1 Product Evaluation Guide

Overview

Thank you for choosing to evaluate Websense Cloud Email Security.

Websense Cloud Email Security provides leading protection from today's converged email and Web 2.0 threats. The cloud security model reduces costs and complexity while allowing businesses to retain control and eliminate uncertainty through industry-leading service level agreements. With Websense Cloud Email Security, customers gain mission-critical security while enabling a consolidated security strategy with the trusted leader in Essential Information Protection™.

Why Websense Cloud Email Security?

Today, email security is fundamentally different than it was only a short time ago. Malicious threats used to be concealed in attachments, but today Websense Security Labs reports that 85% of unwanted emails contain a link to a Web site. Protecting email users against converged Web and email threats requires email security that is integrated with the best-in-class Web security expertise of Websense.

The Websense ThreatSeeker Network™ uses more than 50 million real-time data collecting systems that continuously monitor Internet content for emerging threats, and feeds this intelligence to its email, Web, and data security solutions. The Websense ThreatSeeker Network scans more than 40 million Web and 10 million email sites every hour, and captures more than 10 million unsolicited spam, phishing, or exploit campaigns every day. ThreatSeeker allows Websense to adapt to the rapidly-changing Internet at speeds that are not possible for traditional security and email filtering solutions.

Websense Cloud Email Security stops spam, virus, phishing, and other malware attacks before they reach the network, dramatically reducing email bandwidth and storage requirements. Because there is no hardware or software, business costs associated with installation, troubleshooting, and applying patches or upgrades are eliminated.

With the rise of botnet-driven spam storms, email volumes can quickly spike and overwhelm on-premise email infrastructure. Websense Cloud Email Security acts as a shock absorber that seamlessly and predictability handles large email volume spikes and reduces the capacity required for on-premise email infrastructure.

Highly effective, Websense Cloud Email Security is backed by a 99% spam detection SLA and has received premium antispam certification from West Coast Labs (an independent testing facility) for stopping 99% of spam with zero false positives. Websense utilizes multiple layers to maximize protection from spam and viruses with each message processed through 3 commercial antivirus engines, and the Websense ThreatSeeker Network. The proactive protection of ThreatSeeker stops zero-hour attacks hours, and often days, in advance of traditional antivirus technologies, greatly shortening the window of exposure.

Content filtering provides granular content analysis on inbound and outbound email. It includes comprehensive and configurable lexical dictionaries and polices to help organizations comply with regulations such as HIPAA, SOX, and global privacy standards.

Encryption secures email communications among business partners and individuals to ensure that their email content is safe and private. With nothing required on-premises or at the endpoint, cloud encryption is a simple and cost-effective alternative to client-based encryption solutions, which can be difficult to deploy and maintain.

Summary and detailed reports, combined with the dashboard feature, show key email indicators and provide forensic details on the real-time email security protection provided by Websense. Administrators can delegate and schedule reporting access to any department within the organization to enable appropriate managers to receive reports automatically by email.

Websense has multiple global data centers, and the cloud service has been certified to ISO27001 standards to provide the highest degree of global and localized security, privacy, and confidentiality. All email is routed to 2 data centers in different geographical regions to provide redundancy and fault tolerance. The service is backed by a 99.999% uptime SLA and includes email spooling and disaster recovery provisions as standard. Built-in redundancy, failover, and business continuity ensure that email always stays up and running, even if the network is temporarily unavailable.

Methodology

This guide has been created to help you evaluate Websense Cloud Email Security once you have set it up. (For setup instructions, please see the *Websense Cloud Email Security Getting Started Guide*.) This guide demonstrates the ease with which an IT administrator can configure, monitor, and analyze inbound and outbound mail delivery while taking into account the varying requirements of specific users and departments within an organization.

The guide is organized into the task areas most beneficial for the IT administrator:

- **Dashboard** – View up-to-date graphical data for email volumes, inbound email composition, and spam detection rates.

