

Title: Installation and demonstration of sawmill on windows OS. Generate a custom report.

Objective:

The objective of this experiment is to install and demonstrate the usage of Sawmill on a Windows operating system, specifically for generating a custom report.

Some information about “Sawmill”:

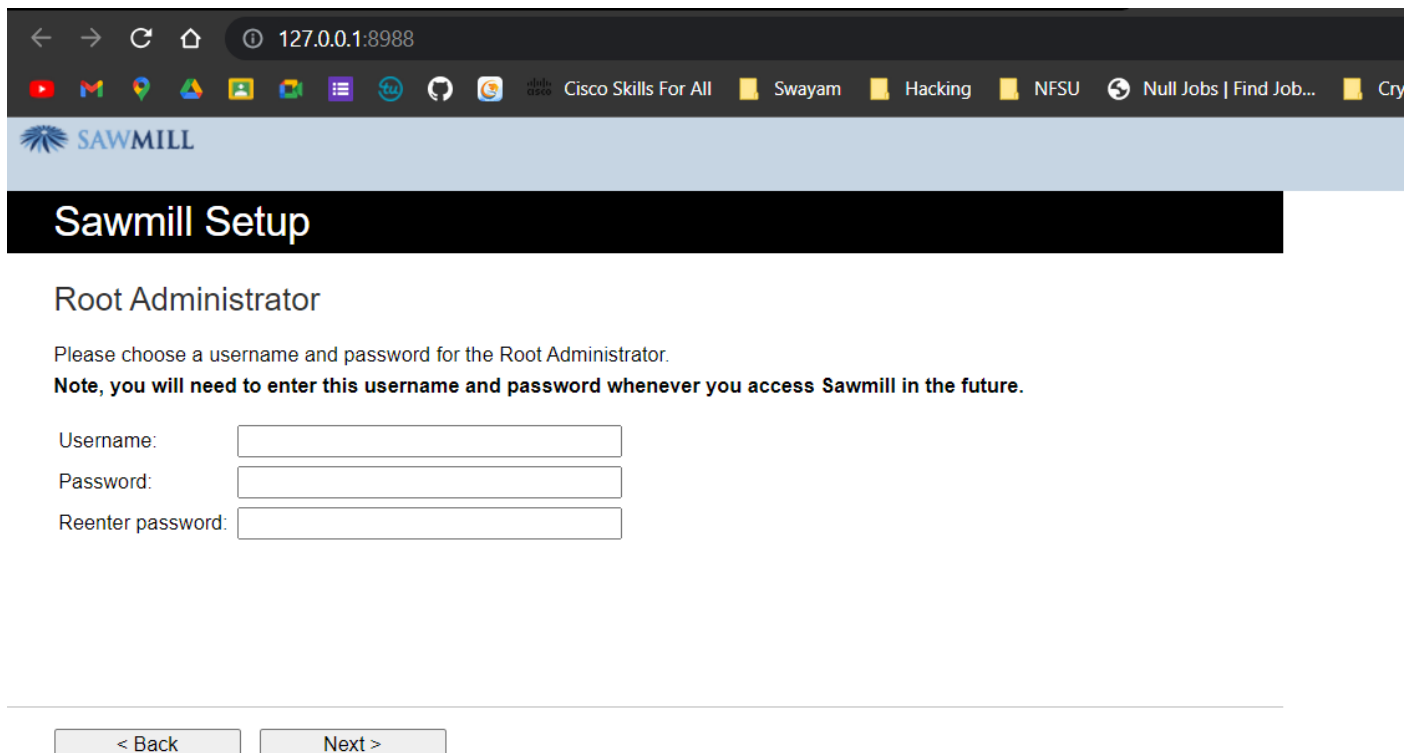
Sawmill software is used for log analysis and reporting, providing insights into website traffic and user behaviour. It processes log files and generates customizable reports, helping administrators and marketers understand website performance and security-related information.

Requirements:

Sawmill installer

Procedure/Experiment Steps:

1. Download the latest version of the Sawmill software from the official website.
2. Launch the installer and follow the on-screen instructions to install Sawmill on the Windows OS.
3. Once the installation is complete it ask for first time Configuration detail like Language, Licence agreement, username and password we need to set for the first time.



127.0.0.1:8988

SAWMILL

Sawmill Setup

Root Administrator

Please choose a username and password for the Root Administrator.

Note, you will need to enter this username and password whenever you access Sawmill in the future.

Username:

Password:

Reenter password:

< Back Next >

4. Configure the necessary settings, such as specifying the log file or data source for analysis.

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Back Next Cancel

Log source

[More Info](#)

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

Log source: Local disk or mapped/mounted disk ▼

Folder with optional file name, e.g.: C:\logs, C:\logs\access.log

Pathname: C:\logs [Add file mask](#) [Browse](#)

☐ Process subfolders [i](#)

Show Matching Files

Best Practice Tip

Log files are your company's asset and irreplaceable. We strongly recommend that you retain your historical log files for as long as possible. Read more in [Log File Management](#).

☐ Don't show again

5. Choose log file format to import the log data.

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Back Next Cancel

Manual log format selection

Select a log format.

Filter log formats by ... (1146)

- Microsoft Windows Event Log (CSV)
- Microsoft Windows Event Log (dumpeventlogs.vbs export)
- Microsoft Windows Event Log (Tab Delimited)
- Microsoft Windows Event Log (XML)
- Microsoft Windows Event Logs (Powershell ETVX to CSV)
- Microsoft Windows Firewall
- Microsoft Windows NT Scheduler
- Microsoft Windows NT Syslog
- Microsoft Windows NT4 Event (save as CSV)
- Microsoft Windows Performance Monitor
- Microsoft Windows Syslog
- Microsoft Windows XP Event Log (LogParser CSV Export)
- Microtech ImageMaker
- Microtech ImageMaker
- MikroTik Router
- MikroTik The Dude
- MikroTik Web Proxy
- Mirapoint Message Server

6. Set the appropriate log file parameters, including file location, log format, and any specific customization options.

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

BackNextCancel

Database

[More Info](#)

Please choose the preferred database.

