



# Email Reputation Services

## Administrator's Guide

Dynamic Spam Protection at the Network Layer



Messaging Security

## **Privacy and Personal Data Collection Disclosure**

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

Email Reputation Services collects and transmits all data you provide on the console to Trend Micro servers. In order to discontinue the collection of data, you must unregister from the service.

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before using this service, please review the latest version of the applicable user documentation, which is available from the Help drop-down list at the top of the screen (**Help > Download Manual**).

Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2020. Trend Micro Incorporated. All rights reserved.

Document Part No.: EREM05936/130415

Release Date: May 2013

Document Version No.: 3.00

Protected by U.S. Patent No.: 7,606,214; 7,926,108; 7,814,540

The Trend Micro™ Email Reputation Services Administrator's Guide is intended to introduce the main features of the service. You should read through it prior to using the service.

Detailed information about how to use specific features within the software may be available in the Online Help file and the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at [docs@trendmicro.com](mailto:docs@trendmicro.com).

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

# Table of Contents

## **Preface**

Preface .....	v
Documentation .....	vi
Audience .....	vi
Document Conventions .....	vi

## **Chapter 1: Introducing Email Reputation Services**

Trend Micro Email Reputation Services .....	1-2
Standard Service .....	1-2
Advanced Service .....	1-3
Trend Micro Smart Protection Network .....	1-3
Trend Micro Threat Analysis Team .....	1-4
How It Works .....	1-5
Blocking Connections As Opposed to Messages .....	1-7

## **Chapter 2: Blocked?**

Step 1: Determine Your IP Address .....	2-4
Step 2: Check the Status of Your IP Address .....	2-4
Step 3: Send a Removal Request .....	2-5
Step 4: Investigation .....	2-6

## **Chapter 3: Getting Started**

Configuring Email Reputation Services .....	3-2
Creating an Account .....	3-2
Request Trial Account .....	3-4
Configuring Your MTA .....	3-5
Logging Onto the Console .....	3-5
Forgot Password .....	3-6

## Chapter 4: Using the Administrative Console

Email Reputation Services Console .....	4-2
Global Spam Threats .....	4-2
Your Network .....	4-3
IP Reputation .....	4-4
Look Up IP Addresses .....	4-4
Global Approved List .....	4-5
Managing the Policy .....	4-7
Approved Lists .....	4-8
Blocked Lists .....	4-9
Reputation Settings .....	4-11
Administration .....	4-14
Changing Account Details .....	4-14
Changing the Activation Code .....	4-15

## Chapter 5: Getting Help

Frequently Asked Questions (FAQs) .....	5-2
Why Were You Referred To This Website? .....	5-2
Why is My IP Listed in the Known Spam Source List? .....	5-2
Why is My IP Listed in DUL? .....	5-2
Why is My IP Listed in ETL? .....	5-3
Why is My IP Listed in QIL? .....	5-3
Why Did I Receive A Bounced Email But The IP Address Is Not On Any Blocked List? .....	5-3
Getting Help with the Administrative Console .....	5-3
Contacting Trend Micro .....	5-4
Speeding Up the Support Call .....	5-4
Using the Support Portal .....	5-5
Sending Suspicious Content to Trend Micro .....	5-5
Documentation Feedback .....	5-6

## Appendix A: Glossary

Dynamic Reputation Database (QIL) .....	A-2
---	-----

Dial-up User List (DUL) .....	A-2
Emerging Threat List (ETL) .....	A-2
False Positive .....	A-2
Global Approved List .....	A-2
HTTP .....	A-3
HTTPS .....	A-3
IP .....	A-3
Known Spam Source List .....	A-3
Marketing Message List .....	A-3
Phish Attack .....	A-4
Ping .....	A-4
SOCKS 4 .....	A-4
TCP .....	A-5

## **Index**

Index .....	IN-1
-------------	------



# Preface

## Preface

Welcome to the Trend Micro™ Email Reputation Services Administrator's Guide. The guide introduces the main features of the service and configuration instructions for your production environment. Please read through this guide before configuring the service.

