Sawmill Integration

Contents

Sawmill Integration with Swivel

Sawmill is a log analysis tool and can produce reports from Swivel logs. Log output from a syslog server can be also read by Sawmill.

Prerequisites

This article assumes you are running Swivel 3.2 or later and Sawmill Version 8

The Swivel Custom plugin for Sawmill (http://store.sawmill.co.uk/store/index.asp?pid=41) is also required

For Sawmill Enterprise Enterprise Edition a single copy license of the plug-in is provided for free, contact sales@sawmill.co.uk for further information.

Baseline

Swivel 3.5

Sawmill 8.08

Architecture

Swivel produces XML log files, there are several deployment scenarios which can be used:

1. These can be copied to a log server for analysis
2. Pulled from the Sawmill server from the PINsafe server.
3. Analysis of log files from Syslog log files.

Swivel Configuration

Ensure that the PINsafe logs are readable by the Sawmill server.

Sawmill Configuration

Copy Across PINsafe log filter files

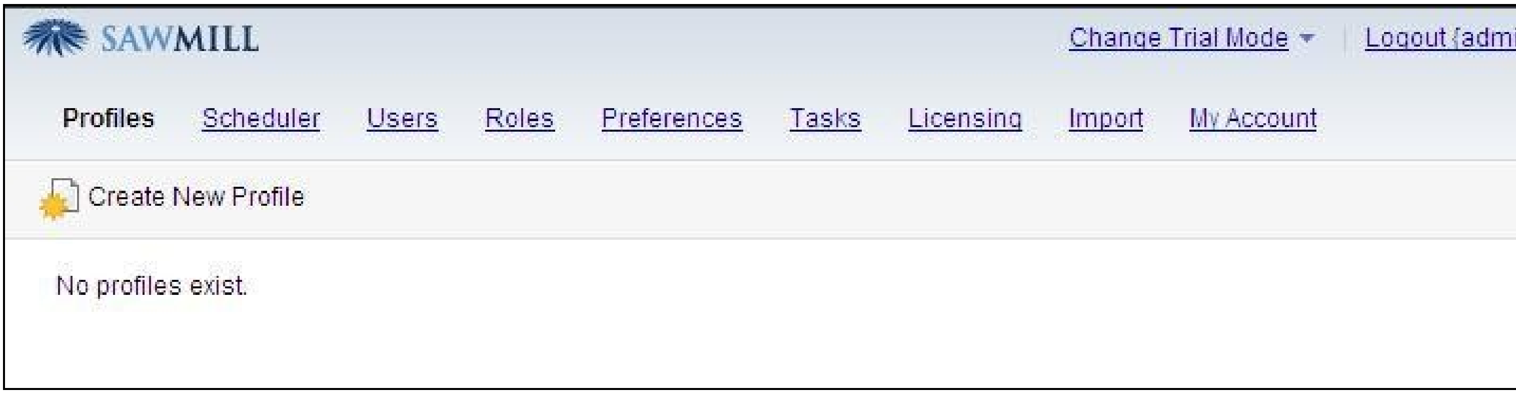
The Log format files (swivel_pinsafe_xml.cfg and swivel_pinsafe_syslog.cfg) need to be copied to the Sawmill Server into Sawmill 8\LogAnalysisInfo\log_formats

Example:

C:\Program Files\Sawmill 8\LogAnalysisInfo\log_formats

Start the New Profile Wizard

From Profiles select Create New Profile



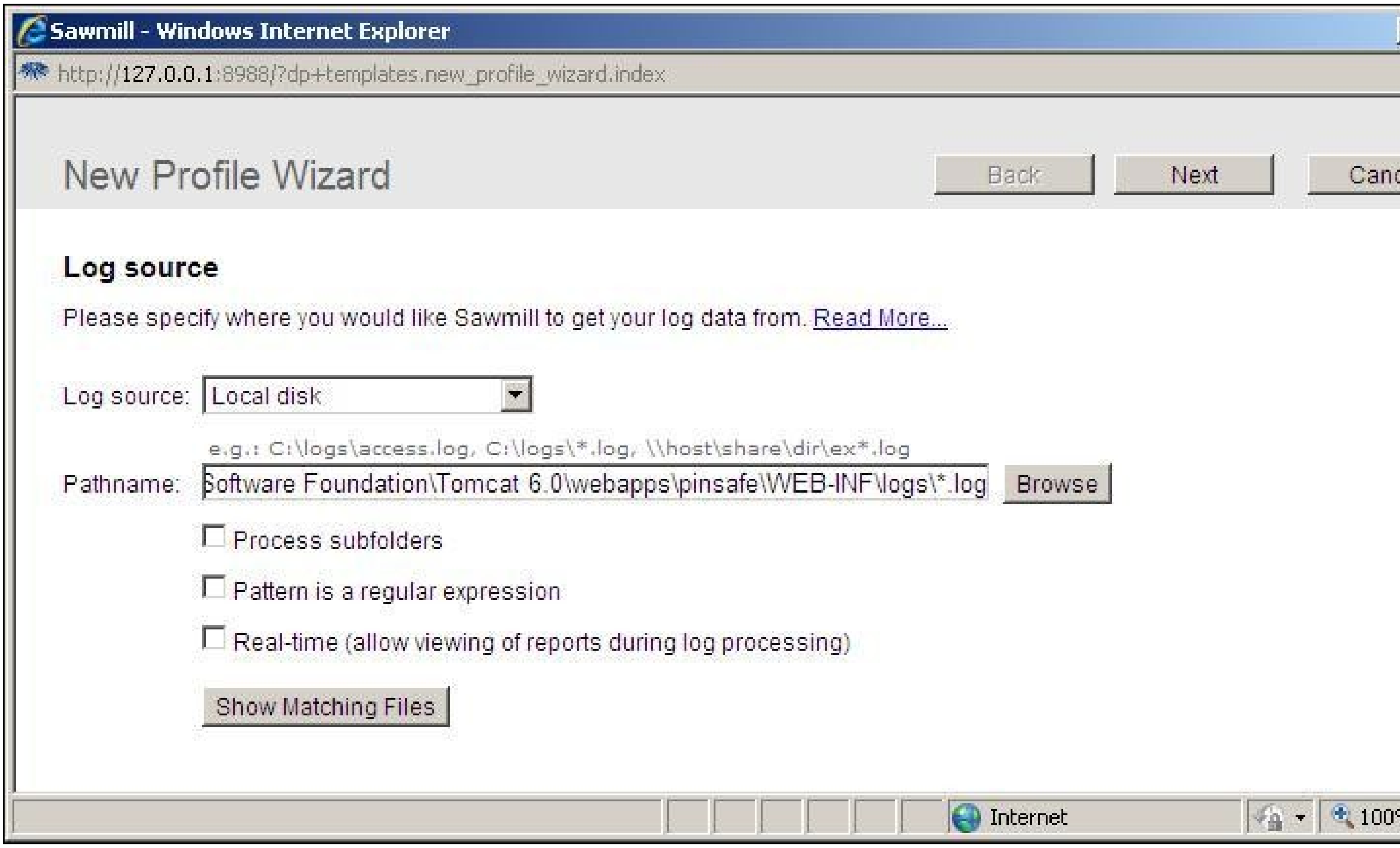
No profiles exist.

Enter the Log Source

Enter the log Source and any required information such as pathname for the PINsafe logs.

This setting will depend on which logs you are using, for example if Sawmill is deployed on the same server as PINsafe the path would be

```
\usr\local\apache-tomcat-x.xx\webapps\pinsafe\WEB-INF\logs\*log
```



http://127.0.0.1:8988/?dp+templates.new_profile_wizard.index

New Profile Wizard

Log source

Please specify where you would like Sawmill to get your log data from. Read More...