Note: for highest performance, and the smallest database, choose Internal.

Database server type:

Database folder: (optional) [i](#)

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

BackNextCancel

Database performance options

[More Info](#)

Please specify whether or not to turn on database field indices and cross reference groups.

Enabling all will result in fast report generation but increases the database build time and size.

- ☒ Turn on database field indices
- ☒ Turn on cross reference groups

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

BackNextCancel

Numerical field options

[More Info](#)

Please select the numerical fields which you would like to have in the reports.

[Select All](#) | [Deselect All](#)

- ☒ Packets
- ☒ Size
- ☒ Unique source IPs

Sawmill - Google Chrome

127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

BackFinishCancel


Profile name


Please define a name for the new profile and click the Finish button.

Profile name:

The profile "Firewall" has been created

Please decide what to do next.

**Process Data & View Reports**
Take this action if no additional customization is required. This action goes straight to the reports and automatically starts building the database by processing all log data in the log source.

**View Profile in Config**
Take this action if you require additional customization prior to processing all log data in the log source, for example you wish to:

- Add or change log filters
- Turn on DNS lookup of IP addresses
- Add, delete or change database fields
- Other configuration options available in the Config pages

[Close Window](#)

- Initiate the log data import process to populate the Sawmill database.
- Once the data import is complete, navigate to the reporting section within Sawmill.
- Select the desired report customization options, including specific data fields, filters, date ranges, and visualization preferences.

test - Reports

Date PickerFiltersMacrosMiscellaneousPrinter FriendlyCustomize

Calendar

Overview

Overview

No date applied. The date filter "" is out of the available log date range.

	Avg/day
Messages	0
Length	0 B

Config OptionsDatabase / ToolsAdmin

Log Source

Log Parsing Filters

Log Filters

Log Fields

Log Processing

Database Server & Tuning

Database Filters

Database Fields

Cross Reference Groups

Reports Editor

Report Options

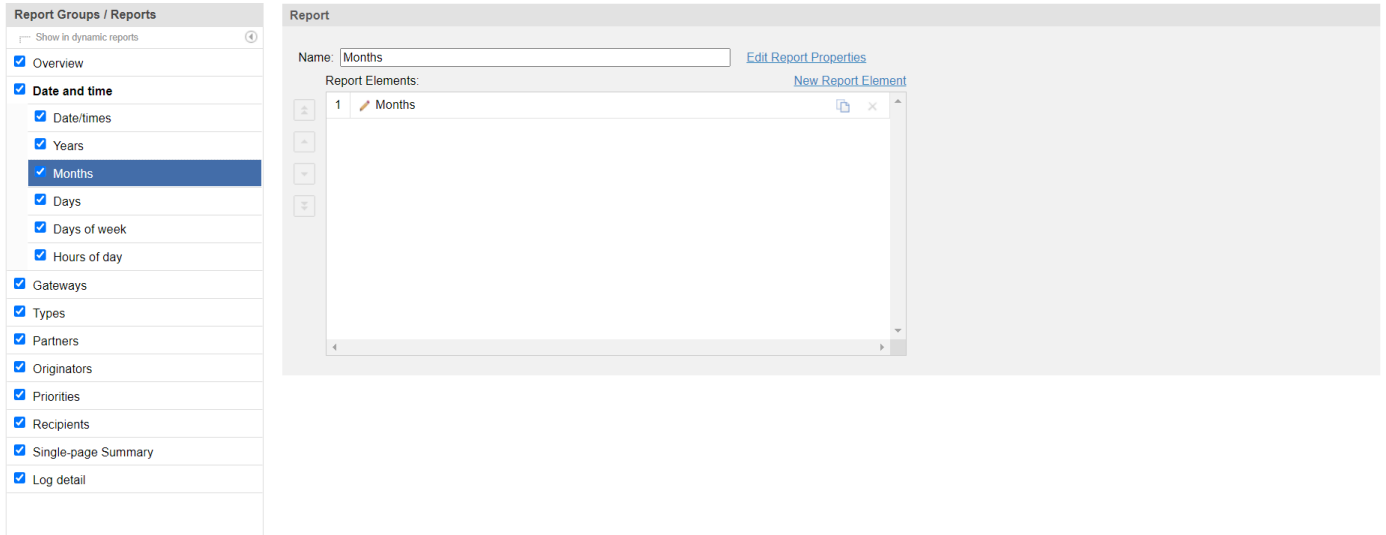
Report Fields

DNS Lookup, Support & Action Email

New Field Wizard

Snapons

10. Generate the custom report based on the selected parameters.



11. Review and analyze the generated custom report for insights and information.

Result:

The custom report generated from Sawmill provides valuable insights and analysis based on the selected parameters. It allows for in-depth exploration and understanding of the log data, assisting in identifying patterns, anomalies, and trends.

Conclusion:

The installation and usage of Sawmill on the Windows operating system enable the generation of custom reports, offering an effective approach to analyse and interpret log data. The custom report assists in understanding the logged information, identifying important trends, and making informed decisions.

Future Scope:

1. Exploring advanced customization options within Sawmill to generate more specific and targeted reports.
2. Integrating Sawmill with other security tools or log sources to consolidate and analyze data from multiple sources.
3. Conducting further research on log analysis methodologies and techniques to enhance the effectiveness of Sawmill reports.