

Intrusion Detection System

An intrusion detection system (IDS) is a software application that monitors a network or systems for malicious activity or policy violations. An IDS specifically does not aim to prevent malicious actions but instead to monitor and log every event, and in cases where a rule has been defined, take a predefined action.* As of [Tiki 18](#), [Expos](#)™ is available as a [package](#) to provide website threat identification for Tiki.

*From <https://en.wikipedia.org/wiki/PHPIDS>

INTRODUCTION

"An IDS system should not be relied upon for sole protection in your environment! It should only be used in the first level of threat identification. Please read up on [Defense in Depth](#) for more information on a layered security approach" (from <https://github.com/enygma/expose>).

"Here's a quick list (of features):

- A queue system that lets you do offline processing (store on request, cron to check or something similar)
- Notifications of results (just email right now)
- Setting thresholds for notifications

Since it was based on the PHPIDS system, it also has features in common with it:


- Setting exceptions
- Setting restrictions ("only look at...")

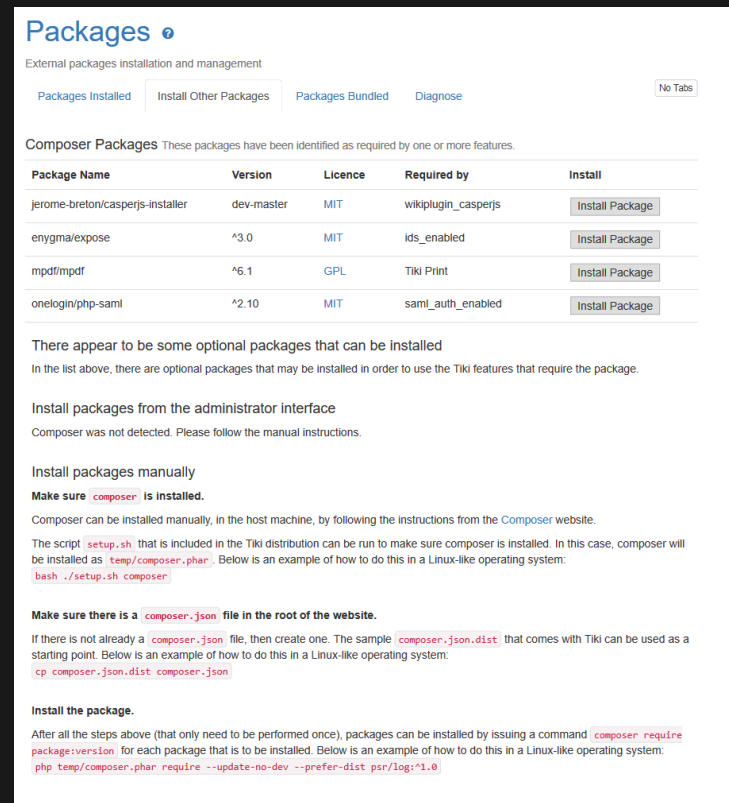
- Uses the same filter definitions


I tried to make it so that anyone that's used PHPIDS will feel pretty at home using Expose."

From https://www.reddit.com/r/PHP/comments/1iydsm/expose_a_php_ids/cb9a6z4/

INSTALLATION

Composer isn't bundled with Tiki as an external library by default. Instead, it can be installed "on demand" via the  **Packages** feature.



Packages 

External packages installation and management

Packages Installed | Install Other Packages | Packages Bundled | Diagnose No Tabs

Composer Packages These packages have been identified as required by one or more features.

Package Name	Version	Licence	Required by	Install
jerome-breton/casperjs-installer	dev-master	MIT	wikiplugin_casperjs	Install Package
enigma/expose	^3.0	MIT	ids_enabled	Install Package
mpdf/mpdf	^6.1	GPL	Tiki Print	Install Package
onelogin/php-saml	^2.10	MIT	saml_auth_enabled	Install Package

There appear to be some optional packages that can be installed

In the list above, there are optional packages that may be installed in order to use the Tiki features that require the package.

