



# Quick Start Guide

Version 3.50

## Introduction

There are 7 easy steps to configuring WebTitan, which will be described in further depth in this guide.

### 1: Install the License

You require a valid license from WebTitan. This can be obtained from [www.webtitan.com](http://www.webtitan.com)

### 2: Wait for the URL Database to Download

Once the license has been installed the URL database will automatically download. This will take up to 30 minutes depending on the speed of your connection. The size is roughly 500MB

### 3: Import Users and Groups from Active Directory or LDAP

You will need the IP address of Active directory or LDAP

### 4: Create Custom Policies

Initially all groups will be assigned the Default policy and if a user is a member of multiple groups the most permissive policy will apply

### 5: Set up WebTitan Authentication

For NTLM authentication i.e. Windows Domain Log on, you need. Domain Name, Domain Controller name and IP username and password with sufficient something

### 6: Automatic Proxy Configuration

User's browsers can be configured to automatically use WebTitan by the Group Policy proxy setting on your Windows server or using a WPAD file.

### 7: Check WebTitan is Filtering Traffic

Once you've completed the above steps you can check that WebTitan is operating correctly by viewing real time viewing activity via Reporting History.

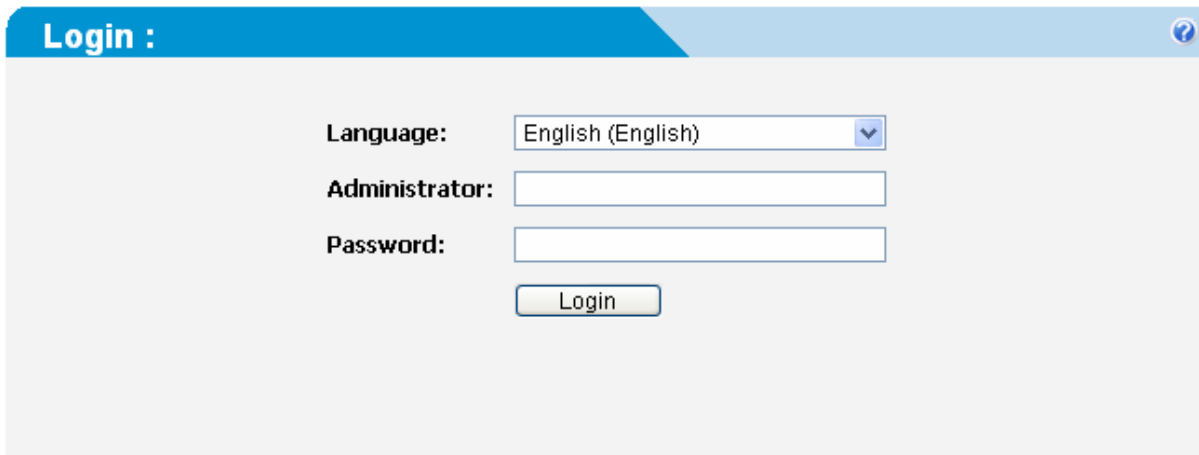
WEBTITAN SUPPORT ARE HERE TO HELP

- Web: <http://www.webtitan.com/>
- Knowledge Base: <http://getsatisfaction.com/webtitan>
- Telephone: +353 91 540054
- Email: [support@webtitan.com](mailto:support@webtitan.com)

# 1. Install the License

Before WebTitan can be configured to filter web traffic you require a valid license. Once you have received the license by e-mail, you log on to WebTitan by first going to the URL you gave to WebTitan during installation and entering the required Login fields as follows

Administrator: admin  
Password: hiadmin



**Login :**

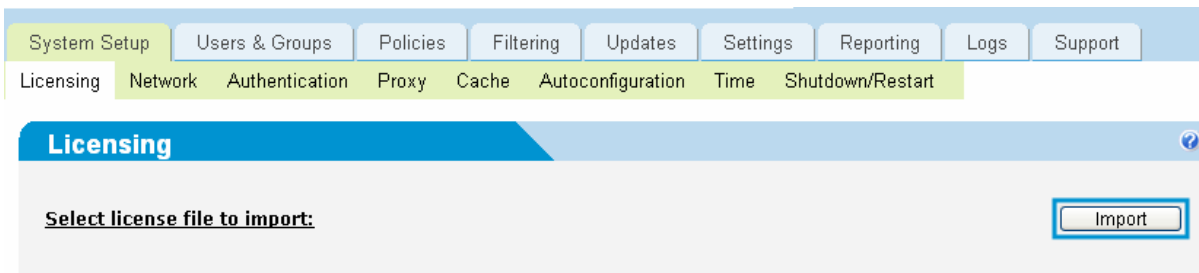
**Language:** English (English) ▼

**Administrator:**

**Password:**

Login

Then navigate via the tabs to System Setup -> Licensing. Click “Select License File to Import” and browse to where you have saved the license and then click IMPORT.




