



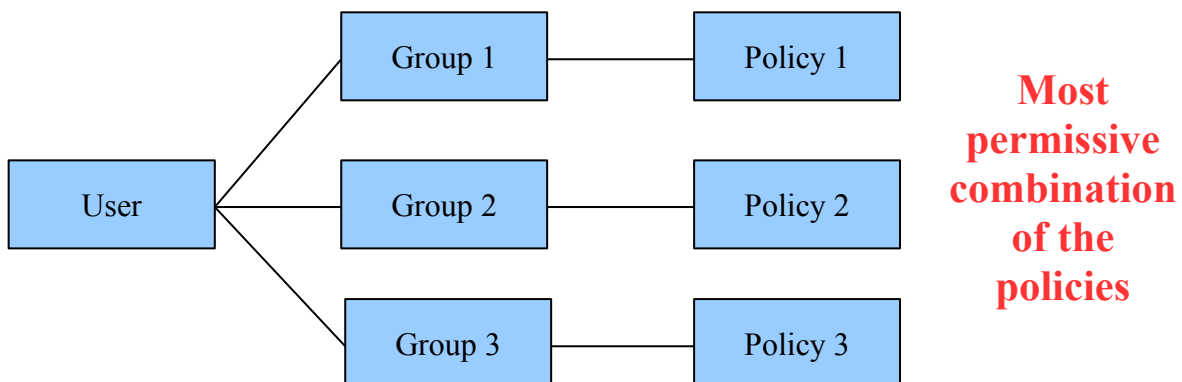
Quickstart guide to Users, Groups, Policies and Filtering

Introduction

WebTitan operates on a filtering and policy basis. Filtering allows the WebTitan administrator to operate a blanket approach to all users and groups, whereas the use of policies allows for a tailored and more specific control method.

The basic premise of policies in WebTitan is

- A user is assigned to one or more groups.
- A group is assigned to one and only one policy.
- It is the most permissive setting of the combined policies assigned to a user that will apply.



This guide 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.

Users

Within WebTitan, a user can be created manually or imported from an LDAP server**.

** See <http://webtitan.com/support/documentation> for LDAP server importation details.

Once a user has been created, there are two methods by which an Internet browser can be linked to the WebTitan user

- By manually assigning an IP address or range of IP addresses to a WebTitan user.
- By authenticating the Internet browser using one of the following authentication methods
 - IP based authentication
 - LDAP based authentication
 - NTLM based authentication
 - IP and LDAP based authentication
 - IP and NTLM based authentication

Manually assigning an IP address

By adding a new user or editing an existing user, a range of IP addresses or a specific IP address can be assigned as demonstrated in the screen shot below.

The screenshot shows the 'Edit User' interface with the following details:

- Username:** Demo Test
- Fullname:** Demo
- Description:** Demo of range and specific IP addresses
- Managed via LDAP:** No
- IP Addresses:** A table with two entries:

1	10.0.0.62	X
2	10.0.0.100-10.0.0.199	X
- Groups:**
 - Available:** Default, Administrators, Sin bin, developers, sales, guests
 - Selected:** guests, sales

Buttons for 'Save' and 'Cancel' are located at the bottom right.

Authenticating the Internet browser

WebTitan authentication settings are done via the System Setup > Authentication tab. As outlined above, there are five available authentication methods. Below is a screenshot of example NTLM based authentication settings.