- *Documentation on page vi*
- *Audience on page vi*
- *Document Conventions on page vi*

## Documentation

The Trend Micro Email Reputation Services documentation consists of the following:

- **Online Help:** Helps you configure all features through the user interface. You can access the online help by opening the web console and then clicking the help icon.
- **Administrator's Guide:** Helps you to plan for deployment and to configure all service settings.

## Audience

The Email Reputation Services documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP protocol
- Message transfer agents (MTAs)



### Note

You have to know how to configure your MTA to make a DNS Known Spam Source List query before you change the settings for Email Reputation Services.

---

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

## Document Conventions

The documentation uses the following conventions.

**TABLE 1. Document Conventions**

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
<b>Navigation &gt; Path</b>	The navigation path to reach a particular screen  For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface
 <b>Note</b>	Configuration notes
 <b>Tip</b>	Recommendations or suggestions
 <b>Important</b>	Information regarding required or default configuration settings and product limitations
 <b>WARNING!</b>	Critical actions and configuration options



# Chapter 1

## Introducing Email Reputation Services

Trend Micro Email Reputation Services delivers high-performance, cost-effective hosted security services, helping protect businesses against spam, viruses, and inappropriate content before they reach your network.

- *Trend Micro Email Reputation Services on page 1-2*
- *How It Works on page 1-5*

## Trend Micro Email Reputation Services

As the first line of defense, Trend Micro Email Reputation Services helps stop more than 80% of spam before it can flood your network, overload email gateway security, and burden your system resources.

When your email server accepts an initial connection from another email server, your email server records the IP address of the computer requesting the connection. Your email server then queries its DNS server, which in turn queries the Trend Micro reputation database(s) to determine if there is a record for the IP address of the requesting computer.

If the host is listed in a database, Email Reputation Services recommends an appropriate action. You can also customize actions.

Trend Micro offers two levels of Email Reputation Services service: Standard and Advanced.

### Standard Service

This service helps block spam by validating requested IP addresses against the Trend Micro reputation database, powered by the Trend Micro Smart Protection Network.

This ever-expanding database currently contains over 1 billion IP addresses with reputation ratings based on spamming activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

Email Reputation Services Standard Service is a DNS single-query-based service. Your designated email server makes a DNS query to the standard reputation database server whenever it receives an email message from an unknown host. If the host is listed in the standard reputation database, Email Reputation Services reports that email message as spam. You can set up your Message Transfer Agent (MTA) to take the appropriate action on that message based on the Email Reputation Services results.

**Note**

Trend Micro recommends that you configure your MTA to block an email message from an IP address that is on the standard reputation database.

---

## Advanced Service

This service identifies and stops sources of spam while they are in the process of sending millions of messages.

This is a dynamic, real-time anti-spam solution. To provide this service, the Trend Micro network of automated expert systems along with Trend Micro spam experts continuously monitor network and traffic patterns and immediately update the dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity increases or decreases, the dynamic reputation database is updated accordingly.

Like Standard, Advanced Service makes a DNS query to the standard reputation database and the dynamic reputation database (a database updated dynamically in real time). These databases have distinct entries, allowing Trend Micro to maintain an efficient and effective database that can quickly respond to highly dynamic sources of spam.

Email Reputation Services Advanced Service has blocked more than 80% of total incoming connections in customer networks. Results will vary depending on how much of your incoming email stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

## Trend Micro Smart Protection Network

Email Reputation Services is powered by the Trend Micro Smart Protection Network, a global network operated by highly trained spam investigators who research, collect, process, and distribute reputation ratings on IP addresses. These specialists monitor spam activity, develop information on spam sources, verify the accuracy of reputation ratings, and work with organizations to ensure that the service is tracking spammers correctly.

Working around the clock to assure availability and quick response times, the Smart Protection Network delivers real-time updates to the database for immediate availability. This high level of service is the key component for building and maintaining a reliable reputation database.

## Trend Micro Threat Analysis Team

As part of the Smart Protection Network, the Trend Micro Threat Analysis Team maintains the reputation databases to ensure that ratings are accurate and up-to-date. Every rating includes comprehensive spamming histories and spam samples for complete transparency into the databases. This service is unique because it is fully auditable by anyone with questions regarding an assigned rating.

