smoothwall®

The Web You Want

Carisbrooke Update 1

End User Guide

Contents

Introduction

Hot on the heels of the Carisbrooke release, Carisbrooke Update 1 (September 2015) includes two new features.

Search Term Logging and Reporting

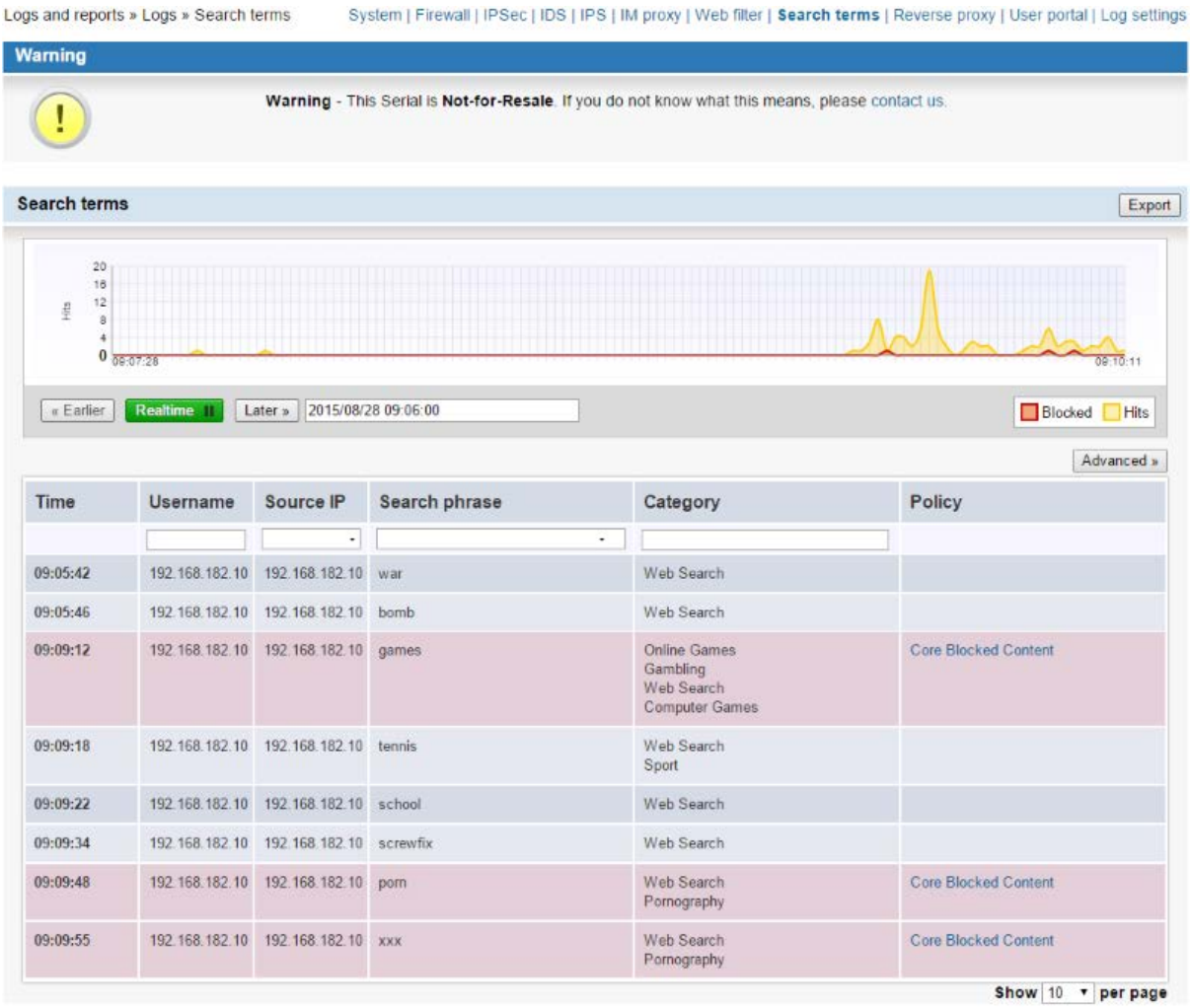
Scope

To improve the reporting of the Guardian **search terms** filtering by offering a new log viewer, plus improved reporting sections and templates.

What's changed

Search Term Log viewers

Introduction of a new log viewer similar to the Web filter and Email log viewers. This is added in realtime mode to **Logs and Reports > Realtime > Search terms**, and in the non-realtime log through **Logs and Reports > Logs > Search terms**.



The basic operation of this log viewer is no different to the operation of either Guardian's Web filter logs, or Anti-Spam's Email logs. It does, however, display different information by default.