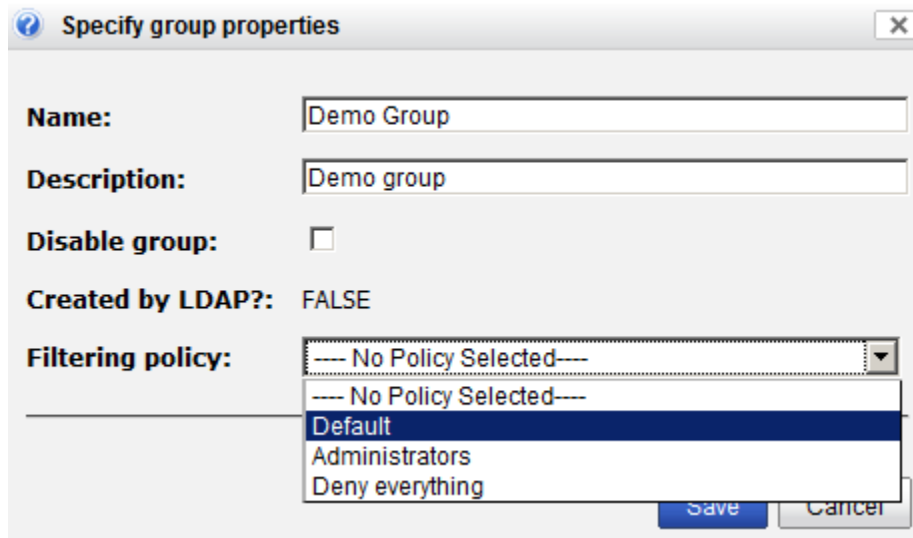
The screenshot displays the WebTitan Administration Console interface. At the top left is the 'WEB TITAN' logo. The top right corner shows the user is logged in as 'admin', with links for 'Dashboard' and 'Logout', and displays the version '1.12' and license 'WTP-1-0050-606730'. A navigation menu below the header includes 'System Setup', 'Users & Groups', 'Policies', 'Filtering', 'Updates', 'Settings', 'Reporting', 'Logs', and 'Support'. A secondary menu below that includes 'Licensing', 'Network', 'Authentication', 'Proxy', 'Cache', 'Autoconfiguration', 'Time', and 'Shutdown/Restart'. The main content area is titled 'Authentication Policy' and features a 'Disable' button. The 'Enable Authentication' toggle is set to 'ON'. The 'Policy type' is set to 'NTLM based authentication'. The configuration fields are as follows: 'NT domain name' is 'DOMAIN', 'Primary domain controller name' is 'HELLO', 'Primary domain controller IP address' is '10.0.0.20', 'Backup domain controller name' is empty, 'Backup domain controller IP address' is empty, 'Username' is 'administrator', 'Password' is masked with dots, and 'Number of NTLM authenticators' is '10'. A 'Save' button is located at the bottom right of the form area. The browser's address bar at the bottom shows 'WebTitan - Mozilla Firefox'.

IP, NTLM, IP and NTLM based authentication methods are transparent to the end user, whereas with LDAP, the end user will be prompted for their username/password when they open their first Internet browser. They will not be prompted after this.

Groups

Once you have your users created, then you will need to set up your groups. If you have imported your users and groups using LDAP, then this will not be necessary. However, if you have manually created your users, or elected to just import your users and not the groups from LDAP, then you will need to do this.

Groups are created in the Users and Groups > Groups tab. When a Group is been created, it must be assigned to a policy. If you do not have any bespoke policies created, then you can assign your new group to one of three policies provided by WebTitan which are 'Default', 'Administrators' and 'Deny everything'. Any groups imported via LDAP will be automatically assigned the 'Default' policy. The screen shot below shows the 'Default' policy been assigned to a new group called 'Demo Group'.



The screenshot shows a dialog box titled "Specify group properties" with the following fields and options:

- Name:** Demo Group
- Description:** Demo group
- Disable group:**
- Created by LDAP?:** FALSE
- Filtering policy:** A dropdown menu is open, showing the following options: "---- No Policy Selected----", "Default" (highlighted), "Administrators", and "Deny everything".

At the bottom right of the dialog box, there are "Save" and "Cancel" buttons.

Once you group has been created, a user can be assigned to it or more policies by editing an existing user or adding a new one. Simply drag and drop a group from the 'Available' list to the 'Selected' list. The screen shot belows shows the 'guests' and 'sales' groups have been assigned to the 'Demo Test' user.