Log source: Local disk

e.g.: C:\logs\access.log, C:\logs\*.log, \\host\share\dir\ex*.log

Pathname: Software Foundation\Tomcat 6.0\webapps\pinsafe\WEB-INF\logs\*.log

☐ Process subfolders

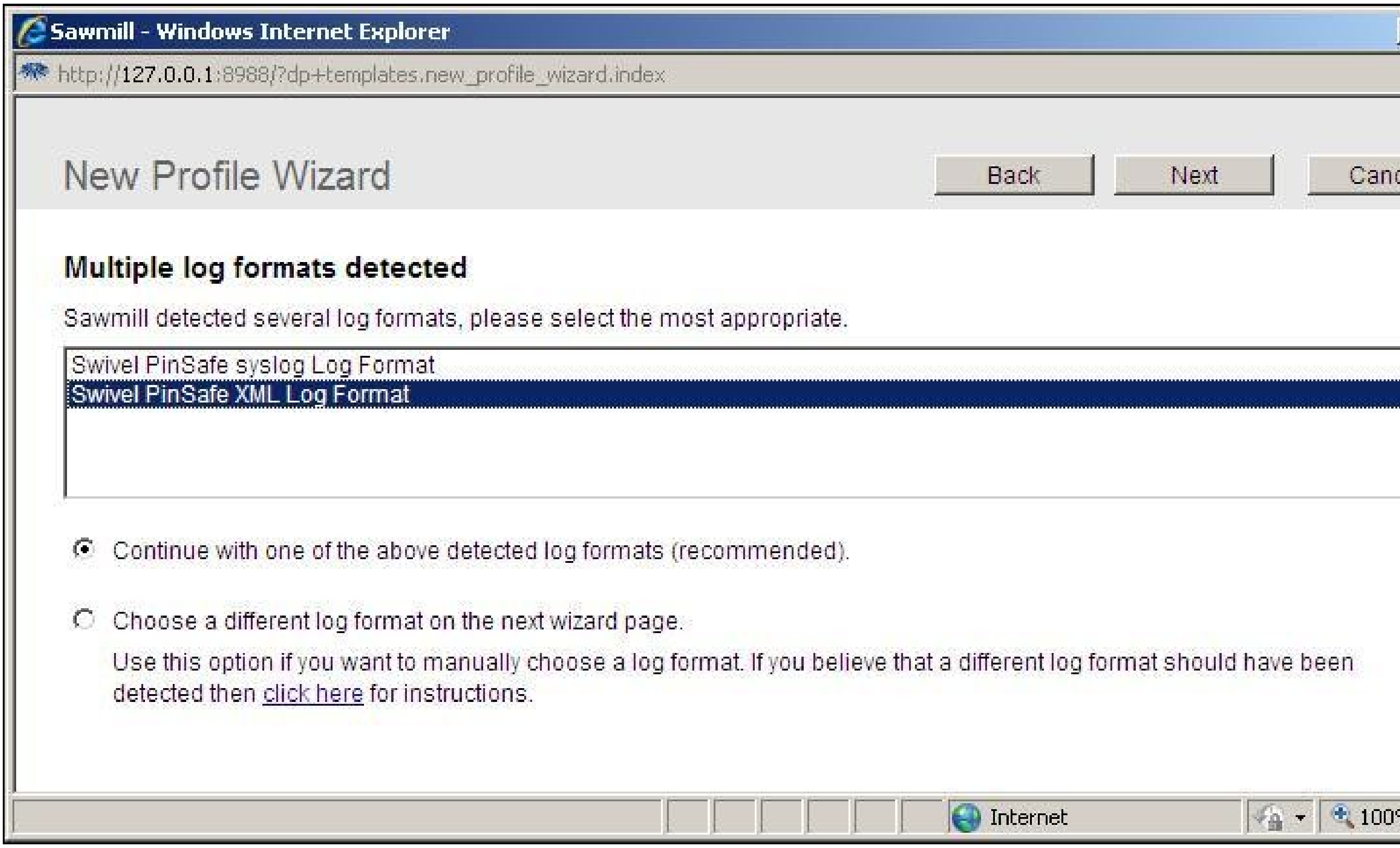
☐ Pattern is a regular expression

☐ Real-time (allow viewing of reports during log processing)

Sawmill will automatically attempt to identify the correct log format options.

Select Log Format

Select the required log format, then click on Next


Sawmill - Windows Internet Explorer
http://127.0.0.1:8988/?dp+templates.new_profile_wizard.index
Back
Next
Canc
Internet
100

New Profile Wizard

Multiple log formats detected

Sawmill detected several log formats, please select the most appropriate.

Swivel PinSafe syslog Log Format
Swivel PinSafe XML Log Format

● Continue with one of the above detected log formats (recommended).

○ Choose a different log format on the next wizard page.
Use this option if you want to manually choose a log format. If you believe that a different log format should have been detected then click here for instructions.

Complete Profile

The following steps complete the profile, these are standard Sawmill steps and deafuault settings are probably acceptable.