## Reputation Assignment

The investigators on the threat analysis team follow stringent policies and guidelines for the nomination and removal of IP addresses from the databases that are part of the Email Reputation Services Standard level of service. An IP address receives a reputation assignment if it:

- Sent spam or in some way has supported the sending of spam (for example, offering services to spammers or allowing their resources to be used by those who send spam).
- Is an unsecured email server (“open relay”) that has been used to send spam.
- Is an unsecured port on a machine (“open proxy”) that has been used to send spam.
- Is a dynamically assigned address that should not be used as an email server.

Before processing an IP address, the Smart Protection Network categorizes it according to careful guidelines. The same investigator who assigned the reputation can also check any requests to change the assigned reputation. Every effort is made to make sure the reputation record is accurate and that changes are made in a timely manner.

Each reputation record includes samples of the actual spam received from the IP address, the history of spamming behavior, a record of any correspondence regarding mediation, any resolution of issues, and other related information. For dynamically assigned IP addresses that were submitted to the standard reputation database by the ISP, the reputation record will include submission dates and any limitations that the ISP placed upon it.

To check the reputation of an IP address, refer to [Look Up IP Addresses on page 4-4](#).

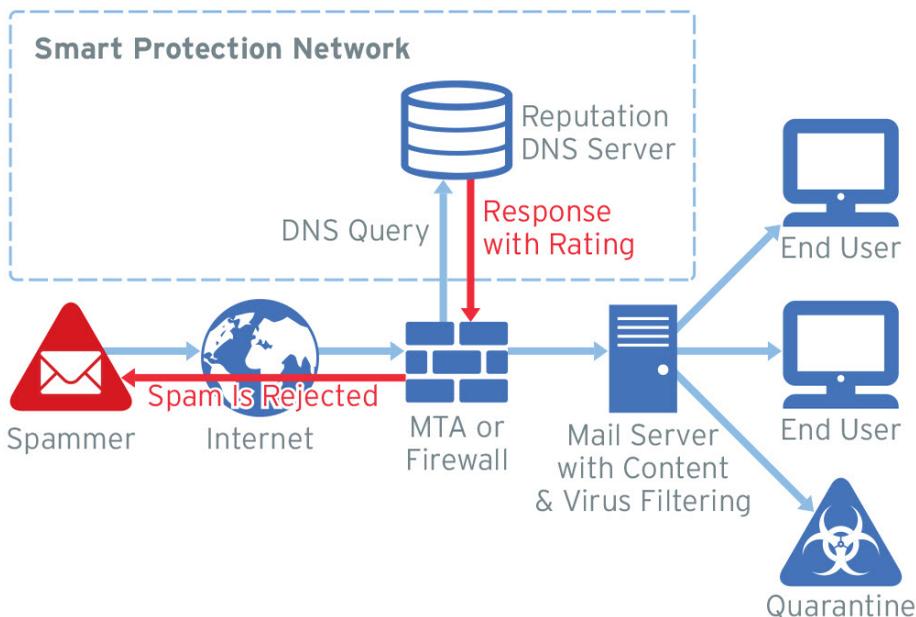
## Delivery Infrastructure

Trend Micro has built some of the largest IP networks and data centers in the world. The Trend Micro network DNS and database servers are geographically distributed in major facilities worldwide, and continuously monitor and tune the network to assure the highest availability possible for Email Reputation Services customers.

## How It Works

The actual implementation of Email Reputation Services involves one DNS look-up per IP address. When an email server accepts the initial connection from another email server, it records the IP address of the machine

requesting the connection. The receiving email server then queries its DNS server to determine if there is a record for that IP address.



**FIGURE 1-1. Smart Protection Network Workflow**

For Standard, a single DNS query is sent to the standard reputation database, which contains known and documented sources of spam as well as an extensive listing of dynamic IP addresses. Any positive response from this database should result in your email server's returning a 550 error, or rejection of the requested connection.

For Advanced, a single DNS query is sent to the standard and dynamic reputation databases. A positive response from the dynamic database should result in your email server's returning a 450 error, or "temporary failure" of the requested connection. Listings in this database are occasionally legitimate email servers that have compromised hosts behind them that are temporarily sending spam. If the connection request is from a legitimate email server, it will requeue and try again later, causing a delay in email delivery until the listing expires but will not block the email.

