Sitelok Zendesk Plugin

V1.3

Sitelok Zendesk Plugin

Contents

Chapter 1 Introduction

What is the Sitelok Zendesk plugin?

The Sitelok Zendesk plugin allows a single sign-on (SSO) between Sitelok and Zendesk. In other words Sitelok will be the login system used by Zendesk so a user only needs to enter their Sitelok login details to have access to Zendesk as well.

Chapter 2 Installation

Installing for the first time or upgrading

1) Extract the contents of the zip file to your PC.
2) Upload the plugin_zendesk folder to your existing Sitelok slpw folder using FTP. There are no special permissions required on most servers.
3) Login to the Sitelok control panel.
4) Open the following URL in the browser

   http://www.yoursite.com/slpw/plugin_zendesk/install.php

   which will start the installation process. If all is well you will be taken to the plugin preferences page where you will see the plugin listed.

If you have any problems with installation please let us know so that we can help you.

If you are upgrading from a version earlier than V1.0 or V1.1 please go to the plugin page and change the older Zendesk Login URL with just your Zendesk subdomain.

Setting up your Zendesk account

Before Zendesk will allow Sitelok to login in users we need to enable Single Sign-On.

Before enabling SSO in Zendesk you should ensure that you create a user in Sitelok with the same email address as the admin user in Zendesk. If you ever manage to lock yourself out of Zendesk you can always login at

https://account.zendesk.com/access/normal

1) Login to to Zendesk as admin, go to Admin - Security

2) Click the End-users link at the top

3) Click the Single Sign-On (SSO) checkbox

4) Check JSON Web Token

5) Set the Remote login URL to

   http://www.yoursite.com/slpw/plugin_zendesk/zendesklogin.php

6) Set the Remote logout URL to

   http://www.yoursite.com/slpw/plugin_zendesk/zendesklogout.php

7) Leave the IP ranges field blank

8) Check the Allow update of external ids? checkbox.

9) Make a note of the Shared Secret token that is generated. If you don't see it you cam click the link to generate a new one.

10) Click the Save button

Once setup the screen should look something like this.

Security

Admins & Agents   **End-users**   Global

End-user login authentication

By default, your end-users are authenticated and logged in using Zendesk's user authentication. You can however bypass this and require your end-users to log in via single sign-on using Zendesk Remote Authentication or SAML (available in Plus and Enterprise).

○ ⚙ **Zendesk**
Your customers log in with their Zendesk accounts.

✔ 🔒 **Single sign-on (SSO)**
Your customers use your SSO service to log in to your Zendesk. Requires configuration.

☐ **SAML**
SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. Learn more.

☑ **JSON Web Token**
JWT, a widely adopted open standard, provides a flexible framework for creating a custom SSO solution. Learn more.

Remote login URL

`http://yoursite.com/slpw/plugin_zendesk/zendesklogin.php`

This is the URL that Zendesk will redirect your users to for remote authentication, e.g.
`https://www.example.com/services/login`

Remote logout URL

`http://yoursite.com/slpw/plugin_zendesk/zendesklogout.php`

This is the URL that Zendesk will redirect your users to after they log out, e.g.
`https://www.example.com/services/logout`

IP ranges (optional)

Requests from these IP ranges will always be routed via remote authentication. Requests from IP addresses outside these ranges will be routed to the normal login form. To route all requests through remote authentication, leave this blank. An IP range is in the format n.n.n.n, where n is a number or an asterisk (*) wild card. Separate multiple IP ranges with a space. Your current IP address is: 213.123.39.245

Update of external IDs? `On ⇕`

It is safe to ignore this setting if you do not use external_id's. When checked, the external_id of the user being signed in can be updated. This only happens when no user with the external_id was found, but the user's email address was. The external_id is unique for an account. Users without an external_id will have one added if it's present in the authentication request.

Once you enable SSO it is best to block users from changing their profile and password in Zendesk as this is now handled by Sitelok. To do this

1) Go to Admin - Customers.

2) Uncheck the checkbox labelled Allow users to view and edit their basic profile data.

3) Uncheck the checkbox labelled Allow users to change their password.

4) Click the Save tab button.

Allow users to view and edit their profile data	☐ **Enabled**
	Allow end-users to change profile data, such as name and phone, in Zendesk.
	You should disable this option if you use SSO (Single Sign-On) to populate and update your users in Zendesk (using the API).
Allow users to change their password	☐ **Enabled**
	Allow end-users to change their password. Disable this if you administer users and passwords in another system and rely on SSO (Single Sign-On).

Setting up the plugin

Now that Zendesk SSO has been enabled we need to make a few settings in the plugin. You can access the Zendesk plugin configuration by selecting Zendesk from the Plugins menu. This will display a page like this.

1) Set the Zendesk subdomain to account name (subdomain)

2) Set the Shared Secret Token. This should be kept secret.

3) Check the Use user id's checkbox

4) Click the Save button.

Disabling the Plugin

To disable the Zendesk plugin select **Plugin Preferences** in the **Plugin** menu option of Sitelok. Uncheck the enable box for the plugin and click the **Save** button. You can enable it again in the same way.

Uninstalling the plugin

To permanently remove the plugin and its settings follow these steps.

1) Disable the plugin as above.
2) Click the delete icon next the plugin in the disabled plugins section.
3) Confirm the action in the alert box.

If the plugin is uninstalled successfully you will be returned to the plugin preferences page.

Chapter 3 Using the plugin

How does SSO work on your site

Login

Once setup Zendesk will use Sitelok as its login and registration system. So you can add users to Sitelok as you do now (via registration forms, payment, Linklok etc) and these users will automatically have access to Zendesk.

If a user visits your Zendesk page and clicks the login link they will see the Sitelok login form (or your custom login template) if they are not already logged in. After login they will be returned to Zendesk.

If a user logs in to Sitelok then you can have that user auto login to Zendesk by linking to Zendesk using the link

http://www.yoursite.com/slpw/plugin_zendesk/zendesklogin.php

if you wish.

Logout

When a user clicks the logout link in Zendesk the user is logged out of Sitelok as well as Zendesk.

As Zendesk don't provide an API call to close a Zendesk session if a user logs out of Sitelok (from a members page) they won't be logged out of Zendesk. One way to solve this is to replace Sitelok logout links with the URL

https://account.zendesk.com/access/logout

replacing account with your Zendesk subdomain. This way clicking logout will logout the user from Zendesk and then Sitelok in one go.

Using User id's

By default Sitelok passes unique user id's to Zendesk. This means that if the user changes their email address in Sitelok Zendesk will still know who

the user is. You can if you wish disable User Id's in both the Zendesk settings and the plugin.

Chapter 4 Support

Hopefully if you have followed this manual carefully everything will be working fine. However sometimes things don't go quite so smoothly so if you have any questions or problems then please check the FAQ on the support page or email us.

Support area: http://www.vibralogix.com/support/

Email: support@vibralogix.com