



CYREN

Outbound Anti-Spam Daemon (ctasd) Implementation Manual

Version 5.00

© 2015 CYREN Inc.

All rights reserved

ctasd Outbound Module and Documentation Usage Restrictions

This program and the accompanied documentation is SECRET AND CONFIDENTIAL, and constitute a proprietary trade secret of CYREN Software Ltd. and/or CYREN Inc. (herein after referred to as "CYREN").

No person is allowed to copy, decompile, reverse engineer, use, sublicense or otherwise access this program unless the prior express, written consent is received from CYREN. The possession and use of this program shall be governed by the terms of a license agreement between CYREN and each authorized licensee. Unauthorized use of this program is strictly prohibited, and those perpetrating such unauthorized uses shall be prosecuted to the fullest extent of the law. The confidentiality and non-disclosure obligations of licensee shall be strictly maintained at all times by licensee and licensee, in receiving a copy of this program, acknowledges that it shall not be disclosed to third parties; rather, only to employees or consultants having a firm need to know, and provided that they are bound by confidentiality restrictions at least as restrictive as those adopted by licensee within the framework of its relationship with CYREN.

The failure to maintain confidentiality will likely cause severe damages and irreparable harm to CYREN and, therefore, in addition to any other remedies and rights available at law, CYREN shall be entitled to seek injunctive relief without the need for the posting of any bond or other guarantee.

Trademark and Copyright Statement

CTT00-402-101-111-R1

© CYREN Software Ltd. 1991 - 2015 All rights reserved.

The information contained in this document is subject to change without notice. CYREN makes no warranty of any kind. CYREN will not be liable for any direct, indirect, incidental, consequential or other damage alleged in connection with the furnishing or use of this information. Except as allowed by copyright laws or herein, reproduction, adaptation or translation without prior written permission is prohibited.

RPD™, ctasd™, and ctengine™ are trademarks of CYREN Software Ltd. All other trade/service marks or names that may be referenced and/or mentioned in this document belong to their respective owners. Microsoft is a trademark and/or registered trademark of Microsoft Corp. Linux is a trademark of Linus Torvalds. Red Hat is a trademark of Red Hat, Inc. in the United States and other countries. Debian is a registered trademark of Software in the Public Interest, Inc.

COPYRIGHT AND PERMISSION NOTICE Copyright (c) 1996 - 2015, Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Contacts

Any technical questions you or your developers have about using the ctasd should be addressed to support@cyren.com.



About CYREN

CYREN™ provides proven Internet security technology to more than 150 security companies and service providers including 1&1, Check Point, F-Secure, Google, Microsoft, Panda Security, Rackspace, US Internet, and WatchGuard, for integration into their solutions. CYREN's GlobalView™ and patented Recurrent Pattern Detection™ (RPD™) technologies are founded on a unique cloud-based approach, and protect effectively in all languages and formats. CYREN Antivirus utilizes a multi-layered approach to provide award winning malware detection and industry-leading performance.

CYREN technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, enabling our partners to protect end-users from spam and malware, and ensure safe, compliant browsing. The company's expertise in building efficient, mass-scale security services mitigate Internet threats for thousands of organizations and hundreds of millions of users in 190 countries.

CYREN, formerly known as Commtouch, was founded in 1991, is headquartered in the US in McLean, Virginia, with offices in Palo Alto, California, Herzliya, Israel, Berlin, Germany, and Reykjavik, Iceland.

For more information about enhancing security offerings with CYREN technology, visit our website at www.cyren.com, see our blog at <http://blog.cyren.com> or write to info@cyren.com.