Install packages from the administrator interface

Composer was not detected. Please follow the manual instructions.

Install packages manually

Make sure `composer` is installed.

Composer can be installed manually, in the host machine, by following the instructions from the [Composer](#) website.

The script `setup.sh` that is included in the Tiki distribution can be run to make sure composer is installed. In this case, composer will be installed as `temp/composer.phar`. Below is an example of how to do this in a Linux-like operating system:

```
bash ./setup.sh composer
```

Make sure there is a `composer.json` file in the root of the website.

If there is not already a `composer.json` file, then create one. The sample `composer.json.dist` that comes with Tiki can be used as a starting point. Below is an example of how to do this in a Linux-like operating system:

```
cp composer.json.dist composer.json
```

Install the package.

After all the steps above (that only need to be performed once), packages can be installed by issuing a command `composer require package:version` for each package that is to be installed. Below is an example of how to do this in a Linux-like operating system:

```
php temp/composer.phar require --update-no-dev --prefer-dist psr/log:^1.0
```

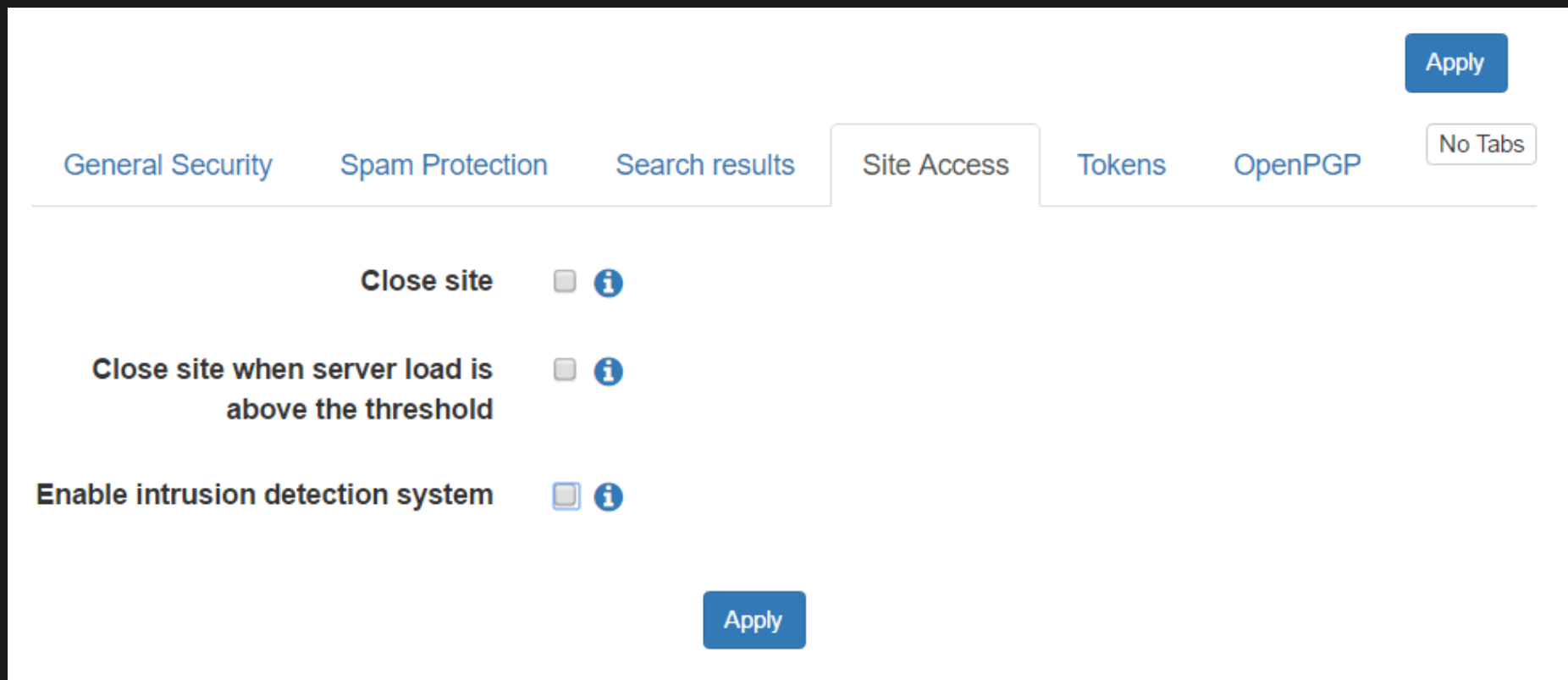
Please follow the standard [instructions](#) for package installation. Note: in some edge cases, there may be a problem with the package installation GUI. For example, currently (pre-Tiki 17 release) in a Windows WAMP localhost server, there's an error that Composer can't be found. In this case, Expose™ may be successfully fetched and