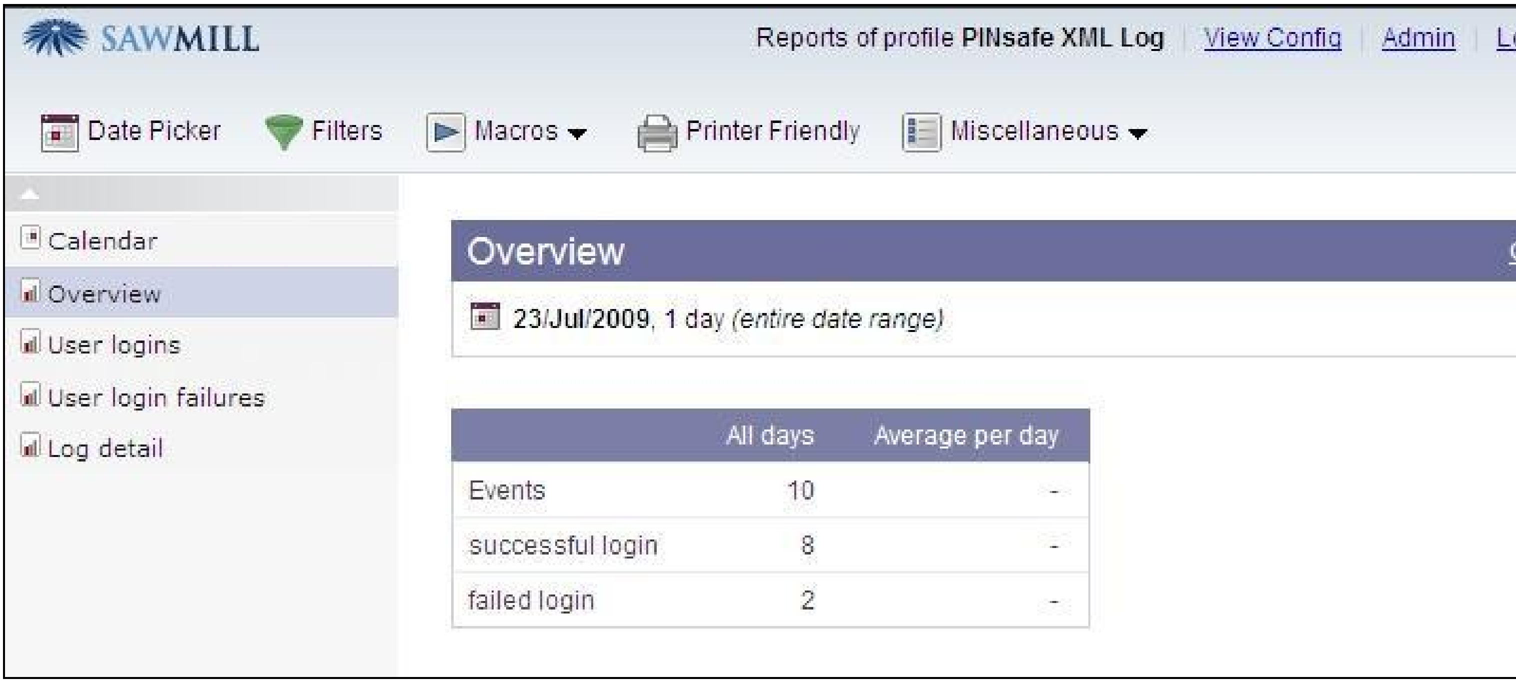
Enter the required Sawmill Database, then click on Next, then the Performance options.

Select the required Numerical Field options then click on Next.

Give a name for the profile, then click on Next.

Process Data and View Reports

Click on Process Data and View Reports to create the database and generate reports.



Overview

23/Jul/2009, 1 day *(entire date range)*

	All days	Average per day
Events	10	-
successful login	8	-
failed login	2	-

For scheduled processing of the PINsafe logs into the database, create a task in the Sawmill scheduler.

Verifying the Installation

Reports should show information, as in the above screen shot.

Troubleshooting

Check that the Swivel logs have some data in them, such as successful and failed login attempts..

View the Task log on the Sawmill server from Tasks/View Task Log, and check for any errors.

Known Issues and Limitations

If attempting to read PINsafe syslog output, the data needs to be sent to a syslog server first.

Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com

For Sawmill assistance please contact support@sawmill.co.uk.