System Setup Users & Groups Policies Filtering Updates Settings Reporting Logs Support

Licensing Network Authentication Proxy Cache Autoconfiguration Time Shutdown/Restart

**Licensing**

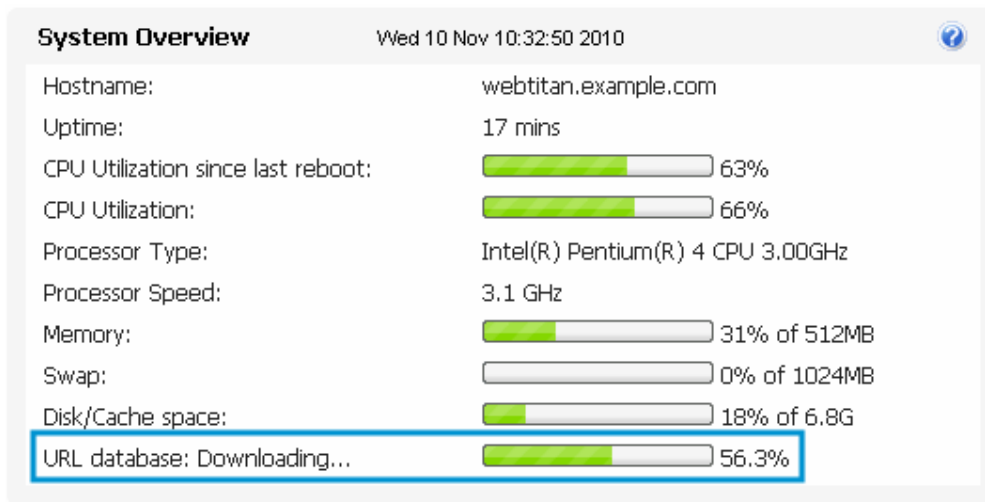
Select license file to import:

 Note: Listed below are the minimum versions of the following browsers required to view the WebTitan web based GUI

- Internet Explorer 8
- Firefox 3.5
- Google Chrome 6
- Apple Safari 5
- Opera 10.63

## 2. Wait for URL database download

Once the license has been validated, WebTitan will begin to download the URL database which contains a list of millions of URLs and their categorization. This is a one-time operation and will take about 20-30 minutes depending on your Internet speed. The file size is roughly 500 MB. This a once off download. The URLs will be updated every night with the download of a smaller file.



The status of the database download can be checked on the 'System Overview' section of the Dashboard (The dashboard is available for selection in the top right of the UI). When completed, the version number of the database and date will appear. When the download is complete you can then proceed to configure your user's browsers to use WebTitan as their proxy.

While you are waiting for the URL database download to complete you can proceed to step 3.

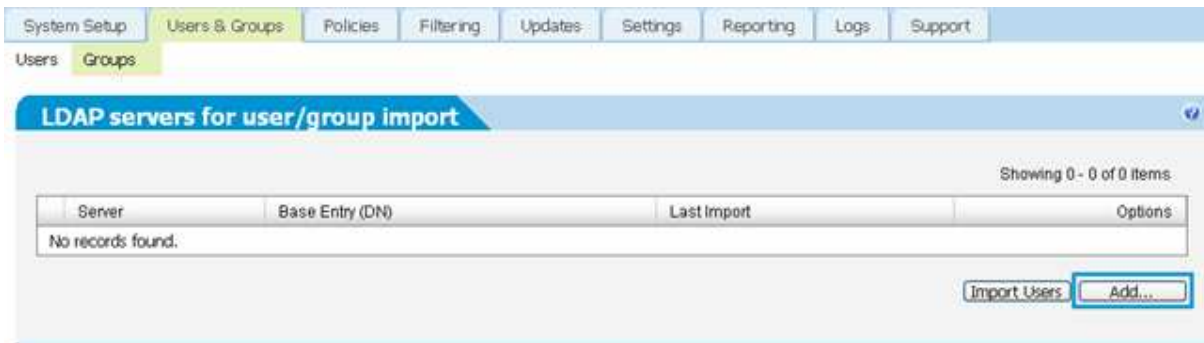
### 3. Import Users and Groups from Active Directory or LDAP

Note: If you will not be using LDAP or Active Directory the instructions to manually set up users and groups can be found in the administrators guide.


You will need the IP address of Active directory or LDAP sever.

#### ***LDAP user/group importation***

To import users and groups in WebTitan, navigate to the Users & Groups > Users tab which appears as follows.



Click the 'Add' button under 'LDAP servers for user/group import'. You will then be prompted to input the details of your LDAP server. The following screenshot provides a sample entry.

 Please note that your password must not contain the '£' character

## Sample Entry

The screenshot shows a dialog box titled "Add LDAP Server" with the following fields and values:

- LDAP server: 10.0.0.150
- Base entry (DN): dc=company,dc=local
- Server login user: admin@company.local
- Server login password: ••••••
- Enable multi-domain support:
- Domain: (empty)
- LDAP Server Type: Open LDAP
- Disable group imports:
- Enable periodic import:
- Import frequency: 24 hours

Buttons: Save, Cancel

Note that the following options are available when configuring the LDAP server settings which are as follows