Table of Contents

1	INTRODUCTION	1
1.1	Different Sources of Outbound Spam.....	1
2	OUTBOUND IMPLEMENTATION POLICIES	3
2.1	Message Classification Policies.....	3
2.2	Sender-Based Policies.....	3
2.3	Message Classification and Sender-Based Policies.....	4
2.4	Spam Classifications	4
2.4.1	Optional Actions for Spam Classifications	4
2.5	Virus Outbreak Detection (VOD) Classifications.....	5
2.5.1	Optional Actions for VOD Classifications.....	7
2.6	Guidelines for Sender Threshold Crossing Events	7
2.6.1	Walled Garden.....	8
2.6.2	Account Lock-Out	8
2.6.3	Quarantining Messages.....	8
2.6.4	Optional Actions for Crossed Thresholds	9
3	GENERAL GUIDELINES.....	12
3.1	License Key	12
3.2	RefID	12
3.3	Spamd.....	13
3.4	Reporting Classification Mistakes to CYREN.....	13

1 Introduction

CYREN Advanced Security Daemon (a.k.a. ctasd™) is a plug-n-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. ctasd is intended for Service Providers and OEMs who partner with CYREN to protect their messaging infrastructure from being abused by spammers trying to send spam and malware such as viruses, phishing messages, etc.

Service Providers and OEM partners often unwittingly transport spam messages and therefore run the risk of being blacklisted on a daily basis, a situation which immediately affects subscriber satisfaction. The ramifications of even one infected server or PC being used in spam attacks can potentially stop every subscriber from sending email as they share the same public IP address range.

ctasd's Outbound Spam Protection Service not only detects spam but also identifies the spammer, giving Service Providers and OEMs the power and tools to find and stop spammers from using their networks as a means of spamming others. ctasd can be integrated to deliver the following services:

- Outbound Spam Protection
- Outbound Virus Outbreak Detection (VOD)

Each service can be licensed and provisioned separately without affecting other CYREN services. Both services share a single license key code, and are provisioned accordingly on the CYREN Datacenter. Once provisioned, the Service Provider may choose to disable one or more services locally for testing purposes.

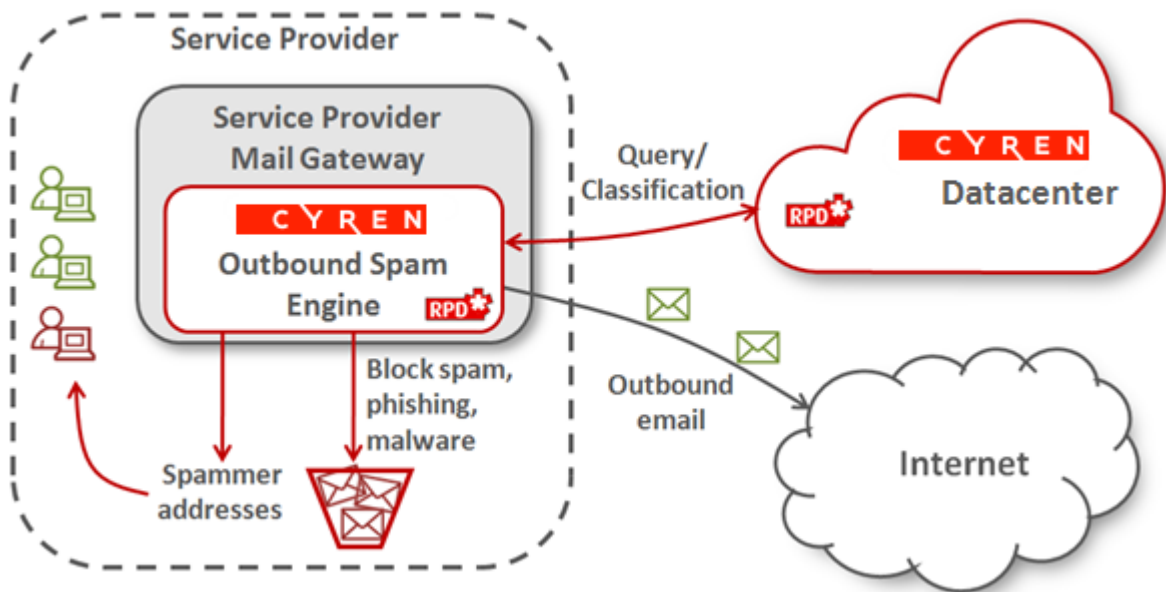
The purpose of this document is to outline implementation guidelines for Service Providers and OEM partners. It offers recommendations based on CYREN's experiences, for integrating ctasd with another messaging or security application to provide outbound spam and virus protection services.

