation.



**NB. Following the above step is vital to deliver correct filtering.**

-  This icon will appear in your system tray after the client is installed.
-  The icon will appear to spin round when a web request is made .
-  A no entry sign is shown when a request is being blocked.
-  If you are seeing a yellow warning symbol with an exclamation mark in the system tray check the following:-

- Ensure that you have allowed the WebDefender client (nsfx.exe) access out through your PC's firewall.
- Check that TCP port 3431 has access to the internet from your network:-
  - This can be tested by opening a command prompt and typing the following and pressing return:  
**telnet test.policy.webdefender.co.uk 3431**
  - The command prompt screen should go blank. Press return a few times and if you see the policy server returning “**Error - - 0**”, the test is successful.

If you are still experiencing problems *after* ensuring that your desktop and network firewalls are allowing outbound connection attempts on TCP port 3431 by following the steps above, please contact the intY Technical Support Helpdesk on **0870 124 4689** or via email at **support@inty.net..**

Tick box when done

# WebDefender Enterprise

## Step 5 - Test default web filtering

Test the operation of filtering by browsing to sites that you believe should and shouldn't be blocked. (By default *weapons* and *pornography sites* are blocked.) You can also test out the application blocking, URL and keyword filtering. For details how to configure application blocking and URL / Keyword filtering please see the **WebDefender Enterprise Admin Guide**. Details of this are in your welcome email.

For more details on this please contact the intY Technical Support Helpdesk.

Tick box when done



## Step 6 - Create a Web Filtering Policy

Create your first policy and apply URL category to a filtering group. Test it works correctly for users of that group. **See P 1-6 in the Admin Guide**

Create as many policies as you need for the operational groups in your organisation and apply them to the relevant filtering groups.

For more details please view your WebDefender Admin guide or contact our Technical Support Helpdesk.

Tick box when done



## Step 7 - Roll out the client to all users

Roll out the WebDefender client to all PCs. You can install the WebDefender client manually on each PC or install using Active Directory.

The EXE client can be installed via Active Directory by using a login or logout script. For more details please visit the Microsoft website.

<http://technet2.microsoft.com/WindowsServer/en/library/e9028566-1be7-45f8-a219-6b09dce34f8d1033.mspx>

The MSI version of the client can also be installed via Active Directory using a group policy object.

Please see Microsoft's support page for more information regarding the Group Policy Object installation.

- For windows 2000 visit <http://support.microsoft.com/kb/314934>
- For windows 2003 go here <http://support.microsoft.com/kb/816102/en-us>

Tick box when done



## Step 8 - Proxy your site traffic for virus scanning

Proxy browser traffic through WebDefender. If you currently using a proxy sever on your site configure it to send Internet browser traffic to **wdfproxy.inty.net** on TCP port 3128. If you do not use a proxy server on site simply set your Internet browser's proxy to point to **wdfproxy.inty.net** using port 3128.

Tick box when done



## Step 9 - Use reporting to check policy operation

WebDefender has pre-configured reports to display web usage. You can also set up your own customised reports for tracking virtually any type of online activity.

See the *WebDefender Enterprise Reporting Guide*, details of which will be in your welcome email.

Tick box when done



## Step 10 - Refine your Internet Policy

By regularly reviewing reports you can monitor web activity to assess how well your policies are performing. The *Email Sending Conditions* facility allows sophisticated tracking of key performance thresholds, so you maintain proactive control of network usage

Apply this process as you use WebDefender to ensure your filtering requirements are always satisfied.