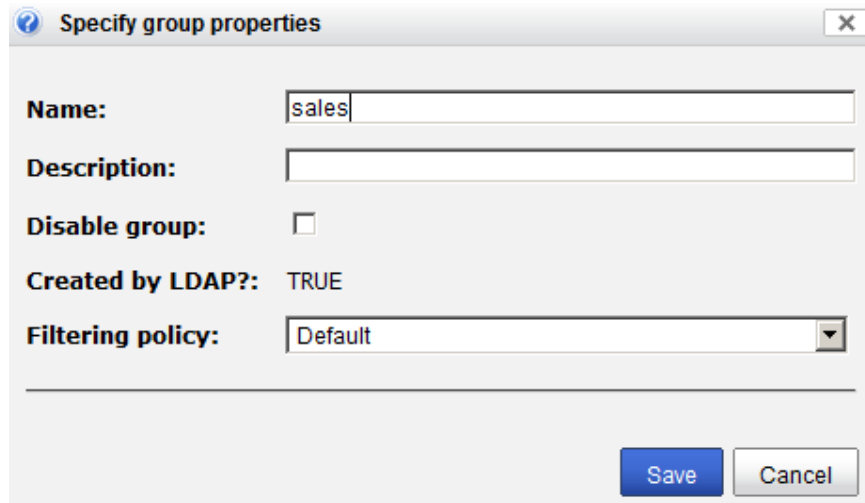
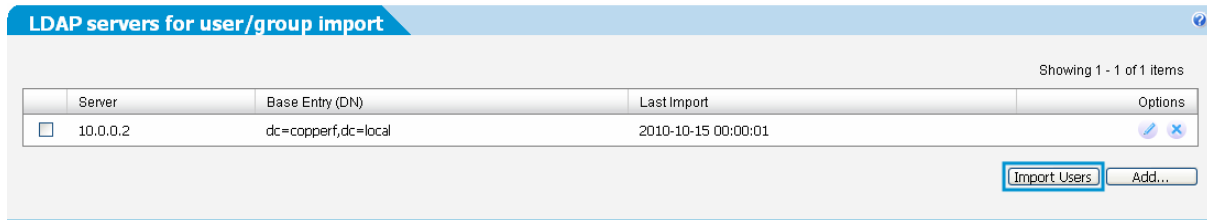
- Enable multi-domain support. i.e. Do you want WebTitan to filter web traffic over multiple domains. Enter the domain name in the succeeding Domain field.
- LDAP server type. i.e. is it Open LDAP, Active Directory server or Novell eDirectory.
- Disable group imports. i.e. Just import the users.
- Enable periodic imports. i.e. Update WebTitan periodically with any LDAP changes made.

When importing, you can use more specific Base entries (DN). The Base entry distinguished name (DN) as configured on the LDAP server. The entry serves as the starting point of the LDAP directory search. E.g.

- Import everything: dc=your.company,dc=local
- Just import a specific user: cn=joe smith,cn=users,dc=your.company,dc=local
- Import an organizational unit: ou=test\_org\_unit,dc=your.company,dc=local

When the server settings are saved, they are then authenticated automatically. Upon successful authentication, the server will then be available for importation of users and groups. To import the

LDAP server users/groups, select the checkbox beside it and click the 'Import Users' button as shown below. Upon successful importation a screen similar to below will be seen with the users and/or groups available under the 'Users' section of the same tab.



Note: the users imported are automatically assigned to their associated LDAP server group if they have been selected for importation also. Also note that any imported groups are automatically assigned to the 'Default' policy.

## **LDAP Import Trouble Shooting**

If you are having issues connecting to your LDAP server, you can test further by downloading the free Softerra LDAP server at <http://www.softerra.com/products.htm>. This is a free product for all types of usage including commercial. You can then test connecting to the Softerra product which will help determine whether your initial LDAP settings were correct or if it was an external issue.

The following error codes returned by WebTitan when validation of the LDAP settings fails could be of use.

<b>Error Code</b>	<b>Explanation</b>
-1	Server couldn't be reached or port 389 was not open.
-2	LDAP bind error.
-3	Couldn't perform the search.
-4	Possible username/password error.
-99	There's no such server id.



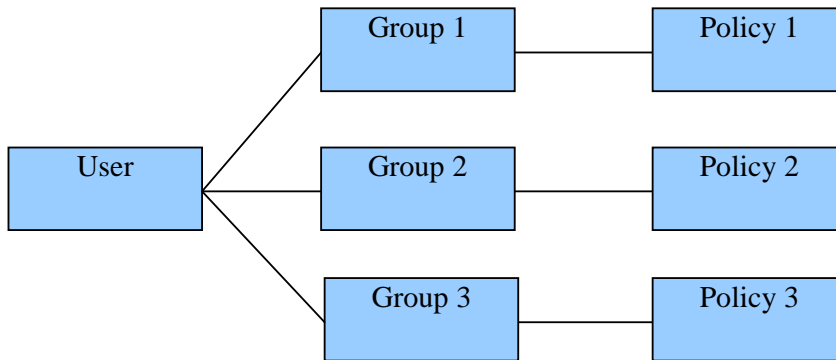
### **Rules to remember about LDAP user/group importation**

- You cannot change the names of LDAP imported users or groups.
- If you delete the LDAP server from WebTitan, all users and groups associated with that server will be automatically deleted.
- Users/Groups reimported from an LDAP server by either manually reimporting them or through a periodic import will overwrite all changes made to the existing users/groups imported.
- If a user doesn't have a group it will be in the default group all groups will be given the Default policy initially.