The available columns are:

- **Time** — The date and time that the request was made
- **Username** — The username of the user who made the request
- **Source IP** — The IP address that the request came from

- **Search domain** — The domain name of the search engine used, using the format:

  `<domain> (<search_engine_if_known>)`

  for example: www.google.com (Google)

- **Search phrase** — The phrase the user searched for, for example, “football clubs in England”
- **Category** — The matching categories
- **Policy** — The matching Guardian filtering policy

You can filter the log viewer by typing into the relevant column. **Search phrase** filtering also has a drop down menu option which allows for the exclusion of **search suggestions** from the results. Search suggestions are entries added by features such as Google’s predictive search, and can often inflate and confuse the results by having entries for built up searches, such as, “f”, “fo”, “foo”, “foot” , and so on.

New reporting section — Search phrases and users

A new reporting section for custom and scheduled reports has been added for detailing search terms — **Search phrases and users**. This is a hybrid between the search terms section and the individual user section. This outputs:

- The users who made the requests
- The IP addresses where the requests originated from
- Any search phrases

This is almost identical to the search term log viewer described above with the most significant difference that it can be scheduled as it is a reporting section.

The section contains a fairly standard set of filtering options:

- Display top
- Exclude search suggestions — This works in the same way as the Search phrase filtering described above
- Category
- Client IP
- Exclude domain
- Group
- Username

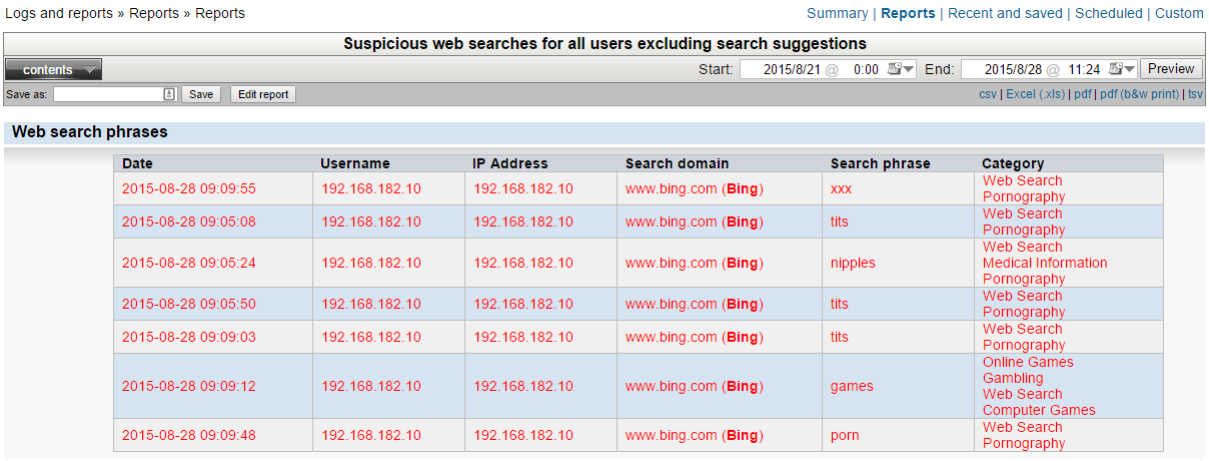
Advanced options are also available, allowing you to:

- Exclude results
- Specify the HTTP request methods
- Specify the request status
- Filter the URLs found

Templates

To use the new reporting section there are two new templates available under **User analysis**:

- Suspicious web searches for all users excluding search suggestions
- Web searches for a specific user



Logs and reports » Reports » Reports

Summary | **Reports** | Recent and saved | Scheduled | Custom

Suspicious web searches for all users excluding search suggestions

contents | Start: 2015/8/21 @ 0:00 | End: 2015/8/28 @ 11:24 | Preview

Save as: | Save | Edit report | csv | Excel (.xls) | pdf | pdf (b&w print) | tsv

Web search phrases

Date	Username	IP Address	Search domain	Search phrase	Category
2015-08-28 09:09:55	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	xxx	Web Search Pornography
2015-08-28 09:05:08	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	tits	Web Search Pornography
2015-08-28 09:05:24	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	nipples	Web Search Medical Information Pornography
2015-08-28 09:05:50	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	tits	Web Search Pornography
2015-08-28 09:09:03	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	tits	Web Search Pornography
2015-08-28 09:09:12	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	games	Online Games Gambling Web Search Computer Games
2015-08-28 09:09:48	192.168.182.10	192.168.182.10	www.bing.com (**Bing**)	porn	Web Search Pornography

Setup

No setup steps are required

Troubleshooting

No new troubleshooting steps have been introduced.

