

Proofpoint Smart Search



Proofpoint Smart Search™ enhances Proofpoint's built-in logging and reporting with advanced message tracing, forensics and log analysis capabilities, offering easy, real-time visibility into message flows across your entire messaging infrastructure. Search and analyze all of your message logs from one convenient, easy-to-use GUI—even across globally distributed Proofpoint deployments.

features

Enterprise-class log search, message tracing and analysis

Proofpoint Smart Search helps you rapidly trace both inbound and outbound messages, analyze how messages were processed by the Proofpoint system and report on the disposition and status of any email message.

With Proofpoint Smart Search, email administrators or IT helpdesk staff can instantly locate messages, understand how they were handled and quickly respond to a wide variety of email troubleshooting or investigation requests. For example:

- **Message tracing:** An executive asks the helpdesk what happened to an important message that was never received by a business partner. Proofpoint Smart Search can quickly locate the message and report on its delivery status.
- **Investigation:** Has an end user been exchanging email with a competitor? What were the subjects of those messages? Proofpoint Smart Search has the answers.
- **Forensics:** The legal department needs to know exactly when and to which server an important notification was delivered. Proofpoint Smart Search provides easy-to-understand details about message handling and delivery.
- **Compliance:** Quickly find all messages related to a specific compliance incident or an entire class of violations. Proofpoint Smart Search helps you quickly understand which Proofpoint rules were triggered and how messages were routed as a result.
- **Trend analysis:** How many outbound messages in the past month triggered a specific Proofpoint rule? Proofpoint Smart Search makes it easy to mine information from consolidated archives of large, complex log files.

Real-time, consolidated log indexing

Powered by IT search technology from Splunk, Proofpoint Smart Search can locate any message across your entire Proofpoint deployment in seconds.

Proofpoint Smart Search consolidates logs from all Proofpoint agents—even across globally deployed clusters—and indexes them for rapid searching. Logs from multiple sources are automatically correlated for a 360-degree view of message handling and disposition.

Log information is continuously updated so that—within minutes of a message's receipt or transmission—details about that message can be found using Proofpoint Smart Search's easy-to-use GUI.

Proofpoint Smart Search is architected for integration with non-Proofpoint messaging systems, allowing you to consolidate logs from your entire messaging system including downstream mail servers, encryption servers and other gateway devices. Messages can be traced across your entire messaging infrastructure.

Empower IT helpdesk staff

Proofpoint Smart Search can be used by IT helpdesk staff to answer the most common email troubleshooting and investigation requests, without requiring any special training or access to your Proofpoint systems. The powerful search and analysis capabilities of Proofpoint Smart Search can be used without impacting the performance of your mission critical email systems, because it operates independently of your Proofpoint Protection Server® software and Proofpoint Messaging Security Gateway™ appliances.



Proofpoint Smart Search at a Glance

- Real-time processing, indexing and correlation of all Proofpoint logs.
- Powerful search features to trace messages across all agents in seconds.
- Easy-to-understand search results display the delivery, timing, rule triggering and disposition for any inbound or outbound message.

Multiple Data Views

- **Summary:** Browse time, sender, recipient, subject and Proofpoint filter actions taken on messages within a given timeframe.
- **Detailed:** Drill-down on individual messages with easy-to-understand detail tables.
- **Raw logs:** View message data in its original log format. Click on any log element to easily narrow your search criteria.

360-degree Insight

Architected to consolidate log information from your Proofpoint servers and other messaging systems including:

- Downstream mail servers
- Archiving systems
- Encryption devices

Contact Proofpoint for the latest information on support and integrations for third-party systems.

Proofpoint Smart Search

features (continued)