## 4. Create Custom Policies

The basic premise of policies in WebTitan is

- A user is assigned to one or more groups.
- A policy is assigned to a group, each group can have only one policy.
- By default it is the least restrictive setting of the combined policies assigned to a user that will apply although this can be changed to least permissive policy from the 'Policies>Global Settings' tab.



This step outlines how to create and link users, groups and policies. It also demonstrates where filtering is set up within WebTitan and concludes with showing how web browsers can be configured to use WebTitan.

### **Policies**

A group can only be assigned to one policy. The policy allows a groups behaviour to be controlled. To create a policy, go to the Policies > Filtering Policies tab and click 'Add Policy'. This screen can be seen below.

Policy	Description	Options
Administrators	Slightly relaxed policy for administrators	
Default	Default filtering policy	
Deny everything	Policy that blocks everything	

When 'Add Policy' has been selected, the policy can then be defined by browsing through the selection of tabs available such as 'Non-working times', 'Categories', 'Web-filter', 'File types', 'Safe Search' and 'Notifications'.

**New Policy**

Name Non-working times Categories Web-filter File types Safe search Notifications

Name: Demo Policy

Description: Demo Policy

Groups:

Save

Once the policy is saved it is immediately available for use by the groups and therefore also by the users. Best practice might be to create the policies first followed by the groups and then the users. But this is at the user's discretion.



### **Rules to remember about users, groups and policies**

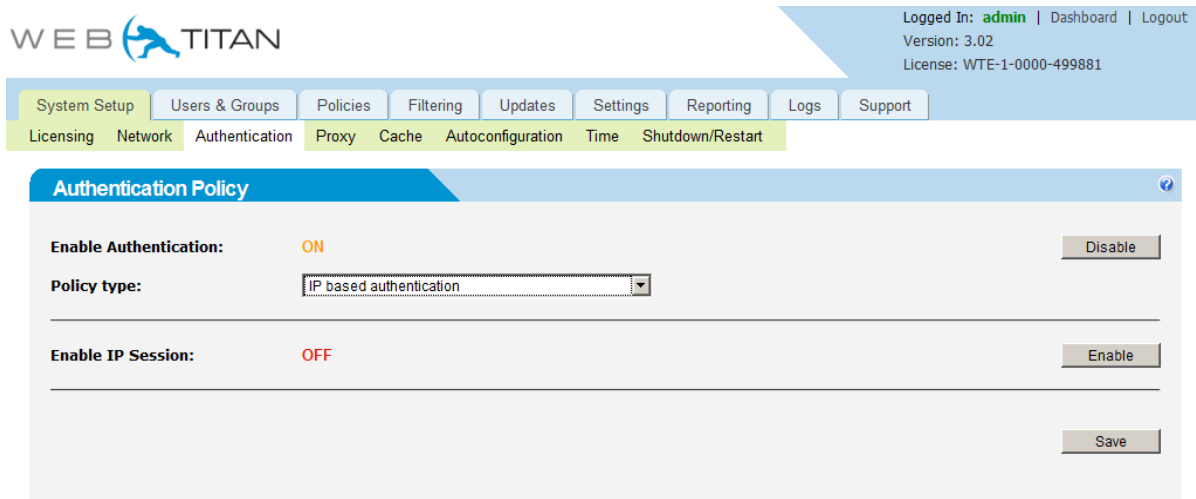
- A user can be assigned to one or more groups.
- A group can be assigned to one and only one policy.
- It is the most permissive setting of the combined policies assigned to a user that will apply unless you change this option at the 'Settings > Global Settings' tab.

## 5. Set up WebTitan Authentication

WebTitan provides the option to define how users authenticate themselves to WebTitan before accessing external web sites.

By default, authentication is disabled, which means that any user is accepted by the WebTitan appliance without authentication. Should authentication be required, it can be enabled via the System Setup > Authentication tab which can be seen below. The method of authentication can be selected from the 'Policy type' drop down list. WebTitan provides 5 methods of user authentication which are as follows.

- NTLM (NT LAN Manager) based authentication, which is Windows Domain log on.
- IP and NTLM based authentication, in which users are authenticated by IP or NTLM as described below.
- LDAP based authentication
- IP and LDAP based authentication, in which users are authenticated via IP or LDAP methods as described below.
- IP based authentication



The screenshot displays the WebTitan Administration Console interface. At the top left is the 'WEB TITAN' logo. On the top right, it shows 'Logged In: admin | Dashboard | Logout', 'Version: 3.02', and 'License: WTE-1-0000-499881'. Below this is a navigation menu with tabs for 'System Setup', 'Users & Groups', 'Policies', 'Filtering', 'Updates', 'Settings', 'Reporting', 'Logs', and 'Support'. Under 'System Setup', there are sub-tabs for 'Licensing', 'Network', 'Authentication', 'Proxy', 'Cache', 'Autoconfiguration', 'Time', and 'Shutdown/Restart'. The 'Authentication Policy' page is active, showing the following configuration:

- Enable Authentication:** ON (with a 'Disable' button)
- Policy type:** IP based authentication (selected in a dropdown menu)
- Enable IP Session:** OFF (with an 'Enable' button)
- A 'Save' button is located at the bottom right of the configuration area.