- **Directory synchronization** – Simplify user management and prevent directory harvest attacks by synchronizing Active Directory data with Websense Cloud Email Security.
- **Policies and fine-tuning** – Create policies for users to enable them to use email as a productive business tool, while restricting unwanted or undesirable messages or those that pose security risks.
- **Reporting** – Examine trends and statistics for messages passing through Websense Cloud Email Security.
- **Message Center** – Review quarantined messages and choose whether to deliver, forward, or discard them.
- **After Setup** – Administer the service after the initial configuration, and enable end users to manage their email.
- **Integration with Websense Cloud Web Security** – The advantages of an integrated email and Web security solution.

For detailed information on any aspect of Websense Cloud Email Security, refer to the *Websense Cloud Email Security Help*. Click the **Help** menu in the portal to access this guide.

Corporate Web site

www.websense.com

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for more than 43 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and cloud security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies.

Dashboard

The dashboard provides a snapshot view of how Websense Cloud Email Security is performing. To view your dashboard, click **Dashboard** on the portal’s main menu bar.

Note the following significant features:

- The **Email activity overview** displays the number of inbound and outbound email requests processed for your account in the last 7 days.
- **Inbound and outbound composition categories** reveals how Cloud Email Security categorized your inbound and outbound email. Examples of composition categories include Phishing, Commercial Bulk, and Backscatter

  - Phishing - attempts to acquire information, such as usernames, passwords, or credit card information by masquerading as a trusted or well-known entity
  - Commercial Bulk - solicited bulk email, such as newsletters
  - Backscatter - maliciously generated bounce messages (e.g., non-delivery report/receipt (NDR); delivery status notification (DSN); and non-delivery notification (NDN) messages) sent by spammers to spoofed return addresses
- **Top 5 viruses** indicates the top 5 viruses seen in your account along with the number of email carrying each of these viruses.
- **URL categories in email** reveals how Cloud Email Security classified all of the URLs found in your organization's email.

You have the option of viewing this data in either a bar graph or pie chart.

Directory Synchronization

Organizations that use Microsoft Active Directory and other LDAP services can synchronize primary and secondary email addresses and groups into the portal. This has the following advantages:

- Administrators can manage email address and group details from the Active Directory instead of from the cloud service portal, greatly reducing the time spent maintaining service configuration.
- Scheduled synchronization means new employees in a company can be added to the cloud service automatically; likewise, those leaving can be removed from the service automatically.
- Improves spam detection by quarantining email sent to unknown users.
- Helps to prevent directory harvest attacks, by checking the validity of email addresses and domains when a server is trying to send large numbers of messages for the purposes of directory harvesting.

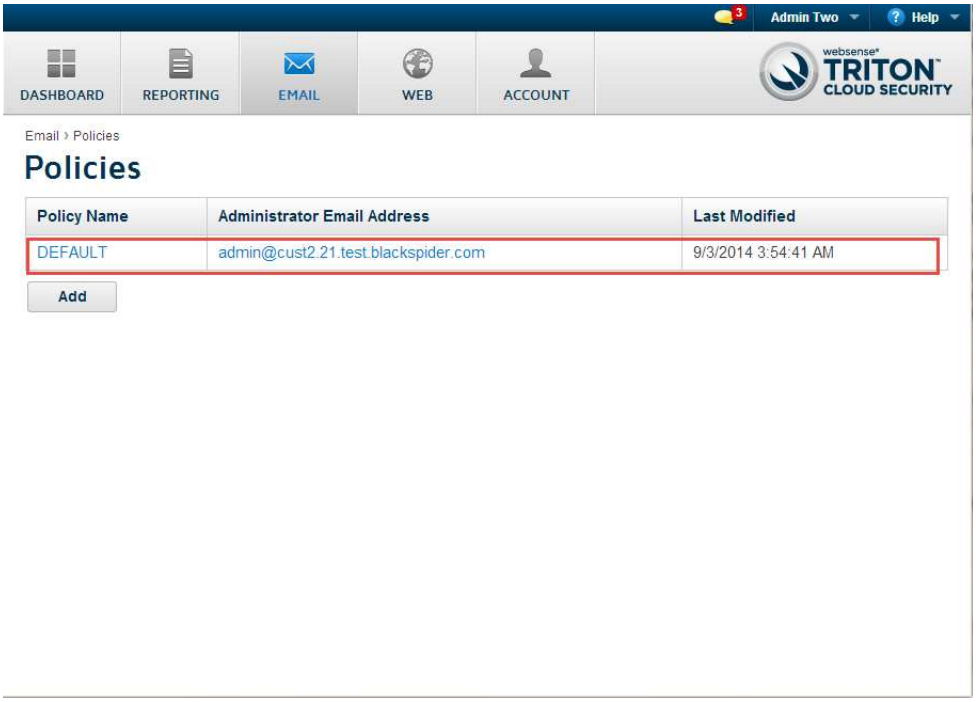
For full instructions on setting up and using directory synchronization, see the *Websense Cloud Email Security Help*, and the *Directory Synchronization Client Administrator's Guide*, both available from the Websense Technical Library.