1.1 Different Sources of Outbound Spam

Outbound spam emails coming from Service Provider networks typically originate from multiple sources. These include compromised user accounts and spammer accounts abusing the Service Provider's MTA resources; or alternatively, zombie computers and customer MTAs who send spam directly to the Internet using port 25 (or 465).

The Outbound Spam Protection service can be implemented to address direct MTA abuses and/or port 25 abuses.

- If the MTA resources of a Service Provider are being abused, the outbound ctasd filter solution can be placed inline with the outgoing MTAs of the Service Provider or OEM partner.
- If port 25 is being abused, a customer can filter out rfc 822 packets, and reconstruct messages for ctasd to perform outbound spam filtering.



2 Outbound Implementation Policies

A Service Provider can decide whether to implement and enforce outbound policies on one of the following:

- The outbound message classification
- The sender of the message
- A combination of both outbound message classification and the sender

2.1 Message Classification Policies

Message classification policies perform actions on a specific message. Policies may include blocking spam messages with a bounce back notification; or placement of outbound spam messages in a quarantined area with or without notification to the sender.

2.2 Sender-Based Policies

Enforcing a message classification-based policy may result in costly false positives by incorrectly blocking a message from its own subscribers. This, in turn, may cause subscriber dissatisfaction and complaints that the Service Provider is not providing the contracted services.

Therefore, it may be more effective to implement sender-based policies rather than classification-based policies. The Outbound Spam Protection Service enables Service Providers and OEMs to quickly and accurately identify spammers. This includes spammers of different types, including: zombie computers, compromised accounts, spamming accounts and spamming MTAs.

Each Service Provider can configure the appropriate header to define the SenderID in the configuration file using the SenderIDHeaderName parameter. This implementation decision is important as it will define how senders are tracked and managed in the system. SenderID definitions may include the message Sender IP; FROM header; SMTP Auth account etc. More advanced SenderID logics, for example setting the SenderID to be the SMTP Auth account, and if not found, than setting the SenderID to be the message Sender IP, is also supported. If the SenderID is not sent explicitly in each message, then this parameter value must be defined. Default value: From header.

Sender-based policies may include sender account lock-out for a predefined period of time; or placement of the sender account behind a walled-garden, meaning all emails of known spammers are sent out using a different set of IP addresses.

A Service Provider may decide whether to define a policy based on any of the following SenderID counters:

- Number of spam messages sent out during the defined time window.
- Number of virus messages sent out during the defined time window (applicable for VOD customers only).
- Number of suspected messages sent out during the defined time window.
- Number of total messages sent out during the defined time window.
- Number of recipients listed in messages sent out during the defined time window.
- Each Service Provider can review the list of senders and decide which ones should be added to one of the following:
 - *Whitelist* – allows the sender to send any mail, including spam messages without maintaining any counters on these outgoing messages. A Service Provider may decide to Whitelist VIP customers.
 - *Bluelist* – allows the sender to send out all non-spam messages.

2.3 Message Classification and Sender-Based Policies

Some Service Providers or OEM partners may select to implement a policy based on combining both the message classification and sender information. Such policies may include spam message rate limiting which is implemented per spammer. This allows each sender only a limited number of spam messages to be sent out per configured time window.

Once this limit is reached, the policy may determine that all additional spam messages sent by the same sender should be blocked within the configured time window. The spam counter is reset once the time window has expired.

2.4 Spam Classifications

Messages are divided into *good*, *bad*, and *suspected* as described in the following table.

- *Bad* emails are messages that contain spam patterns.
- *Good* messages are those that contain no recognized spam patterns.
- *Suspected* messages are those that do not have recognized spam patterns, but have been sent out on a local level at such volumes that require additional review.

2.4.1 Optional Actions for Spam Classifications

Note: ctasd was designed to classify email messages and to report back to the querying device with its findings. It does not implement actions against messages or the senders of messages. Rather, it offers the Service Provider or OEM partner with the necessary information to create policies and implement actions. In the following table, some optional actions are explained for each classification. The Service Provider/OEM

partner is responsible for selecting and implementing external policy management for these or other options, as it chooses.