IP based authentication and NTLM based authentication are transparent to the user, whereas LDAP based authentication will require the user to enter their LDAP username/password credentials on commencing web site browsing. They will only be asked once for this information.

Below describes how to set up WebTitan for each different method of authentication.

## NTLM based authentication

If your network uses NTLM authentication, then the NTLM users can be transparently authenticated against the WebTitan web filter using their Microsoft Windows credentials when they log on to the network.

To facilitate NTLM based authentication within WebTitan, the following must be done.

- NTLM based authentication must be enabled via the System Settings > Authentication tab.
- Users must browse using Internet Explorer, Mozilla Firefox or Google Chrome.

The screenshot below provides a sample NTLM server setting. Authentication of the settings occurs automatically once the 'Save' button is clicked.

The screenshot displays the 'Authentication Policy' configuration page in the WebTitan interface. The page is divided into several sections:

- Enable Authentication:** Set to **ON** (green text). A **Disable** button is visible to the right.
- Policy type:** A dropdown menu is set to **NTLM based authentication**.
- Enable IP Session:** Set to **OFF** (red text). An **Enable** button is visible to the right.
- NT domain name:** Text input field containing **company**.
- Primary domain controller name:** Text input field containing **DCName**.
- Primary domain controller IP address:** Text input field containing **10.0.0.2**.
- Backup domain controller name:** Empty text input field.
- Backup domain controller IP address:** Empty text input field.
- Username:** Text input field containing **administrator**.
- Password:** Password input field with masked characters (\*\*\*\*\*).
- Number of NTLM authenticators:** A dropdown menu set to **10**.

A **Save** button is located at the bottom right of the configuration area.

If your NTLM server does not authenticate successfully, the following error codes returned by WebTitan could be of use.

Error Code	Explanation
-1	NTLM authentication isn't enabled.
-2	The username or password was not correct.
-3	Can't connect to domain controllers.
-4	/usr/local/bin/net join command failed with another reason.
-5	winbindd is not working(wbinfo -p).
-6	winbindd is not working correctly (wbinfo -t).

#### NTLM authentication points

- NTLM based authentication will be transparent to the end user.
- NTLM based authentication only works with Internet Explorer, Mozilla Firefox and Google Chrome.
- Users who do not match any NTLM user account will automatically be controlled by the 'Default' policy and will appear in reports as the 'GDefault' user.

### ***LDAP based authentication***

LDAP authentication is suitable for where the users and groups are being managed by an LDAP server and where it is preferred that the user must enter their LDAP username/password credentials on commencing web site browsing.

To facilitate LDAP based authentication within WebTitan, the following must be done.

- LDAP based authentication must be enabled via the System Settings > Authentication tab.
- There must be at least one LDAP server specified in the Users & Groups > Users tab\*.
- The users associated with the authenticating LDAP server must be imported into WebTitan\*.

Below is a screen shot of LDAP based authentication turned on within WebTitan, which is then followed by a screen shot of a user being prompted for their LDAP credentials. They are only required to enter these credentials once.

System Setup | Users & Groups | Policies | Filtering | Updates | Settings | Reporting | Logs | Support

Licensing | Network | Authentication | Proxy | Cache | Autoconfiguration | Time | Shutdown/Restart

### Authentication Policy

**Enable Authentication:** ON Disable

**Policy type:**

---

**Enable IP Session:** OFF Enable

**IP Session TTL (mins):**

---

**Number of basic authenticators:**

✔ Success: Authentication policy saved

Save

**Authentication Required** ✕

The proxy 10.0.0.182:8881 is requesting a username and password. The site says: ""

User Name:

Password:

OK Cancel

If the web user enters an incorrect username or password, then they will receive the following web page.

## Access Denied

You have attempted to access the following web page:

<http://helpdesk.webtitan.com/index.php/tickets>

Access has been blocked because:

Authentication failed - username or password incorrect

Management have deemed that access to this web page is inappropriate at this time. Please contact your supervisor if you feel that this is incorrect.

---

*Generated on Mon, 23 Nov 2009 15:29:05 +0000*



### LDAP authentication points

- LDAP based authentication requires the end user to enter their LDAP credentials

### ***IP based authentication***

IP based authentication is only suitable where the users have static IP addresses. Also, it is recommended that either LDAP or NTLM authentication is used where LDAP servers are being used to maintain the users and groups within WebTitan. To facilitate IP based authentication within WebTitan, the following must be done.

- IP based authentication must be enabled via the System Settings > Authentication tab.
- Users must be assigned IP addresses via the Users & Groups > Users tab. An IP address can be assigned at the time of user creation or by editing an existing user. The screen shot below shows that users can be assigned both a single IP address or an IP address range.