Policy Setup

The default policy provided with Websense Cloud Email Security allows most organizations to get up and running quickly and easily with minimal configuration. The administrator can modify or create new policies as necessary to manage email traffic to comply with business needs, goals and objectives of the organization.

Policies encompass several elements including rules for spam and virus protection, phrases and lexical rules for content filtering, and notifications of quarantined email. Policy decisions and levels of control may be different for different user groups, but in all cases should be constructed to allow users to effectively use email as a business tool while protecting the company from spam, objectionable or illegal content, and viruses. A default policy is provided with Websense Cloud Email Security, and administrators can also create custom policies to support mail aliases or domains that require differing configurations.

To access the current policies in your account and to create new policies, click **Email** in the portal's main menu bar, then click **Policies**.

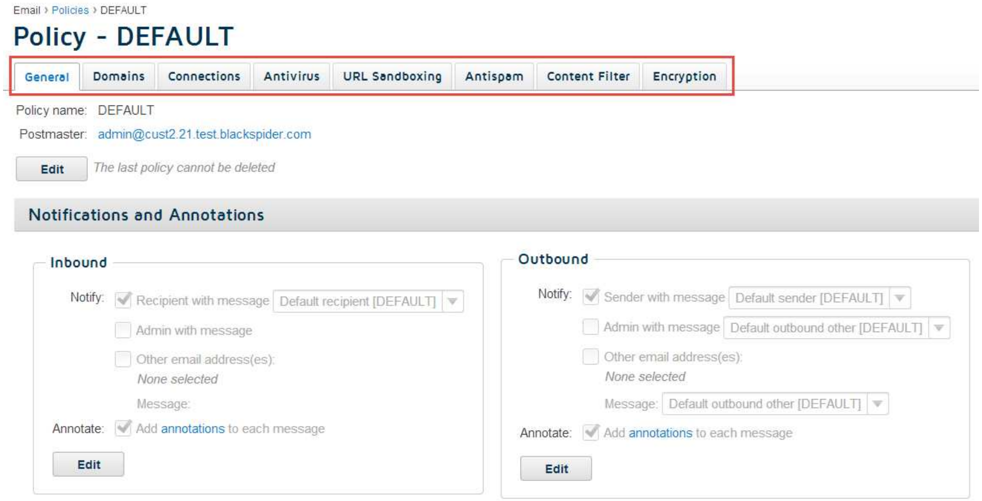


Email › Policies

Policies

Policy Name	Administrator Email Address	Last Modified
DEFAULT	admin@cust2.21.test.blackspider.com	9/3/2014 3:54:41 AM

Click a policy name to view and edit the policy settings. Note that each policy has multiple tabs to configure.