The 'Edit User' dialog box displays the following information:

- Username:** Demo Test
- Fullname:** Demo
- Description:** Demo of range and specific IP addresses
- Managed via LDAP:** No
- IP Addresses:** A table with two entries:

1	10.0.0.62	X
2	10.0.0.100-10.0.0.199	X
- Groups:** Two columns: 'Available' and 'Selected'.
 - Available:** Default, Administrators, Sin bin, devlopers, sales, guests
 - Selected:** guests, sales

Buttons: Save, Cancel

When this assignment is saved, the two groups assigned to the user will be listed beside it as shown below.

The 'Users' list displays the following information:

- Page: 1 2 3 Entries per page: 5 Showing 11 - 11 of 11 items
- Table:

User	Groups	Options
Demo Test	sales, guests	[Edit] [Delete]
- Success: Changes saved
- Add...

Policies

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

The screenshot shows the WEB TITAN interface. At the top, it says 'WEB TITAN' with a logo. On the right, it indicates 'Logged In: admin | Dashboard | Logout', 'Version: 1.12', and 'License: WTP-1-0050-606730'. Below this is a navigation bar with tabs: System Setup, Users & Groups, Policies, Filtering, Updates, Settings, Reporting, Logs, and Support. Under 'Policies', there are sub-tabs: Filtering Policies and Categories. The main content area is titled 'Filtering Policies' and shows a table with 4 items. The table has columns for Policy, Description, and Options. The items are: Default (Default filtering policy), Administrators (Slightly relaxed policy for administrators), Deny everything (Policy that blocks everything), and Demo Policy (Demo Policy). Each item has edit and delete icons. There is an 'Add Policy' button at the bottom right.

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

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'.

The screenshot shows the 'Edit Policy: Demo Policy' page. It has a navigation bar with tabs: Name, Non-working times, Categories, Web-filter, File types, Safe search, Notifications, and Groups. The 'Name' tab is selected. Below the tabs, there are two input fields: 'Name:' with the value 'Demo Policy' and 'Description:' with the value 'Demo Policy'. There is a 'Save' button at the bottom right.

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.

Filtering

As mentioned in the introduction, WebTitan operates on a filtering and policy basis. Filtering allows the WebTitan administrator to operate a blanket approach to all users and groups.

Here the administrator can

- Set up domain properties such as whitelisting and blacklisting.
- Set up Microsoft Update properties.
- Set the score and optionally block specific keywords.
- Set up virus scanning properties.
- Set up file extensions to search for.
- Set up URL redirection.

These options are available via the Filtering tab as can be seen below.

The screenshot shows the WebTitan administration interface. At the top left is the logo 'WEB TITAN'. On the top right, it displays 'Logged In: admin | Dashboard | Logout', 'Version: 1.12', and 'License: WTP-1-0050-606730'. Below the logo is a navigation menu with tabs: System Setup, Users & Groups, Policies, Filtering (highlighted), Updates, Settings, Reporting, Logs, and Support. Under the Filtering tab, there are sub-tabs: Domains, Content, Anti-Virus, Extensions, and Redirection. The main content area is divided into three sections:

- Microsoft Updates:** A section with a blue header. It shows 'Enable Microsoft updates: ON' with a green indicator. A 'Disable' button is located on the right.
- Whitelisted Domains:** A section with a blue header. It includes a pagination control: 'Page: 1' and 'Entries per page: 5'. It shows 'Showing 1 - 1 of 1 items'. Below this is a table with columns 'Domain', 'Flags', and 'Options'. The table contains one row: 'www.google.com' with the flag 'Bypass Filters' and two icons in the options column. An 'Add...' button is at the bottom right.
- Blacklisted Domains:** A section with a blue header. It includes a pagination control: 'Page: 1' and 'Entries per page: 5'. It shows 'Showing 0 - 0 of 0 items'. Below this is a table with columns 'Domain' and 'Options'. The table contains one row: 'No records found.'

Configuring web browsers to use WebTitan

Once WebTitan is installed and configured, 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 **

* The default port for the proxy is 8881. It can be changed via System Setup > Proxy on WebTitan.

** See <http://webtitan.com/support/documentation> for wpad.dat configuration help.

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

