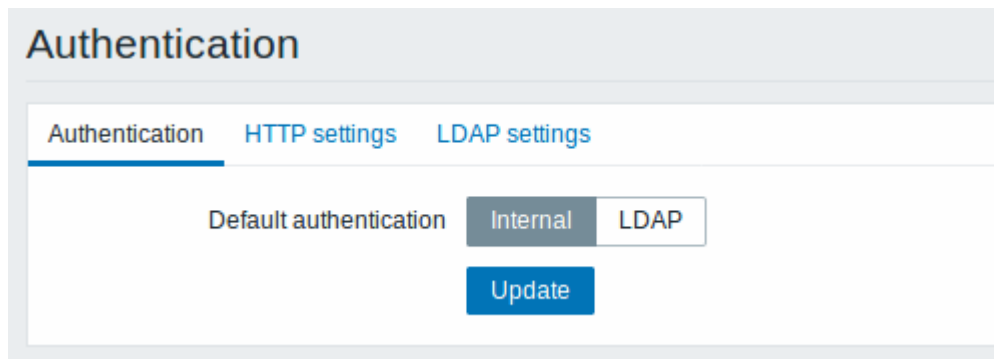


## 3 Authentication

### Overview

In *Administration* → *Authentication* the global user authentication method to Zabbix can be specified. The available methods are internal, HTTP and LDAP authentication.

Note that the authentication method can be fine-tuned on the [user group](#) level.



The screenshot shows the 'Authentication' settings page in Zabbix. At the top, there are three tabs: 'Authentication', 'HTTP settings', and 'LDAP settings'. The 'Authentication' tab is active. Below the tabs, there is a section for 'Default authentication' with two radio buttons: 'Internal' (which is selected) and 'LDAP'. Below these buttons is a blue 'Update' button.

By default, internal Zabbix authentication is used globally. To change:

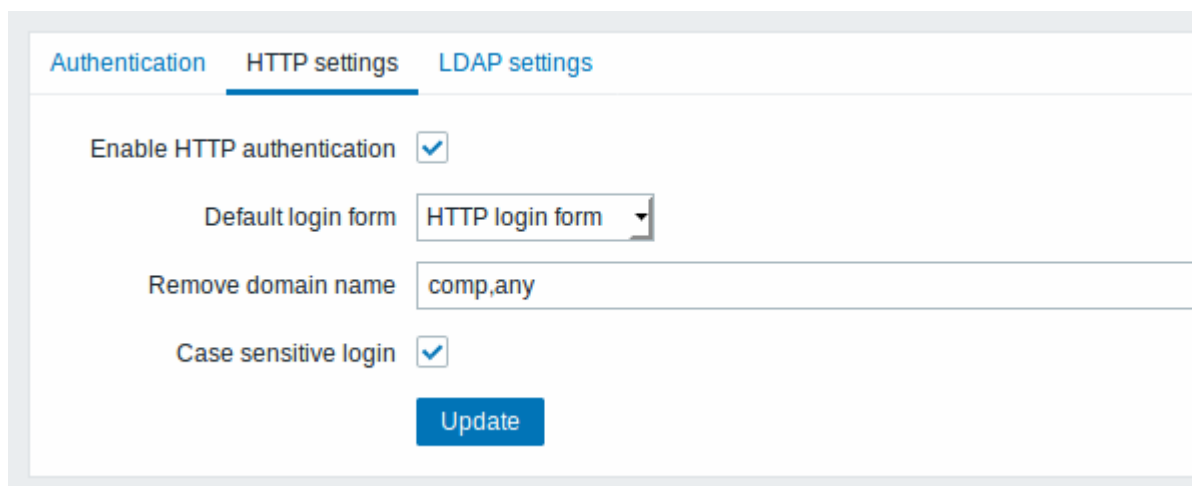
- to HTTP - navigate to the *HTTP settings* tab and enter authentication details;
- to LDAP - select LDAP as *Default authentication* and enter authentication details in the *LDAP settings* tab.

When done, click on *Update* at the bottom of the form.

### HTTP authentication

HTTP or web server-based authentication (for example: Basic Authentication, NTLM/Kerberos) can be used to check user names and passwords. Note that a user must exist in Zabbix as well, however its Zabbix password will not be used.

Be careful! Make sure that web server authentication is configured and works properly before switching it on.



The screenshot shows the 'HTTP settings' page in Zabbix. At the top, there are three tabs: 'Authentication', 'HTTP settings', and 'LDAP settings'. The 'HTTP settings' tab is active. Below the tabs, there are four settings: 'Enable HTTP authentication' with a checked checkbox, 'Default login form' with a dropdown menu showing 'HTTP login form', 'Remove domain name' with a text input containing 'comp,any', and 'Case sensitive login' with a checked checkbox. At the bottom is a blue 'Update' button.

