



Proofpoint Smart Search

Enterprise-class Message Tracing, Log Search and Analysis

Proofpoint Smart Search™ offers easy, real-time visibility into message flows across an organization's entire messaging infrastructure, using built-in logging and reporting capabilities with advanced message tracing, forensics and log analysis capabilities. Search, analyze and export message logs from the centralized graphical user interface, even across globally distributed Proofpoint deployments.

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 an organization's Proofpoint deployments. Proofpoint Smart Search is intended to be used by both technical and non-technical personnel with an easy-to-use, intuitive interface for fielding common help desk questions.

Proofpoint Smart Search	
Feature	Benefit
Real-time processing, indexing and correlation	Real-time processing, indexing and correlation of all Proofpoint Enterprise Privacy and Proofpoint Enterprise Protection email logs.
Powerful search features	Powerful search features to trace sender, recipient, message subject and content across all agents in seconds.
Easy-to-use search options	Easy-to-use search options that support wildcards, and enable search by rules based on company policy.
Easy-to-understand search results	Easy-to-understand search results display the delivery, timing, rule triggering, and disposition for any inbound or outbound message.
Easy access to quarantined messages	Quarantined messages can be easily accessed from Proofpoint Smart Search results by simply clicking a link.

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. Results show message time, sender, recipient, subject and all filter actions. Simple drill-down on individual messages exposes a detailed view that includes the rules that were triggered, message dispositions, MTA dispositions, destination IP address, and much more. Message data can also be viewed in its original, raw log format.

With the 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 timeframe, sendmail QID, module ID, company policy based rules and Proofpoint session ID. Extended free-text searching allows users to build custom searches using regular expressions and Boolean operators.

Proofpoint Smart Search

Enterprise-class log search, message tracing and analysis

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:** Proofpoint Smart Search can quickly locate a message and report on its delivery status.
- **Investigation:** Proofpoint Smart Search has the ability to search for all messages using a variety of attributes (subject, sender, recipient, domain, etc.) to quickly and easily find information.
- **Forensics:** Proofpoint Smart Search provides comprehensive details about message handling and delivery that enables administrators to easily determine the outcome and location of any particular message.
- **Compliance:** Quickly find all messages related to a specific compliance incident or an entire class of violations. Proofpoint Smart Search helps users quickly understand which Proofpoint rules were triggered, and how messages were routed as a result.
- **Trend analysis:** Proofpoint Smart Search makes it easy to mine information from consolidated archives of large, complex log files.

Real-time, consolidated log indexing

Proofpoint Smart Search can locate any message across an organization's entire Proofpoint deployment in seconds, unlike other solutions that take more time due to unconsolidated logs and having to search each appliance individually.

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.

The screenshot shows the Proofpoint Smart Search interface. At the top, there are search filters for Sender, Recipient, Subject, Module ID, Time, Sender Hostname, Attachment Name, Sender IP Address, Virus Name, QID, Rule ID, and Process. Below the filters is a 'Search' button. The 'Recent Searches' section shows three recent searches. The 'Results' section displays a table with columns for Date, Sender, Recipients, Subject, and Final Action. Below the table is a 'Raw Log' view showing detailed log data for the selected message.

Date	Sender	Recipients	Subject	Final Action
2010-10-12 13:06:29 [UTC-0700]	hyacinthe@example.com	mtorme@proofpointdemo.com	Copy DVD Movies - (No Cost) Software Included	Quarantined; Discarded
2010-10-12 13:06:29 [UTC-0700]	yanjun@example.com	apalmer@proofpointdemo.com	Employment Offer - Contact Us!	Quarantined; Discarded
2010-10-12 13:06:28 [UTC-0700]	jeanette@example.com	rstarr@proofpointdemo.com	Search For Singles FREE.	Quarantined; Discarded

Raw Log

```
[2010-10-12 13:06:28.739859 -0700] rprt s=rsppgd32x mod=session cmd=connect ip=10.25.1.146 country=** lip=10.25.1.63 prot=smtpt:mltr hops_active=f routes=internalnet notroutes=frewallsafe_psm_client_users.spfsafe_perlwait=0.001
[2010-10-12 13:06:28.741426 -0700] rprt s=rsppgd32x mod=session cmd=resolve host=admin.proofpointdemo.com resolve=ok rev erse=admin.proofpointdemo.com routes= notroutes=
[2010-10-12 13:06:28.743216 -0700] info s=rsppgd32x mod=mail cmd=hello value=admin.proofpointdemo.com routes=
[2010-10-12 13:06:28.748001 -0700] rprt s=rsppgd32x m=1 x=o9CK6Sr0022641 mod=mail cmd=env_from value=jeanette@example.com qid=o9CK6Sr0022641 ts= routes=outbound notroutes= host=admin.proofpointdemo.com ip=10.25.1.146
[2010-10-12 13:06:28.750545 -0700] rprt s=rsppgd32x m=1 x=o9CK6Sr0022641 mod=mail cmd=env_rcpt r=1 value=rstarr@proofpointdemo.com verified= routes=default_inbound notroutes=ts
[2010-10-12 13:06:28.762339 -0700] info s=rsppgd32x m=1 x=o9CK6Sr0022641 mod=session cmd=data rcpt_routes=default_inbound env_routes=ts data_rcpt_routes=ts notroutes=
```

About Proofpoint

Proofpoint focuses exclusively on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging.

Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA
94089
1.877.647.6488

Multiple data views with Proofpoint Smart Search

- **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 log element to easily narrow search criteria.
- **Export results:** Export search results in CSV or XML format.