Email › Policies › DEFAULT

Policy - DEFAULT

Policy name: DEFAULT
Postmaster: admin@cust2.21.test.blackspider.com

The last policy cannot be deleted

Notifications and Annotations

Inbound

Notify: ☑ Recipient with message Default recipient [DEFAULT]
☐ Admin with message
☐ Other email address(es):
None selected
Message:
Annotate: ☑ Add annotations to each message

Outbound

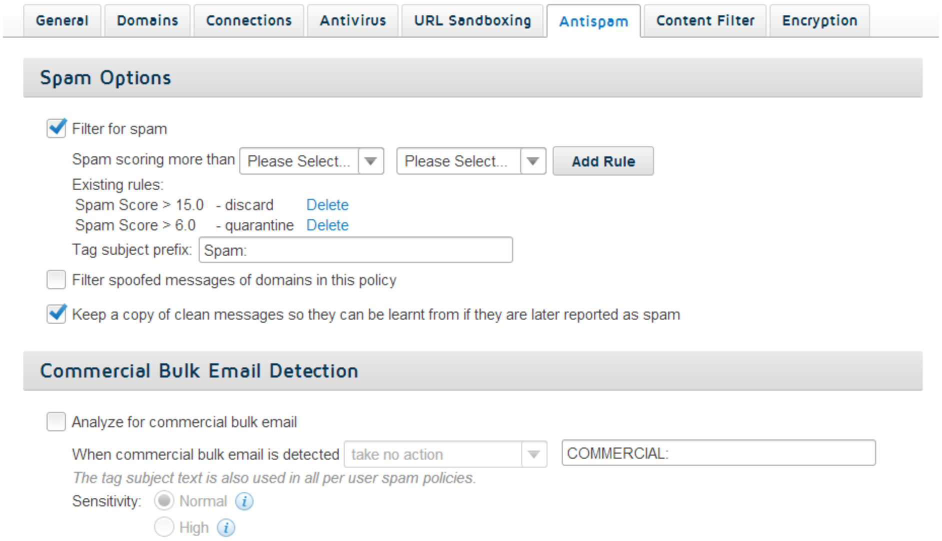
Notify: ☑ Sender with message Default sender [DEFAULT]
☐ Admin with message Default outbound other [DEFAULT]
☐ Other email address(es):
None selected
Message: Default outbound other [DEFAULT]
Annotate: ☑ Add annotations to each message

Setting up antispam rules

It is estimated that 90-95% of all email is spam. Websense Cloud Email Security provides market leading antispam protection through a combination of techniques powered by the ThreatSeeker Network. The Websense approach is unique in that we integrate our Web intelligence into our email security engine, which enables the service to detect blended threat attacks in real-time. Some of the ThreatSeeker technologies include Websense reputation service, integrated Websense URL database, heuristics, fingerprinting, auto-learning technologies, and more.

The email security engine uses a combination of techniques to analyze each email message and assign the message a 'spam score'. This spam score is used to determine the likelihood of the message being spam. The result of the various spam tests may be a positive score (to indicate spam) or a negative score (to indicate valid email). Message scoring above the 'spam threshold' defined by the customer are classified as spam. The results of all tests are taken into account, and this helps to improve accuracy.

To view and edit the current antispam rules for a policy, click the **Antispam** tab.



Spam Options

☑ Filter for spam

Spam scoring more than Please Select... ▼ Please Select... ▼ Add Rule

Existing rules:

Spam Score > 15.0 - discard Delete

Spam Score > 6.0 - quarantine Delete

Tag subject prefix: Spam:

□ Filter spoofed messages of domains in this policy

☑ Keep a copy of clean messages so they can be learnt from if they are later reported as spam

Commercial Bulk Email Detection

□ Analyze for commercial bulk email

When commercial bulk email is detected take no action ▼ COMMERCIAL:

The tag subject text is also used in all per user spam policies.

Sensitivity: ● Normal ⓘ

○ High ⓘ

You can define what happens to spam depending on the score it receives. For example, you might want to create a rule that forces all email with a spam score greater than 6.0 to be forwarded to an administrator, all email with a score greater than 7.0 to be quarantined, and all email with a score over 10.0 to be discarded.

