

# Proofpoint Content Compliance Module



The Proofpoint Content Compliance™ module, a component of the Proofpoint Protection Server® and the Proofpoint Messaging Security Gateway™, allows enterprises to define and enforce acceptable-use policies for message content and attachments. Proofpoint Content Compliance can be used to identify and prevent a wide variety of inbound and outbound policy violations—including offensive language, harassment, file sharing, and many more.

## features

### Rapid creation of acceptable-use policies

Proofpoint Content Compliance includes common filters and standard dictionaries to help quickly establish corporate messaging policies or support existing policies, giving organizations an immediate benefit in controlling the most frequently encountered issues with messaging abuse. Examples of acceptable use policies that can be created include:

- Maximum message size
- Allowable attachment types with attachment type verification
- Acceptable encryption policy
- Monitoring for offensive language
- Maximum number of recipients and/or attachments
- Custom disclaimers or footers automatically appended to messages

### Enterprise-grade content compliance filtering

Both inbound and outbound email messages are monitored and classified in real-time, providing organizations with proactive control of their messaging infrastructures. Any suspected or noncompliant email is flagged and can be quarantined for further review or audit, before exposing the company to any liability. A point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content.

The four key messaging analysis functions of Proofpoint Content Compliance are:

#### ○ Policy Definition

Easily define a specific set of policies for different groups, email routes, and compliance areas. The Proofpoint Messaging Security Console™ provides a 100 percent web-based, graphical user interface for managing all types of messaging policies. (See reverse for example message attributes that can be used to build policies.)

#### ○ Real-time Monitoring

Monitor email message flow, including attachments, for compliance throughout your enterprise.

#### ○ Enterprise Classification

Filtered messages can be categorized into any number of compliance or content-related classifications.

#### ○ Flexible Message Handling Options

Based on your defined policies and classifications, Proofpoint Content Compliance lets you take action on messages that violate these rules. For example, an email containing suspected harassing content could be forwarded to the human resources department for further review. Proofpoint supports the widest array of message dispositions in the industry. Options include sending the noncompliant message to a quarantine, rejecting or discarding the message, replying to the sender with explanatory text, redirecting the message for further review, rerouting to other systems (such as secure messaging systems), and many more.



### Complete Content Security

Beyond the inbound messaging threats of spam, viruses and phishing attacks, corporations, universities and government organizations are looking for messaging security solutions that help them enforce outbound email policies, defend against leakages of confidential information and help them comply with email-related regulations. Proofpoint provides a complete suite of easy-to-configure modules that solve these problems.

Proofpoint Content Compliance allows acceptable use policies to be created based on a wide variety of message attributes, dictionary-based content, regular expressions and keyword matches. Additional, advanced content analysis features can be enabled with the optional Proofpoint Digital Asset Security and Proofpoint Regulatory Compliance modules:

- The advanced, unstructured data detection capabilities of Proofpoint Digital Asset Security™ keep valuable assets and confidential information from leaking outside your organization via email.
- With the ability to detect all types of structured privacy information—such as private identity, healthcare and financial information—Proofpoint Regulatory Compliance™ ensures customer and employee data privacy and protects your organization from liabilities associated with data protection and privacy regulations such as HIPAA and GLBA.

# Proofpoint Content Compliance Module

## customizable

---

### Meet internal policy requirements

Proofpoint Content Compliance compares message content with dictionaries in order to protect businesses from the use of inappropriate or offensive content and other issues that can surface through email usage. A variety of built-in dictionaries are supplied with the Content Compliance module, such as an offensive language dictionary that can be employed to discourage the use of improper or abusive language.

### Adapts to unique corporate requirements

In situations where Proofpoint's preconfigured dictionaries do not meet a company's or department's needs, custom dictionaries can be created to manage specific policies. Furthermore, preexisting databases can be imported to leverage policies and information already in use in your company.

Custom policies are easily created using Proofpoint's graphical user interface, which allows messages to be analyzed and processed based on a comprehensive list of message attributes such as:

- Attachment attributes including: File size, filename, file extension, number of files, number of files in archive, file depth in archive, presence of protected files, presence of corrupt archives, etc.
- Message attributes including: Text in message body, dictionary scores, message size, presence of encryption, MIME type, HTML tags, etc.
- Message header, envelope and routing attributes including: Email headers, envelope recipient, envelope sender, sender hostname, sender IP address, recipient, number of recipients, DNS block list status, message route (e.g., inbound or outbound), etc.
- System attributes including: Total concurrent connections, total connections, total messages, etc.
- Recipient group membership: Different policies can be defined and enforced for different groups of users. As in all Proofpoint modules, policies can be defined at the global, group or individual end-user level.

### Attachment scanning and support for custom or proprietary document types

Built-in attachment scanning capabilities allow you to apply your policies to the contents of message attachments. Policies can be enforced on content in more than 400 types of document attachments, including word processing formats (such as Microsoft Word), spreadsheets (such as Microsoft Excel worksheets), Adobe Acrobat PDF documents, presentation formats (such as Microsoft PowerPoint) and documents included in archives (including ZIP, GZIP, TAR, and TNEF formats).

In addition to the hundreds of built-in document types that Proofpoint's outbound email security modules natively understand, administrators can use Proofpoint's File Type Profiler to easily extend support to new, custom or proprietary file types (e.g., proprietary CAD/CAM formats).

### Benefits

Proofpoint's solutions are designed, from the ground up, to provide a balance of robust content control and corporate flexibility. Benefits of the Proofpoint Content Compliance module include:

- Powerful policy enforcement
- Rapid deployment
- Real-time message classification
- Adaptable to meet the custom needs of your business
- Message disposition flexibility

©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, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, and Proofpoint Messaging Security Console 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