



Quickstart guide to Authentication

Introduction

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 Settings > 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.

- IP based authentication
- LDAP based authentication
- NTLM based authentication
- IP and LDAP based authentication
- IP and NTLM based authentication

The screenshot shows the WebTitan web interface. At the top left is the WebTitan logo. At the top right, it displays "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. Underneath, there are sub-tabs for Licensing, Network, Authentication, Proxy, Cache, Autoconfiguration, Time, and Shutdown/Restart. The main content area is titled "Authentication Policy" and contains three settings: "Enable Authentication:" set to "ON" with a "Disable" button; "Policy type:" set to "IP based authentication" with a dropdown arrow; and "Enable IP Session:" set to "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.

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 been 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

Username: Demo user

Fullname: Demo user

Description: Demo user

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	

Save Cancel

IP authentication points

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

LDAP based authentication

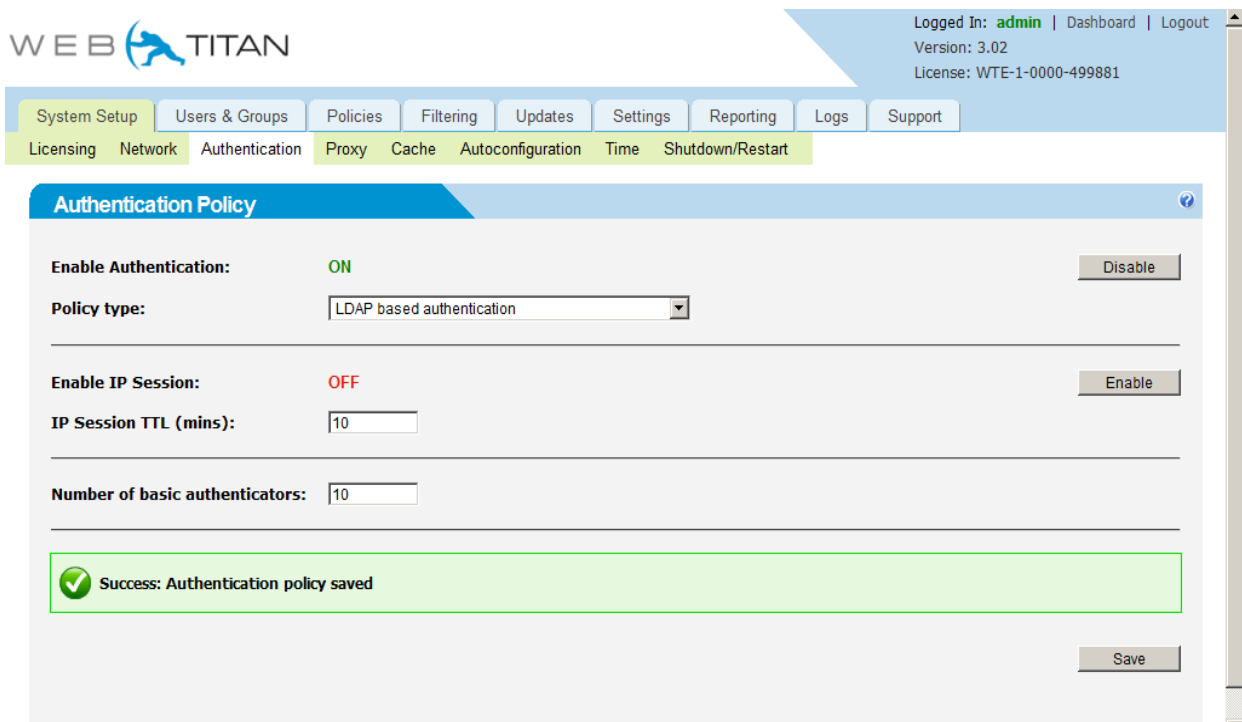
LDAP authentication is suitable for where the users and groups are being managed by an LDAP server and where it is preferred that the user must enter their LDAP username/password credentials on commencing web site browsing.

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*.

*Please click [here](#) to see the 'Quickstart Guide to LDAP Setup' for details on how to connect to an LDAP server within WebTitan and also how to import LDAP users.

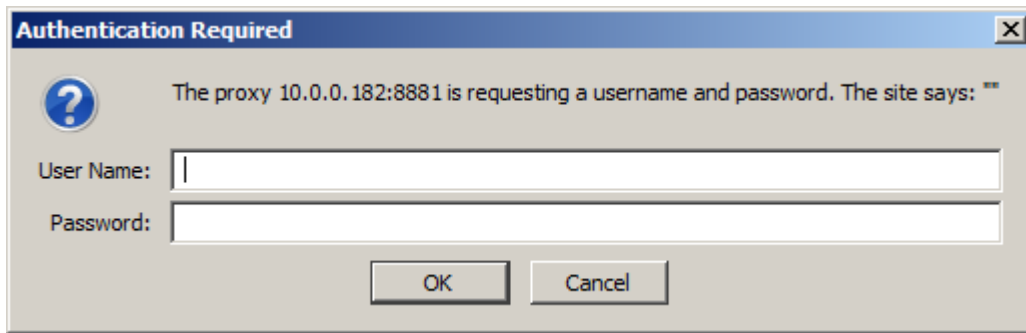
Below is a screen shot of LDAP based authentication turned on within WebTitan, which is then followed by a screen shot of a user being prompted for their LDAP credentials. They are only required to enter these credentials once.



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 '3.02' and license 'WTE-1-0000-499881'. A navigation menu includes 'System Setup', 'Users & Groups', 'Policies', 'Filtering', 'Updates', 'Settings', 'Reporting', 'Logs', and 'Support'. Below this, a secondary menu highlights 'Authentication' under the 'System Setup' section, with other options like 'Licensing', 'Network', 'Proxy', 'Cache', 'Autoconfiguration', 'Time', and 'Shutdown/Restart'. The main content area is titled 'Authentication Policy' and contains the following settings:

- Enable Authentication:** Set to **ON** (green text), with a 'Disable' button to the right.
- Policy type:** A dropdown menu currently showing 'LDAP based authentication'.
- Enable IP Session:** Set to **OFF** (red text), with an 'Enable' button to the right.
- IP Session TTL (mins):** A text input field containing the value '10'.
- Number of basic authenticators:** A text input field containing the value '10'.

A green success message box at the bottom of the configuration area reads: 'Success: Authentication policy saved'. A 'Save' button is located at the bottom right of the configuration area.



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

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.

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 or Mozilla Firefox.

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

The screenshot shows the 'Authentication Policy' configuration page in the WebTitan interface. The page has a navigation bar at the top with tabs for System Setup, Users & Groups, Policies, Filtering, Updates, Settings, Reporting, Logs, and Support. Below this is a sub-navigation bar with tabs for Licensing, Network, Authentication, Proxy, Cache, Autoconfiguration, Time, and Shutdown/Restart. The main content area is titled 'Authentication Policy' and contains the following fields:

- Enable Authentication:** ON (with a 'Disable' button)
- Policy type:** NTLM based authentication (dropdown menu)
- NT domain name:** danielx
- Primary domain controller name:** dnp
- Primary domain controller IP address:** 10.0.0.241
- Backup domain controller name:** (empty)
- Backup domain controller IP address:** (empty)
- Username:** administrator
- Password:** (masked with dots)
- Number of NTLM authenticators:** 10

A 'Save' button is located at the bottom right of the form.

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 and Mozilla Firefox.
- 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.