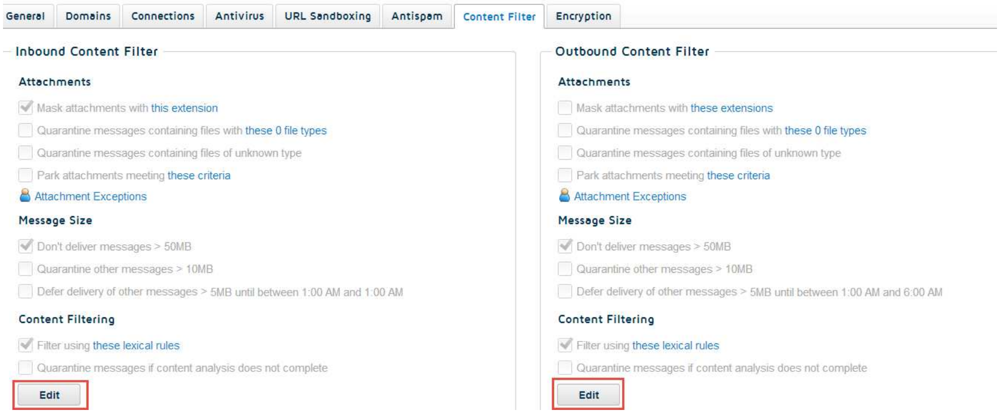
Lower values detect more spam at the risk of false positives - email wrongly detected as spam. Higher values reduce the risk of false positives but could miss some spam. Websense Cloud Email Security aims to ensure that no false positives occur with spam scores over 6.0. This is the recommended default setting for quarantining email.

Content Analysis

Websense Cloud Email Security can perform the following granular content analysis on both inbound and outbound email messages:

- **Executables** – Messages containing scripts and executables can be quarantined. This feature can be set up on a per-user basis within a policy.
- **Attachments** – Attachments can be quarantined by file. This feature can be controlled by including or excluding specific file types. You can also mask attachments: this changes the file to prevent automatic execution.
- **Parking** – Attachments can be parked in the cloud service infrastructure and the original email sent on to the recipient with a URL that locates the attachment for subsequent download if needed. This enables you to minimize the use of Internet bandwidth.
- **Lexical Analysis** – The lexical rules feature scans for words and phrases against both pre-defined and custom dictionaries using Boolean operators and custom weighting and thresholds. This enables you to scan email for profanity and other undesirable content entering your organization. You can also check outbound messages for phrases that might include company confidential information, or could cause embarrassment, loss of reputation, or business.

To view the current content filtering rules for a policy, click the **Content Filter** tab. To edit the displayed rules, click **Edit** under Inbound Content Filter or Outbound Content Filter.



Inbound Content Filter

Attachments

☑ Mask attachments with this extension
□ Quarantine messages containing files with these 0 file types
□ Quarantine messages containing files of unknown type
□ Park attachments meeting these criteria
Attachment Exceptions

Message Size

☑ Don't deliver messages > 50MB
□ Quarantine other messages > 10MB
□ Defer delivery of other messages > 5MB until between 1:00 AM and 1:00 AM

Content Filtering

☑ Filter using these lexical rules
□ Quarantine messages if content analysis does not complete

Outbound Content Filter

Attachments

□ Mask attachments with these extensions
□ Quarantine messages containing files with these 0 file types
□ Quarantine messages containing files of unknown type
□ Park attachments meeting these criteria
Attachment Exceptions

Message Size

☑ Don't deliver messages > 50MB
□ Quarantine other messages > 10MB
□ Defer delivery of other messages > 5MB until between 1:00 AM and 6:00 AM

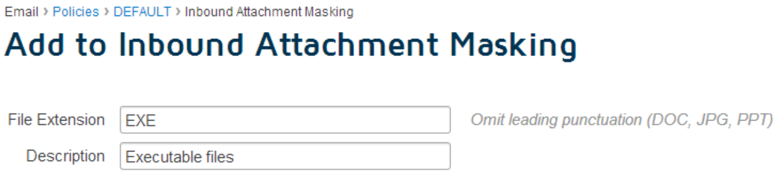
Content Filtering

☑ Filter using these lexical rules
□ Quarantine messages if content analysis does not complete

For example, if an administrator wants to set up an inbound content filter that masks attachments with an EXE file extension:

1. Under Inbound Content Filter, click **Edit**.
2. Check the box labeled **Mask attachments with** these extensions, and then click the link.
3. Click **Add**.
4. In the **File Extension** field, type EXE.