**Add User** [Close]

**Username:**

**Fullname:**

**Description:**


**Managed via LDAP:** No

**IP Addresses:**

		Add
1	10.0.0.62	X
2	10.0.0.130-10.0.0.155	X

**Groups:**

Available	Selected
Default	
Administrators	
Sin bin	
org_group	

 IP authentication points

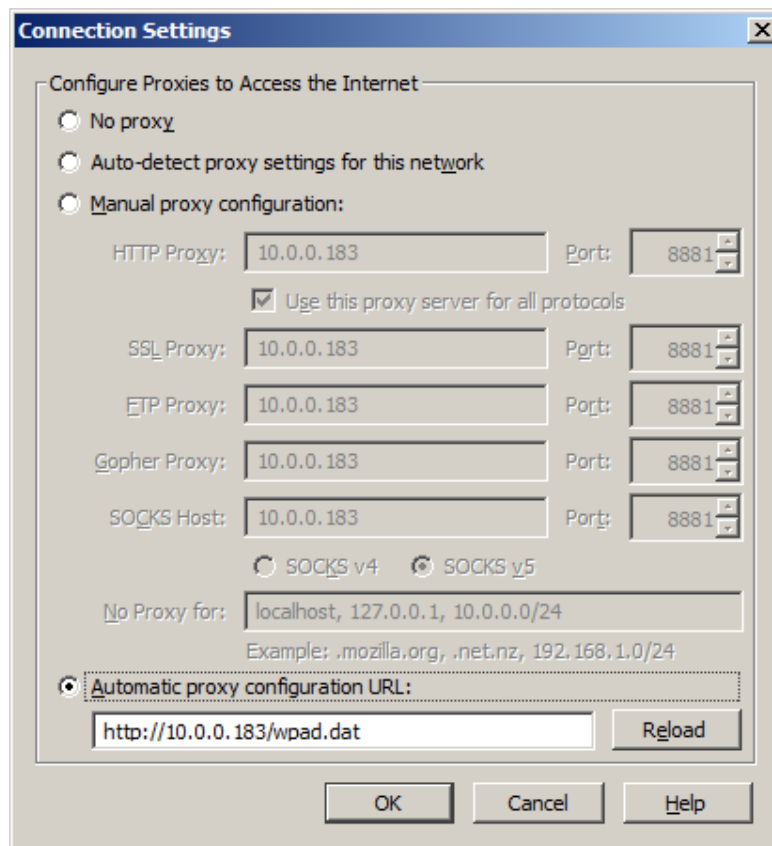
- IP based authentication will be transparent to the end user.
- IP based authentication should only be used for static IP addresses.

## 6. Automatic Proxy Configuration

Internet browsers can be guided to use WebTitan by configuring the web browser settings. This can be done by

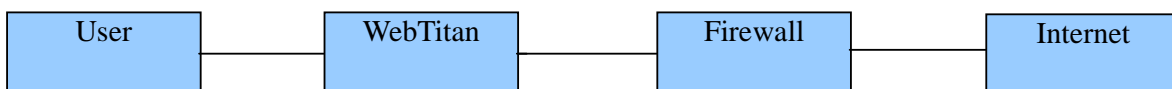
- Manually setting the proxy configuration
- Automatically detect the proxy settings for the network.
- Providing a URL to a wpad.dat file which contains the network proxy settings.

Below is a screen shot of potential settings for the Mozilla Firefox browser.



Automatic detection and automatic proxy configuration both require the use of a wpad.dat file.

### Example of a Network

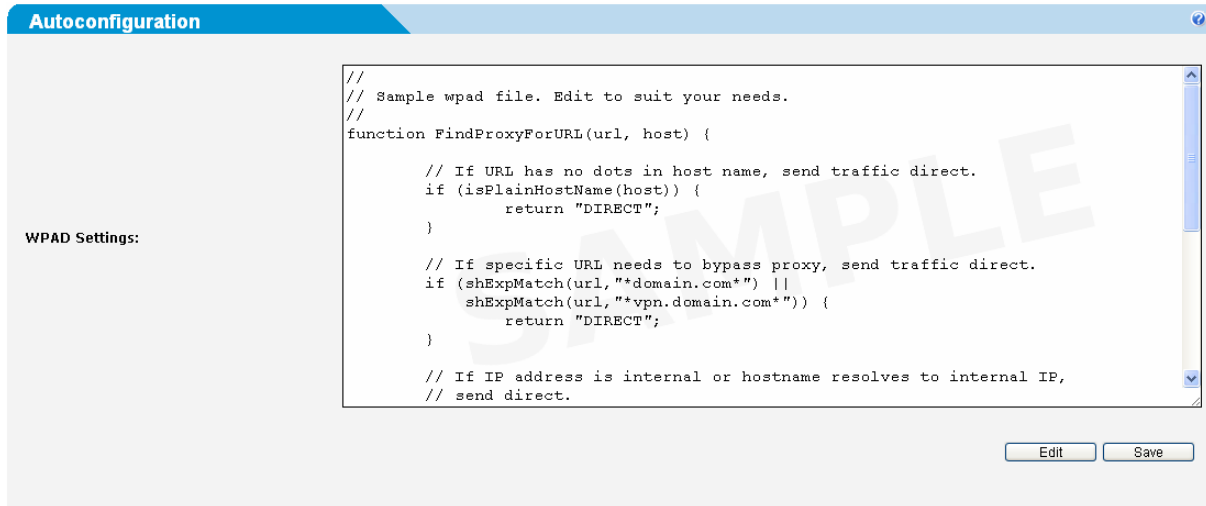


### Loading a wpad.dat file in WebTitan

A WPAD.dat file can be loaded up by WebTitan by going to the System Setup > Autoconfiguration tab which can be seen in the screen shot below.