Classification	Explanation	Optional Action(s)
Confirmed-Spam	Spam messages from known spam sources (e.g. zombies).	<ul style="list-style-type: none"> Block message and generate a bounce-back message to the sender. Direct to site-level outbound quarantine for the administrator to manage.
Bulk	Spam messages from sources that are not confirmed spammers.	<ul style="list-style-type: none"> Block message and generate a bounce-back message to the sender. Direct to site-level outbound quarantine for an administrator to manage. Direct to user-level outbound quarantine for the end-user to review. Send warning message to user that he sent out a Bulk classified message.
Suspect	Messages that are sent locally in slightly larger than average distribution or are unidentified spam messages in the first few seconds of a massive spam outbreak.	<ul style="list-style-type: none"> Allow message to be sent out Send samples to Abuse Team for further review.
Unknown	Messages for which ctasd does not have any incriminating information, and are therefore assumed to represent legitimate correspondence.	<ul style="list-style-type: none"> Allow message to be sent out
Non-Spam	Messages that are confirmed, without doubt, as coming from a trusted source. This classification is very rarely used.	<ul style="list-style-type: none"> Allow message to be sent out

2.5 Virus Outbreak Detection (VOD) Classifications

Because CYREN's Virus Outbreak Detection Services are designed to detect new virus outbreaks, it is highly recommended that you deploy ctasd after the message has already been scanned by your current anti-virus application.

When ctasd finds enough evidence to suggest the likelihood that a virus is present, it is often recommended that you hold the message until the next relevant anti-virus update instead of immediately deleting it (to avoid cases of false positives) or forward it to the targeted recipients (to avoid cases of false negatives).

Holding the message until the next immediate anti-virus update might not always be the best tactic to use, if the anti-virus vendor has not had an opportunity to release the appropriate signature. Therefore, it is recommended that you determine the average response time for detecting new virus outbreaks for whatever anti-virus software you use. You can then calculate how long to hold the message before again passing it to the anti-virus software.

2.5.1 Optional Actions for VOD Classifications

Note: *ctasd was designed to classify email messages and to report back to the querying device with its findings. It does not implement actions against messages or the senders of messages. Rather, it offers the Service Provider or OEM partner with the necessary information to create policies and implement actions. In the following table, some optional actions are explained for each classification. The Service Provider/OEM partner is responsible for selecting and implementing external policy management for these or other options, as it chooses.*

Virus Threat Level (VTL) Classification	Explanation	Optional Action(s)
Virus	The message contains characteristics of confirmed malware.	<ul style="list-style-type: none"> Delete the message. Place the message in the anti-virus quarantine for manual review by the administrator.
High	High likelihood of the message presenting a malware threat.	<ul style="list-style-type: none"> Delete the message. Direct the message to your anti-virus quarantine (if applicable) for manual release by the administrator. Hold the message in a special queue for the next relevant anti-virus update.
Medium	Probable threat of virus in the message has been detected.	<ul style="list-style-type: none"> Hold the message in a special queue for the next 2-3 relevant anti-virus updates. Forward to intended recipients.
Unknown	Threat for virus could not be determined at this time.	<ul style="list-style-type: none"> Treat this as an email without a virus.
Non-Virus	Confirmed that message does not contain a virus.	<ul style="list-style-type: none"> Treat this as an email without a virus.

2.6 Guidelines for Sender Threshold Crossing Events

The Outbound Spam Protection service not only tracks messages but also sender behavior. It enables the Service Provider to track the following information per sender:

- Number of Suspected messages sent
- Number of Spam messages sent
- Total number of total messages sent

- Number of Recipients messages sent
- Number of messages with viruses sent

Based on the selected policies adopted by the service provider, each Service Provider or OEM partner should decide which of the above sender counters to enable. In addition, the Outbound Spam Protection Service enables the service provider to set up to 3 different event thresholds per each counter. Once a sender crosses a defined threshold, the Outbound Spam Protection Service will notify the service provider that such an event occurred.