5. In the **Description** field, type a suitable description of the file extension.



Email › Policies › DEFAULT › Inbound Attachment Masking

Add to Inbound Attachment Masking

File Extension: EXE — *Omit leading punctuation (DOC, JPG, PPT)*

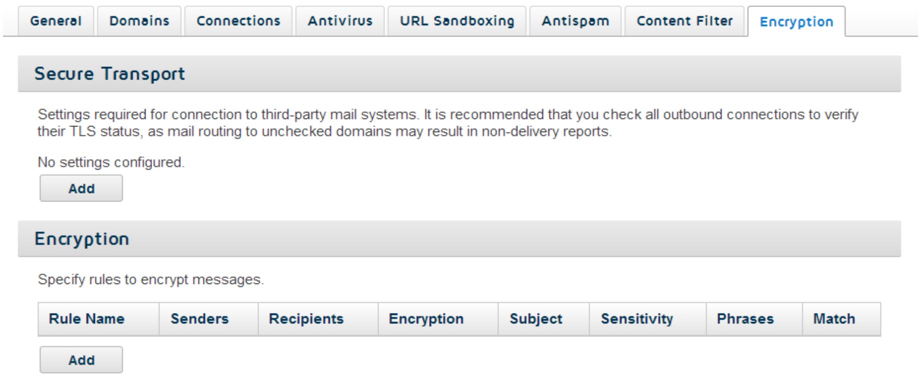
Description: Executable files

6. Click **Submit**.

Encryption

The Websense Cloud Email Security Encryption service secures delivery of email by ensuring that it is not forwarded as plain text “in the clear.” Websense Cloud Email Security Encryption encrypts the transport layer protocols being used to deliver the email at the edge of the network - the point where it leaves the secure environment of the local area network. This enables administrators to configure secure email communications among business partners and individuals, using either a transport layer encrypted “tunnel” between specified email servers or mail transfer agents, ad hoc encryption for mail transfer agents that do not support TLS, or advanced identity-based encryption.

To view the current encryption settings for a policy, click the **Encryption** tab. To edit the displayed settings for a particular encryption type, click the **Add** button.



Secure Transport

Settings required for connection to third-party mail systems. It is recommended that you check all outbound connections to verify their TLS status, as mail routing to unchecked domains may result in non-delivery reports.

No settings configured.

Encryption

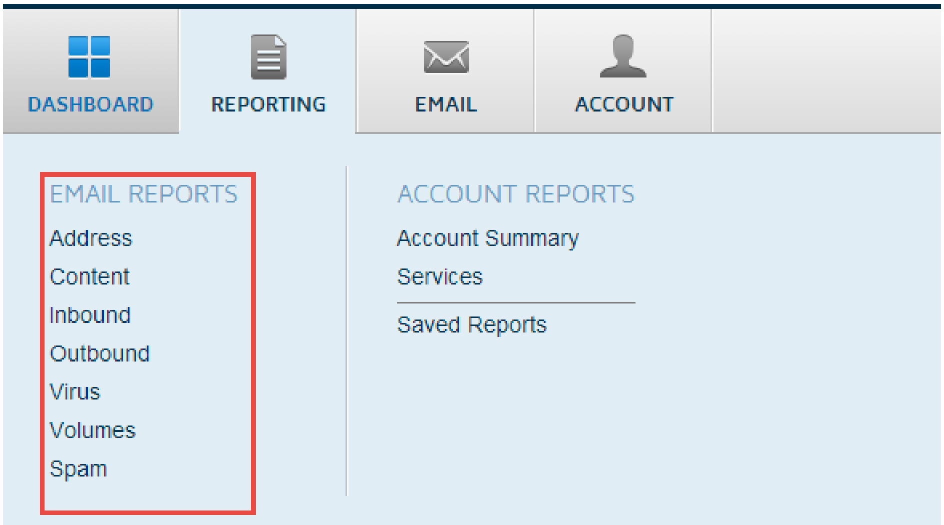
Specify rules to encrypt messages.