Refreshed System > Maintenance > Updates Page

Definitions

- A **Release** is a major castle version (such as Carisbrooke)
- An **Update** is a minor version increment on top of a castle (such as Carisbrooke-1)

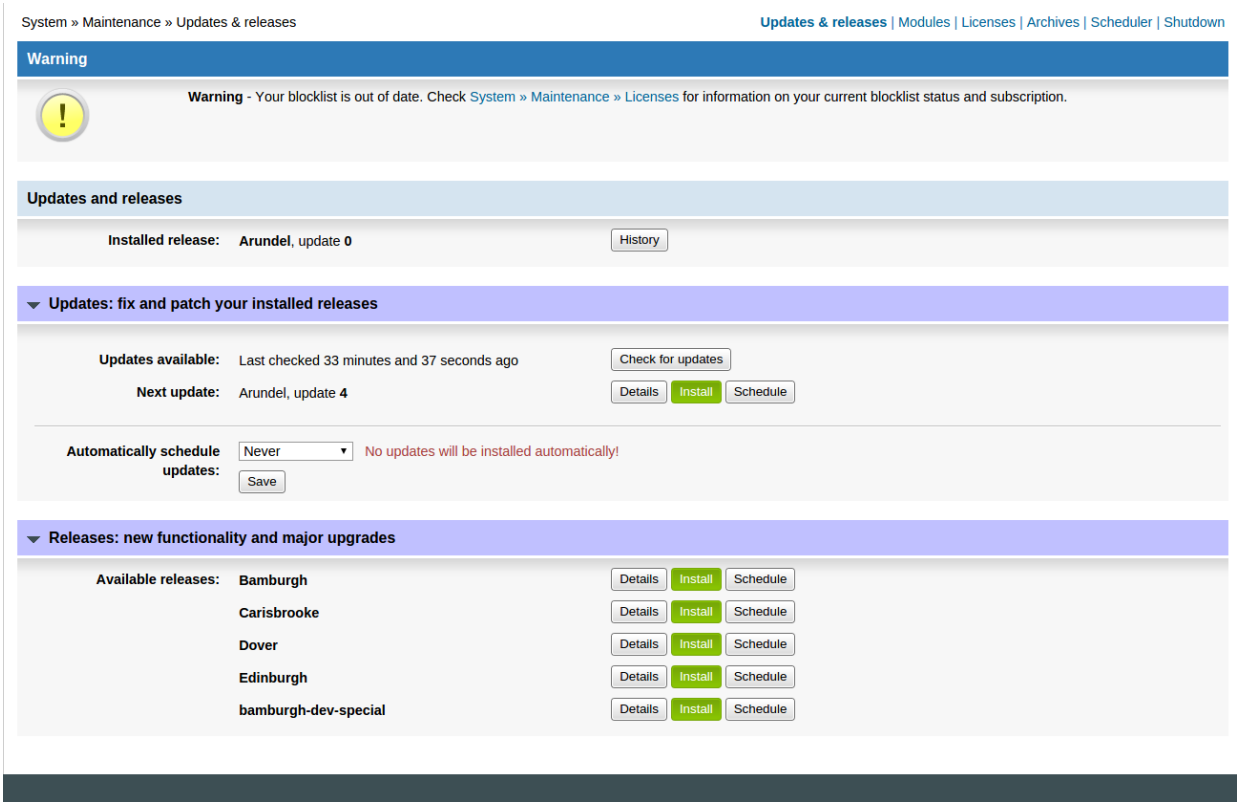
Scope

Revise the way we provide updates to include a concept of major/minor versions, user-selectable major versions, and automatic installs of minor versions. A number of other enhancements around the update mechanism itself have also been made.

What's changed

Single-user update improvements

- The Updates page is now Updates & Releases.
- "Main" release numbers are all gone; replaced with Releases and Updates. This matches what Smoothwall are actually releasing now!



- **Install** now means "download, install and reboot" for both **Releases** and **Updates**, reducing the number of intermediary states a Smoothwall can be in.
- Descriptions are available via the **Details** button for any **Release** or **Update**.
- **Updates** (minor versions) may be placed on a recurring schedule to automatically download, install, and reboot. The schedule is daily.
- **Releases** and **Updates** can still be scheduled (used to be "Install at this time"), but may be scheduled independently.
- To prevent system corruption, the user interface is locked during the installation process. A progress bar is displayed throughout.

- The **System > Maintenance > Modules** page has had a visual refresh, but the functionality is identical.

High Availability update improvements

- Attempting to update the master past the failover node will result in an appropriate warning to update the failover node first
- The standby node will not replicate settings from the master unless both are at the same version level

What hasn't changed

- The ease with which updates arrive on a Smoothwall!
- Central Management replication is unaffected by the version restrictions in High Availability

Setup

Automatically schedule updates migrates as "Never", so we will not automatically apply updates unless expressly asked.

Troubleshooting

Warnings and errors are reported on the interface and under the **Update transcript** section of the System logviewer (**Logs and reports > Logs > System**), while the most common classes of problem (especially surrounding high availability configurations) have been programmatically prevented.