

Stand-Alone Log Viewer

Introduction

The Stand-Alone Log Viewer is provided on the version 4 appliance because customers were finding that the built-in log viewer too inefficient for heavy use.

This log viewer stores the data in a database format, which is much more efficient for searching. It automatically updates the database as text log files are created. For technical reasons, it was not possible to modify the core code to store the logs directly into the database, hence this separate application.

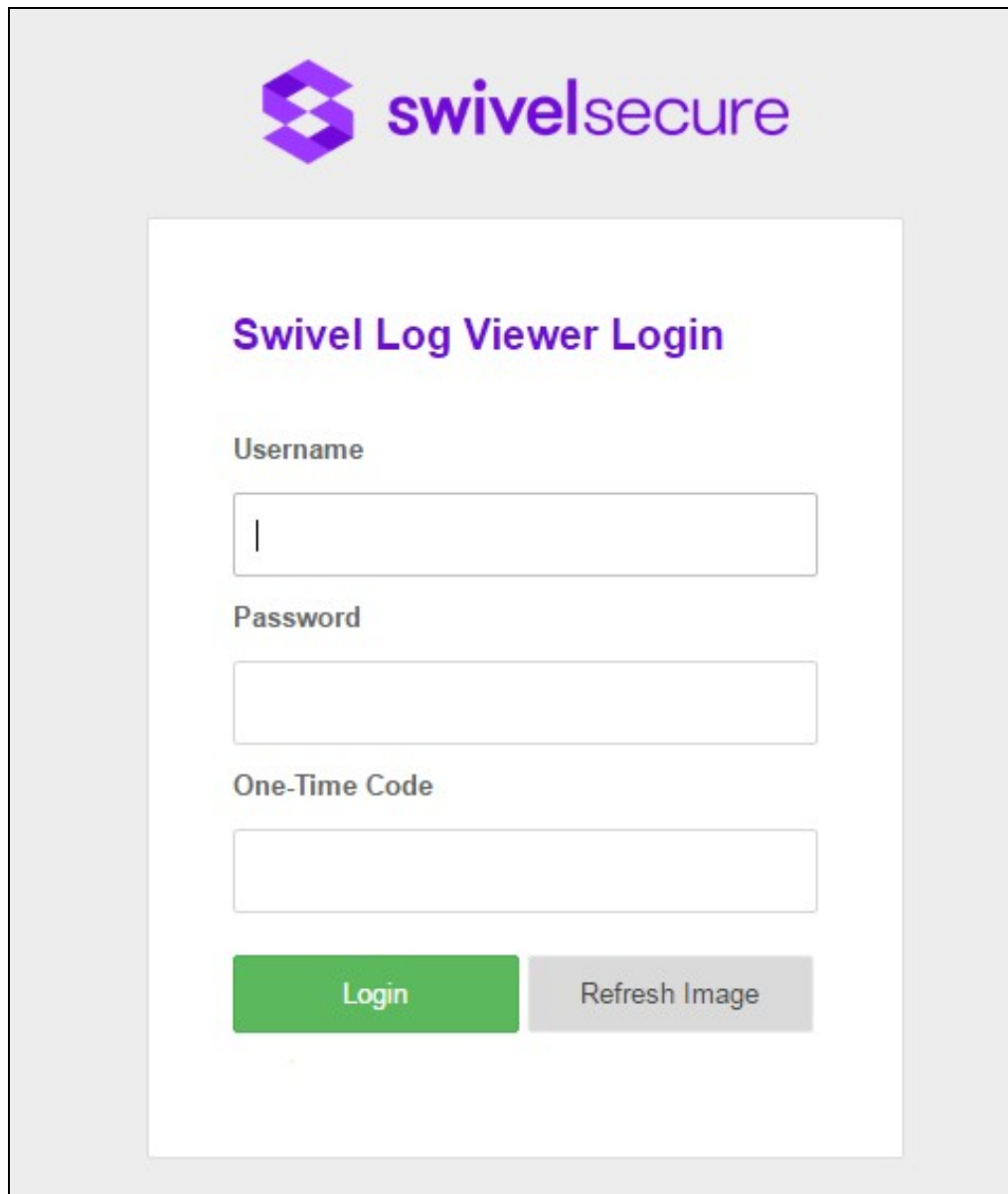
One caveat: the stand-alone log viewer only records completed log files: the core application writes logs to a working file until that file reaches a certain size, at which point the working file is renamed, and a new one is started. For this reason, the stand-alone log viewer will not show the very latest logs. Smaller installations can alleviate this problem by reducing the size of the individual log files.

Using the Stand-Alone Log Viewer

In order to use the log viewer, you must log in. Enter the following URL in a browser:

`https://<swivel_server>:8080/logviewer`

Here, <swivel_server> is the IP address or host name of the Swivel server.

The image shows a web browser window displaying the 'Swivel Log Viewer Login' page. At the top, there is a purple SwivelSecure logo. Below the logo, the title 'Swivel Log Viewer Login' is displayed in a large, bold, purple font. Underneath the title, there are three input fields: 'Username', 'Password', and 'One-Time Code'. Each field has a small vertical line indicating the start of the input area. Below the 'One-Time Code' field, there are two buttons: a green 'Login' button and a grey 'Refresh Image' button. The entire login form is centered within a light grey background.

It uses the core authentication, so any administrator or helpdesk user on the core database can log in



Swivel Log Viewer Login

Username

admin

Password

One-Time Code

Login

Refresh Image

1	2	3	4	5	6	7	8	9	0
3	2	5	4	9	0	7	8	6	1

You will then see the main viewer page

Level:

ALL

Events Per Page:

100

Start Date/Time:

dd/mm/yyyy

--:--

End Date/Time:

dd/mm/yyyy

--:--

Search For:

Events

Displaying 1 to 0 of 0 items

Date/Time

Level

The search facilities are similar to the built-in log viewer: you can search according to

- Level: **ALL**, **INFO**, **WARN**, **ERROR** and **FATAL**
- Start and End date and time
- Search text. Note that, unlike the built-in log viewer, the standalone viewer search is case-insensitive. Also, since it uses the built-in text search features of the database, it ignores certain common words such as *and* and *the*.

Configuring the Stand-Alone Log Viewer

The log viewer as installed is ready to go. However, you may find that you need to alter certain settings if you make changes to the core configuration. The settings for the log viewer can be found on the appliance under

/usr/local/apache-tomcat/webapps/logviewer/WEB-INF/classes/swivel.properties

The following is the default configuration:

```
# Swivel client settings
ssl=false
server=localhost
port=8181
context=sentry
secret=secret
self-signed=true
logfolder=/home/swivel/.swivel/logs
serverid=1
dbtype=mysql
admingroups=SwivelAdmin
helpdeskgroups=SwivelHelpDesk
numberofdaystodeletelogs=60
```

Values you might need to change are:

- **serverid** - this is an identifier for the Swivel server. In a HA environment, if the database is shared between servers, you will need to change this value so that each server can be identified. The log viewer writes database records using this identifier, and only retrieves records that match that identifier.
- **admingroups** - a comma-separated list of Swivel groups that should be treated as administrators. If you add groups apart from the default **SwivelAdmin** group, you will need to update this.
- **helpdeskgroups** - similar to admingroups, but for Helpdesk users.
- **numberofdaystodeletelogs** - specifies how long log records should be kept in the database. You may wish to extend the default value of 60 days.