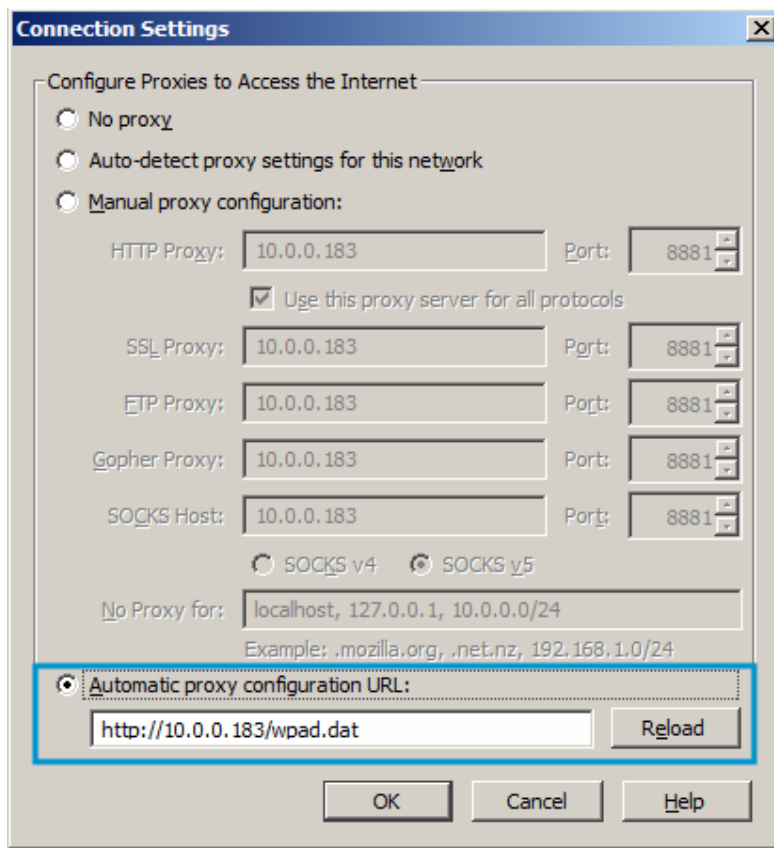
To create a wpad.dat file, click on the 'Edit' button below the dialogue box, you may now edit its contents. Copy and paste the wpad file you wish to use into this box and then click the Save button to save these settings to the WebTitan system.

A sample WPAD file with descriptive comments is provided in the System Setup>Autoconfiguration tab, which can be edited to suit your configuration requirements.



### ***Automatic proxy configuration URL***

Once you have uploaded your wpad file on to WebTitan, you can set the browser to directly pick up your proxy configuration by entering the URL for WebTitan and the path to the wpad.dat file as shown below.



### ***Auto-detect proxy settings***

If you wish the browser to auto-detect the proxy settings, you need to amend your DNS settings and configure an alias for the WPAD entry.

e.g. You could add the following as a DNS alias

10.0.0.131 WPAD



If setting up WPAD using DNS on a Windows Server you may need to remove wpad from the dns global black list. To check if it's on the blacklist from a command window on your Windows Server type: `dnscmd /info /globalqueryblocklist`  
To remove see <http://technet.microsoft.com/en-us/library/ee649158%28WS.10%29.aspx>.

## ***Use Group Policy to set User's Proxy Settings for Internet Explorer***

On your Domain Controller select the Group Policy Editor, and then navigate to User Configuration > Windows Settings > Internet Explorer Maintenance > Connection > Proxy Settings, from here you can configure the IE proxy settings for all users in your domain.

### ***Links***

- Click here: <http://technet.microsoft.com/en-us/library/cc995062.aspx> for how to create a WPAD entry in DNS.
- Click here: <http://support.microsoft.com/kb/968732> for the effect that a security update has for DNS settings on Windows 2003 Server.
- Click here: <http://en.wikipedia.org/wiki/Wpad> for further information on the Web Proxy Auto-Discovery Protocol.