Powerful, easy-to-use search interface

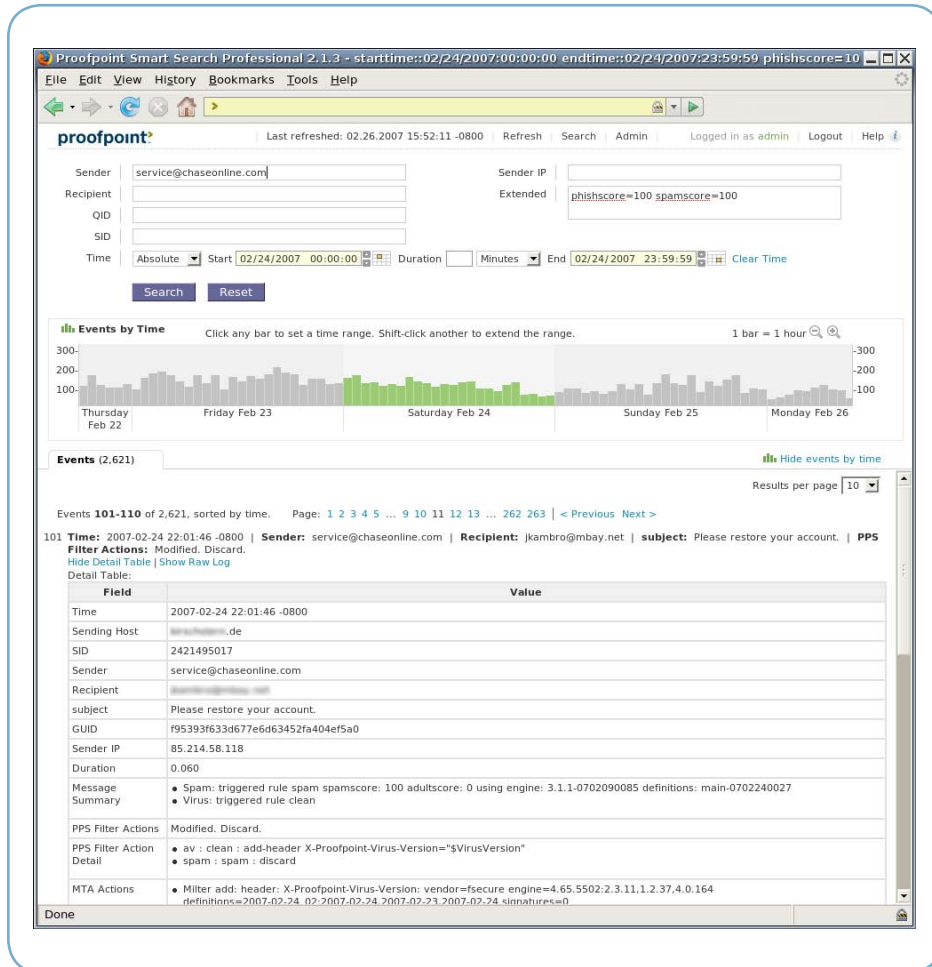
Proofpoint Smart Search features a convenient web-based interface for browsing and searching message information. A search results pane translates data from raw message logs into easy-to-read, actionable information. The summary view shows message time, recipient, subject and all filter actions. Drill-down on individual messages to expose a detailed view that includes the Proofpoint rules that were triggered, Proofpoint message dispositions, MTA dispositions, destination IP address and much more. Message data can also be viewed in its original, raw log format.

Using Proofpoint Smart Search's easy-to-use search interface, messages can be located with pinpoint precision in seconds. Search for messages using a wide variety of criteria including message sender, message recipient, subject, relative or absolute time-frame, sendmail QID and Proofpoint session ID. Extended free-text searching allows you to build custom searches using regular expressions and Boolean operators.

Easy deployment

Proofpoint Smart Search is deployed as a separate appliance that installs quickly and easily alongside your existing Proofpoint servers. In some cases, Proofpoint Smart Search can be deployed as a software module on an existing Proofpoint master appliance.

proofpoint smart search interface



Powered by Splunk

Proofpoint Smart Search incorporates IT search technology from Splunk, enabling real-time indexing, high-speed searching and rapid analysis of messaging logs.



See Proofpoint Smart Search in Action

To see a demonstration of Proofpoint Smart Search, please visit the following URL:

<http://www.proofpoint.com/pssdemo>

Proofpoint Smart Search GUI

The screenshot at left shows the Proofpoint Smart Search graphical user interface. Messages can be located quickly and easily using intuitive controls.

In this example, the event timeline has been used to narrow the search to a specific day (the green bars indicating Saturday, February 24th). This interactive timeline makes it easy to graphically drill-down on specific time periods.

In addition, the "Extended" search capabilities have been used to narrow the message list to only those messages with high Proofpoint phish and spam scores. These sorts of searches are easy to create using Proofpoint Smart Search's point-and-click interface. When in the raw log view, any portion of the log data can be clicked to automatically add extra filtering terms to the Extended search field—letting you quickly zero-in on just the message types you are concerned with.

Below the timeline, you can see the detailed view for a single message, displaying all the message handling information in an easy-to-understand format.

©2007 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway and Proofpoint Smart Search are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 10/07