Depending on the capabilities of your email server, additional options for handling IP connections may be available to you. Some allow for throttling or limiting the number of connections accepted from an IP over a designated time period. Still others allow you to set different levels of scanning to messages from questionable IP addresses as opposed to known IP addresses. The ultimate goal is to reject as many connections as possible upon initial request; those rejected connections represent spam messages that are never accepted and are thus never brought into the email infrastructure. Keeping unwanted spam out of the infrastructure means that valuable bandwidth, processing, and storage resources are not wasted.

## Blocking Connections As Opposed to Messages

Customers find that adding Email Reputation Services to their anti-spam solutions has an exponential impact on offloading existing filtering solutions. What can appear to be only a small increase in blocked connections can translate into a large reduction of actual messages entering the filtering portion of their email infrastructure.

Translating blocked connections into blocked messages is more involved than simply applying a 1:1 ratio. Studies show that while legitimate sources average slightly more than one message per connection, each connection from a spam source contains, conservatively, an average of 1.6 messages.

It is far more efficient to reject spam at the connection level rather than take each message through full anti-spam scanning.

**TABLE 1-1. Connection Blocking and Scanning Requirements**

Connection Blocking Requirements	Scanning Each Message Requirements
The initial portion of the SMTP handshake	The full SMTP-handshake
A DNS query	Complete message parsing, putting strains on computers that run anti-spam solutions



## Chapter 2

### Blocked?

If your ISP address has been blocked but you are not the administrator of the IP address(es) in any of the Email Reputation Services lists, contact your ISP to resolve the problem. Trend Micro Email Reputation Services cannot resolve issues regarding any of the blocked lists with end-users or those who are not directly responsible for the particular network on the blocked lists.

If you are the ISP provider and your IP address, or your subscriber's IP address has been blocked, refer to [Step 3: Send a Removal Request on page 2-5](#).



#### Note

Trend Micro will only remove IP addresses at the request of the valid owner of the IP space.

---

There are several reasons why an IP address may need to be removed from the blocked lists:

- Network reorganization

If an ISP, especially a smaller one with a single or more Class C networks to its name, reorganizes its IP address pool so its fixed servers and dial-ups change places.

- Network inheritance

If you inherited an address pool that had previously been or are still being blocked.

- Listing error

Because IP addresses are dynamic, some IP addresses might have been added to the blocked lists incorrectly.

But why is your address being blocked? Here are some reasons why.

- If your IP address is in the DUL list and:
  - If you use a standard mail client, it is probably because your mail program is set to use a mail server other than the one your current ISP provided you.
  - If you use a mail (SMTP) server on your own computer, or you share your Internet connection with several other people on a local network with a proxy server, it is probably because your recipients cannot tell the difference between your legitimate mail delivery and a spammer's trespassing on their equipment.
- If your IP address is in the Known Spam Source List, your IP address may be getting blocked because the IP address:
  - May be a known spam source
  - May supports a service that sends spam
  - May use multi-hop open relay
  - May be using a compromised host
- If your IP address is in the QIL list, there might be some unauthorized activities happening on your computer or server. This might mean that your computer has been hacked or compromised.
- [Step 1: Determine Your IP Address on page 2-4](#)
- [Step 2: Check the Status of Your IP Address on page 2-4](#)
- [Step 3: Send a Removal Request on page 2-5](#)

- *Step 4: Investigation on page 2-6*

## Step 1: Determine Your IP Address

You can use the command console to find your IP address. But if you are unsure of which IP address to look up, please check the bounced mail message and headers for a line that looks similar to this:

---

### Procedure

- 550 Service unavailable; Client host [127.0.0.2] blocked using Trend Micro RBL+.

Please see [https://www.ers.trendmicro.com/reputations/index?ip\\_address=127.0.0.2](https://www.ers.trendmicro.com/reputations/index?ip_address=127.0.0.2)

---

The IP address you would want to check, in this case, is 127.0.0.2.