Rule Name	Senders	Recipients	Encryption	Subject	Sensitivity	Phrases	Match

Reporting

Websense Cloud Email Security provides exceptional reporting functionality that provides a 360 degree view of email traffic and usage. Administrators can view summary reports and drill down for detailed forensics. Reports can be scheduled to run automatically and be emailed to a designated manager.

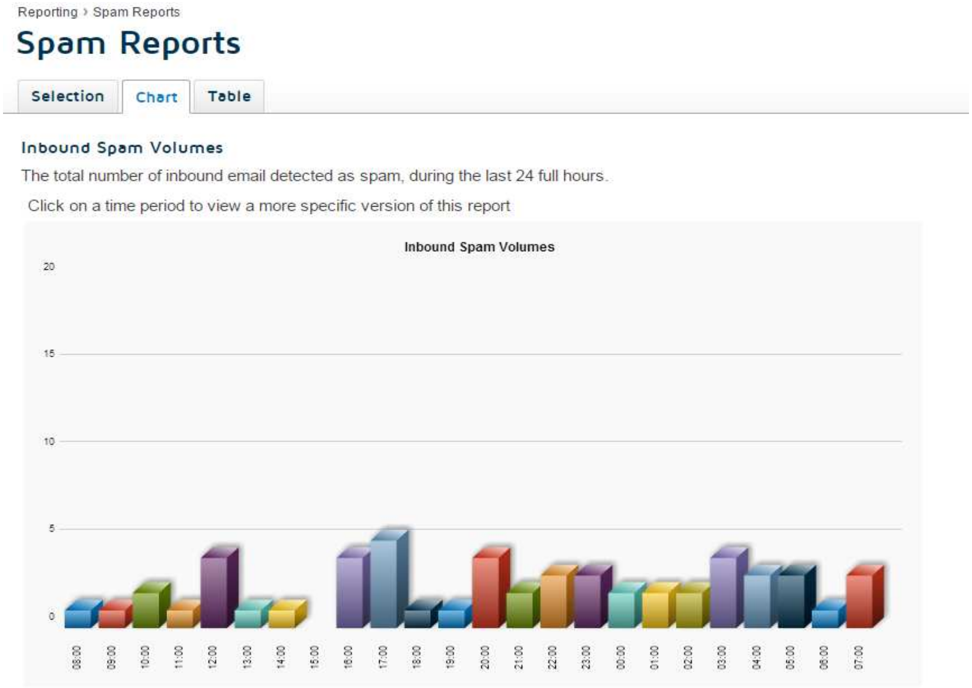
To access the reporting feature, click **Reporting** in the portal's main menu bar. Then select a report type from the **Email Reports** section of the drop-down menu.



Each report option enables you to generate several report types - for example, the Inbound option offers reports of the total volume of inbound messages, the most frequent recipients by volume, the most frequent senders, and the most frequent source IP addresses.

Once you have selected your report type, you can select a time period for the report, and optionally further filters such as inbound policies and domains.

Below is an example of a spam statistics report showing the number of spam emails received each hour for the past 24 hours.



Spam Reports

Inbound Spam Volumes

The total number of inbound email detected as spam, during the last 24 full hours.

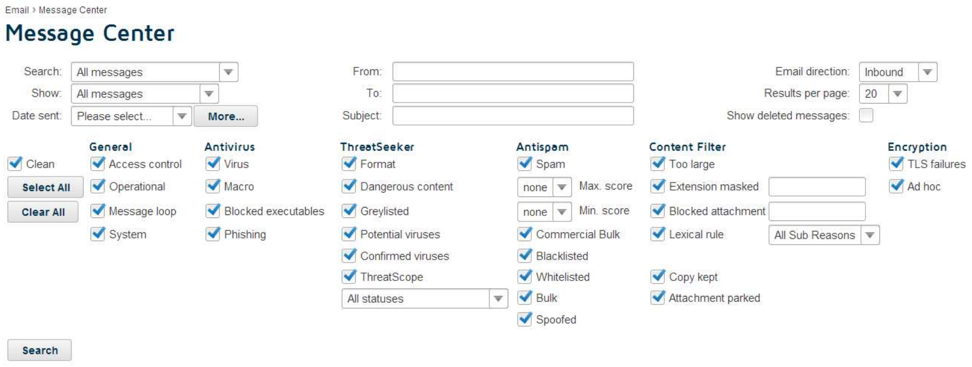
Click on a time period to view a more specific version of this report

You can click on a bar in the chart to drill down further and see the number of spam emails in a particular hour. You can also view the report results as a table, and download the statistics as a CSV file.