When a threshold is crossed it typically means that some restriction may be applied to protect the Service Provider/OEM network from being abused, or to protect intended recipients from receiving spam or malware. Possible actions that may be applied by policies created by the Service Provider might include:

2.6.1 Walled Garden

Walled gardens offer a way to limit senders without completely blocking their ability to send messages. Rather than blocking the users completely, their access can be restricted to a defined set of IPs defined within a walled garden. The activity of these IPs is not monitored, and therefore carries the high risk of being black-listed. The importance of a walled garden is that spammers can be placed within the walled garden without the spamming activity negatively affecting the service provider's IPs servicing legitimate subscribers.

2.6.2 Account Lock-Out

You may decide to specify an Account Lock-Out, which will prevent the sending account from sending any messages for a defined period of time. This may be recommended when the account is being used to send out spam messages or viruses.

2.6.3 Quarantining Messages

Outbound Site-Level Quarantine

To allow global management and diagnostics of blocked messages by system administrators, it is recommended that you develop site-level quarantine with the ability to release, delete or forward blocked outbound spam messages. You can also white-list senders, which allows a sender to send any message (including spam messages), without being factored into the counters.

Outbound User-Level Quarantine

In order to allow user-level involvement, it is recommended that you create user-level outbound mail quarantine. You can then create a method whereby users can access this quarantine to review and release blocked outbound spam messages.

2.6.4 Optional Actions for Crossed Thresholds

The following table describes the sender counters that can be enabled per outbound mail sender, as well as some optional actions that can be performed once a counter crossing event occurs.

Note: ctasd was designed to classify email messages and to report back to the querying device with its findings. It does not implement actions against messages or the senders of messages. Rather, it offers the Service Provider or OEM partner with the necessary information to create policies and implement actions.

In the following table, some optional actions are explained for each classification. The Service Provider/OEM partner is responsible for selecting and implementing external policy management for these or other options, as it chooses.

Event Type	Description	Optional actions
Suspected Counter Threshold crossed	The number of suspected messages sent out by the sender in a pre-defined time window.	<ul style="list-style-type: none"> • Send message sample to Abuse Team for further investigation. • Decide whether to blue-list the sender.
Spam Counter Threshold crossed	The number of confirmed spam and bulk messages sent out by the sender in a pre-defined time window.	<ul style="list-style-type: none"> • Place sender within walled garden. • Notify spammer of detected spamming activity. • Lock-out the account for a predefined time period (account will not be able to send any messages for the defined time period), with sender notification. • Decide whether to white-list the sender.
Bulk Counter Threshold crossed	<p>The number of bulk messages sent out by the sender in a pre-defined time window.</p> <hr/> <p><i>Note: The Bulk and Confirmed counters should be used instead of the Spam Counter when a Service Provider implements different policies for confirmed and bulk classified</i></p>	<ul style="list-style-type: none"> • Place sender within a walled garden. • Notify spammer of detected spamming activity. • Lock-out the account for a predefined time period (account will not be able to send any messages for the defined time period), with sender notification. • Decide whether to white-list the sender.

Event Type	Description	Optional actions
	<i>messages.</i>	
Confirmed Counter Threshold crossed	<p>The number of confirmed messages sent out by the sender in a pre-defined time window.</p> <hr/> <p><i>Note: The Bulk and Confirmed counters should be used instead of the Spam Counter if a service provider implements different policies for confirmed and bulk classified messages.</i></p> <hr/>	<ul style="list-style-type: none"> Place sender within a walled garden. Notify spammer of detected spamming activity. Lock-out the account for a predefined time period (account will not be able to send any messages for the defined time period), with sender notification. Decide whether to white-list the sender.
Total Counter Threshold crossed	<p>The total number of messages sent out by the sender in a pre-defined time window.</p>	<ul style="list-style-type: none"> Rate-limit the sender. Do not allow the sender to send additional messages in pre-defined time window. Send bounce back messages for all blocked messages. <hr/> <p><i>Note: This action may be implemented by tracking the ClassifyMessage X-CTCH-SenderID-Flags response header value. Block only the messages with a flag value indicating that the threshold has been crossed.</i></p> <hr/>
Recipients Counter Threshold crossed	<p>The total number of recipients listed in the messages sent out by sender in a pre-defined time window.</p>	<ul style="list-style-type: none"> Rate-limit the sender. Do not allow the sender to send additional messages in pre-defined time window. Send bounce back messages for all messages that are held back from delivery because they exceed the threshold. <hr/> <p><i>Note: This action may be implemented by tracking the</i></p>