installed via the command line:

```
php temp/composer.phar require enygma/expose
```

CONFIGURATION AND USE

After the Exposé™ package is installed, go to Site Access tab on the Security Admin page (tiki-admin.php?page=security#content_admin1-4).





The screenshot shows the 'Site Access' configuration page. At the top right is an 'Apply' button. Below it is a horizontal navigation bar with tabs: 'General Security', 'Spam Protection', 'Search results', 'Site Access' (selected), 'Tokens', and 'OpenPGP'. To the right of the tabs is a 'No Tabs' button. The main content area contains three settings, each with a checkbox and an information icon:


- Close site** ⓘ
- Close site when server load is above the threshold** ⓘ
- Enable intrusion detection system** ⓘ


At the bottom center is another 'Apply' button.


When the feature is activated, relevant options are displayed.


Enable intrusion detection system  

Admin IDS custom rules

Custom rules file 

Intrusion detection system mode 

Intrusion detection system threshold 

Log to file 

CUSTOM RULES FILE

ExposÃfÆ'Ã†â€™ Ãfâ€ Ãçâ,¬â,,çÃfÆ'Ãçâ,¬Å;Ãfâ€šÃ,Â© uses the PHPIDS project's ruleset for detecting potential threats. This can be extended with custom rules. The default location and name of the custom rules file is *temp/ids_custom_rules.json*.

IDS Rules

Add a new rule

No Tabs

Rule Id

Rule Regex

Description

Tags

Impact

Add

INTRUSION DETECTION SYSTEM MODE

The IDS operation mode needs to be defined, and there are two choices here: *Log only* and *Log and block requests*. Log and block requests will block an intrusion whose impact is over a given threshold. "As the impact scores in Expose are numeric (0 through whatever, depending on the rules matched) you can easily set a threshold to prevent low-level, annoying notifications being delivered" (<https://expose.readthedocs.io/en/latest/>).

INTRUSION DETECTION SYSTEM THRESHOLD

This is to define the IDS threshold as a numerical value, when in the "Log and block requests" mode. "Some applications know for a fact that they will always be getting a certain amount of traffic that is in the 1-2 impact score range. Getting notifications for every one of these requests would get annoying pretty quickly, so you can set your threshold a bit higher." Setting the threshold to 8 means that Expose will only send notifications when the score is greater than or equal to 8.

There's no concept of
high, medium or
low threshold in
Expose as the meanings of these terms vary greatly by environment and application. "NOTE: Currently notifications are the only thing that setting a threshold changes. Logging and other processing is unchanged" (ibid).

LOG TO FILE

Events are logged to a file the default name of which is "ids.log".

HISTORY OF THIS TIKI FEATURE:

[+]

RELATED LINKS

- <https://github.com/enygma/expose>
- <https://expose.readthedocs.io/>
- <http://websec.io/2012/10/12/Core-Concepts-Defense-in-Depth.html>
- <https://www.openhub.net/p/expose>
- <https://www.awnage.com/2014/01/06/ids-showdown-phpids-vs-expose/>
- <https://en.wikipedia.org/wiki/PHPIDS>

- PHPIDS
- Expose
- Exposed to the Internet
- Intrusion Detection System
- IDS