Configuration parameters:

Parameter	Description
<i>Enable HTTP authentication</i>	Mark the checkbox to enable HTTP authentication.
<i>Default login form</i>	Specify whether to direct non-authenticated users to: <b>Zabbix login form</b> - standard Zabbix login page. <b>HTTP login form</b> - HTTP login page. It is recommended to enable web-server based authentication for the <code>index_http.php</code> page only. If <i>Default login form</i> is set to 'HTTP login page' the user will be logged in automatically if web server authentication module will set valid user login in the <code>\$_SERVER</code> variable. Supported <code>\$_SERVER</code> keys are <code>PHP_AUTH_USER</code> , <code>REMOTE_USER</code> , <code>AUTH_USER</code> .
<i>Remove domain name</i>	A comma-delimited list of domain names that should be removed from the username. E.g. <code>comp,any</code> - if username is 'Admin@any', 'comp\Admin', user will be logged in as 'Admin'; if username is 'notacompanyAdmin', login will be denied.
<i>Case sensitive login</i>	Unmark the checkbox to disable case-sensitive login (enabled by default) for usernames. E.g. disable case-sensitive login and log in with, for example, 'ADMIN' user even if the Zabbix user is 'Admin'. <i>Note that with case-sensitive login disabled the login will be denied if multiple users exist in Zabbix database with similar alias (e.g. Admin, admin).</i>

In case of web server authentication all users (even with [frontend access](#) set to Internal) will be authenticated by the web server, not by Zabbix!

For internal users who are unable to log in using HTTP credentials (with HTTP login form set as default) leading to the 401 error, you may want to add a `ErrorDocument 401`

`/index.php?form=default` line to basic authentication directives, which will redirect to the regular Zabbix login form.

### LDAP authentication

External LDAP authentication can be used to check user names and passwords. Note that a user must exist in Zabbix as well, however its Zabbix password will not be used.

While LDAP authentication is set globally, some user groups can still be authenticated by Zabbix. These groups must have [frontend access](#) set to Internal. Vice versa, if internal authentication is used globally, LDAP authentication details can be specified and used for specific user groups whose [frontend access](#) is set to LDAP.

Zabbix LDAP authentication works at least with Microsoft Active Directory and OpenLDAP.

Authentication
HTTP settings
LDAP settings

Enable LDAP authentication

\* LDAP host

\* Port

\* Base DN

\* Search attribute

Bind DN

Case sensitive login

Bind password

Test authentication [must be a valid LDAP user]

\* Login

\* User password

Update
Test

Configuration parameters:

Parameter	Description
<i>Enable LDAP authentication</i>	Mark the checkbox to enable LDAP authentication.
<i>LDAP host</i>	Name of LDAP server. For example: ldap://ldap.zabbix.com For secure LDAP server use <i>ldaps</i> protocol. ldaps://ldap.zabbix.com With OpenLDAP 2.x.x and later, a full LDAP URI of the form ldap://hostname:port or ldaps://hostname:port may be used.
<i>Port</i>	Port of LDAP server. Default is 389. For secure LDAP connection port number is normally 636. Not used when using full LDAP URIs.
<i>Base DN</i>	Base path to search accounts: ou=Users,ou=system (for OpenLDAP), DC=company,DC=com (for Microsoft Active Directory)
<i>Search attribute</i>	LDAP account attribute used for search: uid (for OpenLDAP), sAMAccountName (for Microsoft Active Directory)
<i>Bind DN</i>	LDAP account for binding and searching over the LDAP server, examples: uid=ldap_search,ou=system (for OpenLDAP), CN=ldap_search,OU=user_group,DC=company,DC=com (for Microsoft Active Directory) Anonymous binding is supported since Zabbix 4.0.4.

Parameter	Description
<i>Case-sensitive login</i>	Unmark the checkbox to disable case-sensitive login (enabled by default) for usernames. E.g. disable case-sensitive login and log in with, for example, 'ADMIN' user even if the Zabbix user is 'Admin'. <i>Note</i> that with case-sensitive login disabled the login will be denied if multiple users exist in Zabbix database with similar alias (e.g. Admin, admin).
<i>Bind password</i>	LDAP password of the account for binding and searching over the LDAP server.
<i>Test authentication</i>	Header of a section for testing
<i>Login</i>	Name of a test user (which is currently logged in the Zabbix frontend). This user name must exist in the LDAP server. Zabbix will not activate LDAP authentication if it is unable to authenticate the test user.
<i>User password</i>	LDAP password of the test user.

In case of trouble with certificates, to make a secure LDAP connection (ldaps) work you may need to add a `TLS_REQCERT allow` line to the `/etc/openldap/ldap.conf` configuration file. It may decrease the security of connection to the LDAP catalog.

It is recommended to create a separate LDAP account (*Bind DN*) to perform binding and searching over the LDAP server with minimal privileges in the LDAP instead of using real user accounts (used for logging in the Zabbix frontend).

Such an approach provides more security and does not require changing the *Bind password* when the user changes his own password in the LDAP server.

In the table above it's *ldap\_search* account name.

From: <https://www.zabbix.com/documentation/4.0/> - **Zabbix Documentation 4.0**

Permanent link: [https://www.zabbix.com/documentation/4.0/manual/web\\_interface/frontend\\_sections/administration/authentication](https://www.zabbix.com/documentation/4.0/manual/web_interface/frontend_sections/administration/authentication)

Last update: **2019/05/16 13:42**