Event Type	Description	Optional actions
		<i>ClassifyMessage X-CTCH-SenderID-Flags response header value. Hold only the messages with a flag value indicating that the threshold has been crossed.</i>
Virus Counter Threshold crossed	The total number of Virus and High VOD classified messages sent out by the sender in a pre-defined time window.	<ul style="list-style-type: none">• Place sender behind a walled garden.• Notify sender that a virus was detected in one of the messages coming from the account; indicate this may mean the computer's security may be compromised.• Direct user to guidelines on how to clean a computer from a virus (if available).• Lock-out the account until sender has confirmed performing server clean up.

3 General Guidelines

In the following sections, general guidelines for both spam and virus outbreak detections services are detailed.

3.1 License Key

The CYREN Datacenter is responsible for maintaining a vast repository of threat-related classifications and categorizations related to email and web security. ctasd communicates with the Datacenter to receive information such as spam and virus classifications. Communication is authenticated based on a license key, a mandatory value that is supplied as a parameter in the Connection String, and consists of the following:

- **CYREN token:** 20-character unique identifier provided by CYREN to identify the OEM partner
- **Service Provider token:** A unique identifier (up to 35 alphanumeric characters) provided by the Service Provider partner

The Service Provider's identifier should distinguish between each user, device, or installation. A single ctasd daemon can provide single or multiple Inbound Mail Flow Services without affecting performance and accuracy. However, another ctasd daemon is required to provide single or multiple Outbound Mail Flow services (and vice versa). Once provisioned, the CYREN partner may choose to disable one or more services locally for testing purposes and then enable the service or services for actual production use. If using an OEM token, it should be unique for the lifetime of the host application and should not be changed so that the same Service Provider token is used each time the application is initiated. It can be based on hardware or software-specific data. CYREN needs this full license key format to offer the highest level of customer support and service.

The format for this concatenated parameter uses a colon delimiter, as follows:

`LicenseKey=<CYREN token>:<unique Service Provider token>`

Example: `LicenseKey=0001K032B1010W167E2B:12345-1234A-55555`

3.2 RefID

The RefID is a parameter that is returned by ctasd with every message classification. It contains a transaction tracing code that can help CYREN technical support track the reason for the classification. It is recommended that you create a mechanism to copy this value and add it to a

special x-header of the message in order to provide better service to your customers, should they require CYREN to trace why a message was classified a certain way.

Note: Without this key, CYREN is unable to retroactively determine the reason why a message classification was returned and then reported as a detection mistake. Classifications are constantly updated to reflect the current status of an outbreak and only the most recent classification is retained in the Classification Warehouse.

3.3 Spamd

In addition to its standard protocol, ctasd also supports a SpamAssassin-compatible protocol, referred to as Spamd. The Spamd protocol should be used when a Mail Server has built-in integration to SpamAssassin. In these cases, it may be easier to integrate with ctasd using the spamd protocol, which is compatible for use with the Exim Mail Server. Refer to the Inbound ctasd Integration Manual for details on the spamd protocol.

3.4 Reporting Classification Mistakes to CYREN

Although ctasd delivers a very high detection rate, users may occasionally feel that a message should have been classified differently. It is recommended that you implement a mechanism that enables your users to report these “misclassifications”. By reporting any cases of false negatives and, more importantly, any cases of false positives to CYREN, you can improve the overall performance even further.

For more information about reporting classification mistakes, review the *ctasd Integration Manual* and the *Reporting Classification Mistakes to CYREN* documents that are packaged with ctasd.