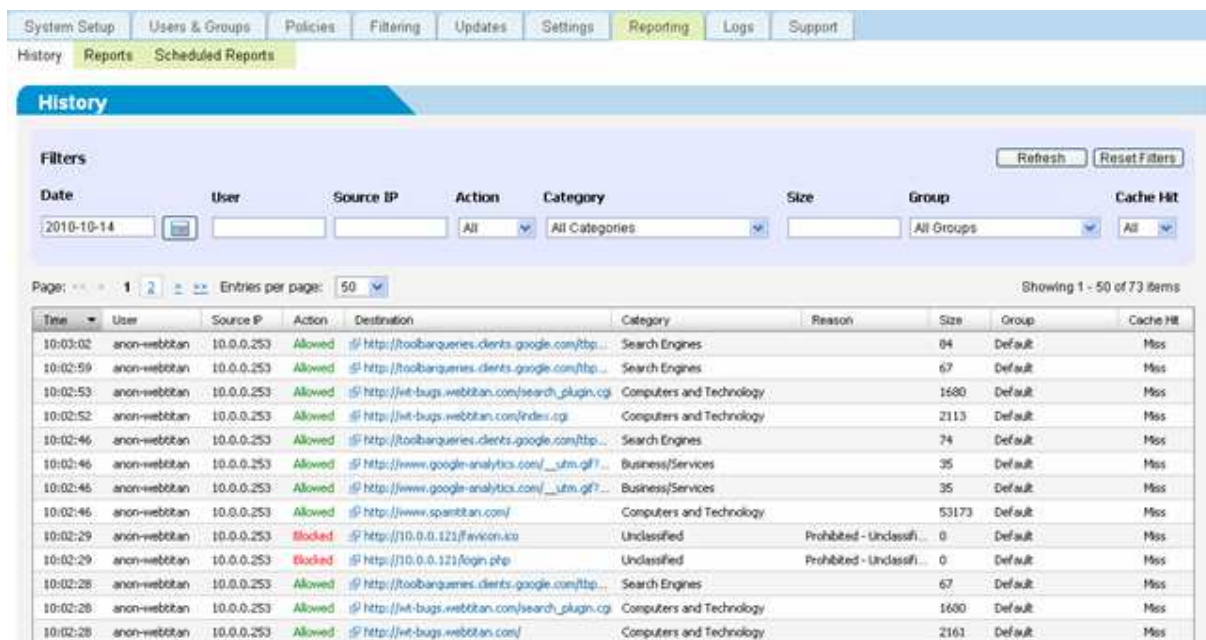
## 7. Check WebTitan is Filtering Traffic

Once you have completed all the above steps you can now check that your WebTitan installation is filtering traffic as you intended.

Navigate to the Reports> History tab. Here you can view a variety of information about the web traffic being processed by WebTitan as it happens, including the URL's and categories of all web requests as well as the action taken by WebTitan upon receiving them, i.e. whether a request is allowed or blocked.

By using this page we can then determine whether traffic is being filtered and whether WebTitan is performing the desired actions when processing web requests.

To determine this, browse to a number of sites from a computer which is being filtered by WebTitan, then press 'Refresh' in the top right hand corner of the tab. If traffic is being filtered by WebTitan you should be returned a series of information about your browsing activity similar to the screenshot below, indicating that WebTitan is indeed filtering web traffic. WebTitan's response to web requests can also be used to determine if it is filtering web traffic as intended.



Time	User	Source IP	Action	Destination	Category	Reason	Size	Group	Cache Hit
10:03:02	anon-webtitan	10.0.0.253	Allowed	http://toolbarqueries.clients.google.com/tp...	Search Engines		84	Default	Miss
10:02:59	anon-webtitan	10.0.0.253	Allowed	http://toolbarqueries.clients.google.com/tp...	Search Engines		67	Default	Miss
10:02:53	anon-webtitan	10.0.0.253	Allowed	http://web-bugs.webtitan.com/search_plugin.cg...	Computers and Technology		1680	Default	Miss
10:02:52	anon-webtitan	10.0.0.253	Allowed	http://web-bugs.webtitan.com/index.cg...	Computers and Technology		2113	Default	Miss
10:02:46	anon-webtitan	10.0.0.253	Allowed	http://toolbarqueries.clients.google.com/tp...	Search Engines		74	Default	Miss
10:02:46	anon-webtitan	10.0.0.253	Allowed	http://www.google-analytics.com/_utm.gif?...	Business/Services		35	Default	Miss
10:02:46	anon-webtitan	10.0.0.253	Allowed	http://www.google-analytics.com/_utm.gif?...	Business/Services		35	Default	Miss
10:02:46	anon-webtitan	10.0.0.253	Allowed	http://www.spamTitan.com/	Computers and Technology		53173	Default	Miss
10:02:29	anon-webtitan	10.0.0.253	Blocked	http://110.0.0.121/favicon.ico	Unclassified	Prohibited - Unclassifi...	0	Default	Miss
10:02:29	anon-webtitan	10.0.0.253	Blocked	http://110.0.0.121/login.php	Unclassified	Prohibited - Unclassifi...	0	Default	Miss
10:02:28	anon-webtitan	10.0.0.253	Allowed	http://toolbarqueries.clients.google.com/tp...	Search Engines		67	Default	Miss
10:02:28	anon-webtitan	10.0.0.253	Allowed	http://web-bugs.webtitan.com/search_plugin.cg...	Computers and Technology		1680	Default	Miss
10:02:28	anon-webtitan	10.0.0.253	Allowed	http://web-bugs.webtitan.com/	Computers and Technology		2161	Default	Miss

By now your WebTitan installation should be up and running. If you encounter any difficulties please don't hesitate to contact WebTitan support via any of the following means.

- Web: <http://www.webtitan.com/>
- Knowledge Base: <http://getsatisfaction.com/webtitan>
- Telephone: +353 91 540054
- Email: [support@webtitan.com](mailto:support@webtitan.com)