Message Center

The Websense Cloud Email Security Message Center is a powerful message tracking and management tool that provides access to all quarantined messages and message logs for your account.

To access the Message Center, click **Email** on the portal's main menu bar, then select **Messages > Message Center**. You are presented with a search form.



Email › Message Center

Message Center

Search: All messages
Show: All messages
Date sent: Please select... More...

From:
To:
Subject:

Email direction: Inbound
Results per page: 20
Show deleted messages: □

☑ Clean

Select All

Clear All

General
☑ Access control
☑ Operational
☑ Message loop
☑ System

Antivirus
☑ Virus
☑ Macro
☑ Blocked executables
☑ Phishing

ThreatSeeker
☑ Format
☑ Dangerous content
☑ Greylisted
☑ Potential viruses
☑ Confirmed viruses
☑ ThreatScope
All statuses

Antispam
☑ Spam
none Max. score
none Min. score
☑ Commercial Bulk
☑ Blacklisted
☑ Whitelisted
☑ Bulk
☑ Spoofed

Content Filter
☑ Too large
☑ Extension masked
☑ Blocked attachment
☑ Lexical rule All Sub Reasons
☑ Copy kept
☑ Attachment parked

Encryption
☑ TLS failures
☑ Ad hoc

Search

Numerous options are available to help you narrow down your results and reduce the search time. This is especially important for large accounts. It is easy to quickly determine whether a message was blocked or delivered by simultaneously searching the quarantine and accepted message logs.

Administrators can perform actions on the messages found by the search, for example releasing, forwarding, or deleting one or more messages.

After Setup

Once the administrator has set up users and customized polices to meet the needs of an organization, there is little ongoing maintenance or configuration required with Websense Cloud Email Security. However, it is good practice to periodically use the dashboard and run reports to review and report on the ongoing email security protection provided by the service.

Administrators can schedule non-graphical versions of account summary reports to be sent to an email address on a daily, weekly, biweekly, or monthly basis.

End User Quarantine Management

The Websense Cloud Email Security service allows end users to manage their own quarantined spam by providing an end-user message report (EUMR). Administrators can also enable end users to populate individual white lists and black lists. This functionality is very easy to roll out to employees with little to no administrative overhead. It is documented in the *Websense Cloud Email Security Getting Started Guide* and the *Websense Cloud Email Security End User Guide*, both available from the Websense Technical Library.

Integration with Websense Cloud Web Security

The close integration of Websense Cloud Email Security and Websense Cloud Web Security enables organizations to optimize their email use and to safely leverage the power of Web 2.0 technology. Customers gain complete web and email security with the benefits of integrated management, reporting, and the value of a consolidated security strategy with the following benefits:

- Blocks web and email threats at their source, improving network efficiency and saving business costs.
- Approximately 85% of email contains a link to a website. The real-time ThreatSeeker Network in Websense Cloud Web Security protects end users from the risks of accessing inappropriate and malicious content, including spyware, phishing, botnets, and other threats, via both Internet browsing and email.
- Email and web protection can be configured through a single portal, requiring the administrator to manage only one set of users and groups and monitor usage through a single dashboard.

Summary

This guide has highlighted the most important aspects of administering Websense Cloud Email Security, and demonstrated the following benefits:

- Threats are blocked before they reach your network, as shown by the statistics on the dashboard. This means reduced bandwidth, storage, and maintenance costs for your organization.
- Default policies enable immediate and effective email security with little administrative time required. Policies can be customized to meet the precise needs of your users while ensuring complete and effective email security.
- The Message Center and reporting functions enable you to track every aspect of email usage, security, and management.
- Integration with Websense Cloud Web Security provides a complete security solution with centralized policies and reporting.

Thank you for evaluating Websense Cloud Email Security.