## Step 2: Check the Status of Your IP Address

If you think your IP address has been blocked, you can use the lookup form to check whether your IP address has been blocked.

---

### Procedure

- If the form cannot find the IP address on any list, please contact your administrator or ISP provider.
  - If the IP address has been blocked, this form will show which list the IP address is on. If the IP address is on more than one list, you will need to send a removal request for each list. For more information, refer to [Step 3: Send a Removal Request on page 2-5](#).
-

**Note**

Make sure you use the correct contact information and process to request removal from a list. Sending your request to the inappropriate contact will cause a delay, and possible inaction, on processing your request.

---

## Step 3: Send a Removal Request

Once you have established that the IP address is being blocked, you can send a removal request for each list.

---

### Procedure

1. Check the status of your IP address. Refer to [Step 1: Determine Your IP Address on page 2-4](#).
  2. Send a request to have it removed:
    - Send a request to your administrator or ISP provider.
    - If you are the administrator or ISP provider, send a request to Trend Micro:
      - a. Click the Request to be removed from the global blocked list link.
      - b. You need to provide the requested information on the web form.
      - c. Click **Send**.
- 

**Note**

Removal requests have to come from an authoritative account such as: abuse@(domain name) or postmaster@(domain name). This ensures that Trend Micro is in contact with the valid owner of the IP block(s).

---

## Step 4: Investigation

After Trend Micro receives the necessary information, the IP address(es) are monitored and Trend Micro will communicate with the IP block owners to determine validity of the claims.

Trend Micro will determine what actions caused the listing, what has been done to resolve these issues and what can be done to prevent them from occurring in the future. If necessary, they will ask about abuse handling policies, acceptable use policies, and any problems encountered in the notification.

These discussions will be documented and studied to proceed with a recommendation for the listing (removal, probation, maintain listing). There is a probationary period where the IP is removed from the list but can be reactivated without a new nomination if there are new occurrences. The listing is monitored for an appropriate period of time to ensure that there are no new instances of spamming activity. If there is no new spamming activity at the end of the probationary period, Trend Micro removes the IP address from the blocked lists.

# Chapter 3

## Getting Started

This chapter includes information on how to get started using Trend Micro™ Email Reputation Services.

- *[Configuring Email Reputation Services on page 3-2](#)*
- *[Logging Onto the Console on page 3-5](#)*

## Configuring Email Reputation Services

Email Reputation Services is most effective when it is the first line of defense in your messaging infrastructure. Trend Micro recommends that you remove any other DNS blocking techniques after you enable Email Reputation Services.

To enable and configure Email Reputation Services see the following:

- [Creating an Account on page 3-2](#)
- [Configuring Your MTA on page 3-5](#)

### Creating an Account

Create an account to sign up. You can try Email Reputation Services (refer to [Request Trial Account on page 3-4](#)) or purchase the full service. After signing up, you will receive an email with instructions on how to proceed.

If you sign up for a trial, you need to complete the request form appropriate to the service level that you wish to evaluate. If you purchase the full service, Trend Micro provides you with instructions on creating a customer account. Afterwards, Trend Micro sends you an Activation Code by email.

The Activation Code allows you access to only the level of service to which you are registered (Standard or Advanced).

**Note**

The Activation Code for Email Reputation Services Advanced includes access to Email Reputation Services Standard, which is a subcomponent.

It may take up to one hour from when your Activation Code is issued before it is recognized by the Trend Micro Email Reputation Services systems.

---

If you don't create an account, you can still query the reputation of an IP address (refer to [Look Up IP Addresses on page 4-4](#)) or nominate an IP address to the Global Approved List (refer to [Global Approved List on page](#)

4-5). However, you will not be able to configure your settings for better spam protection.

---

### Procedure

1. Open your browser to the following URL:

<https://www.ers.trendmicro.com>

2. Click the **Sign up** link below the Logon fields.

The **Create an Account** page displays.

3. Provide the following information:

- Activation code



#### Note

If you have not purchased the service and just want to try out the service, click **Request a trial activation code link**. Refer to *Request Trial Account on page 3-4*.

---

- Email address (twice)
- Password (twice)
- First name
- Last name
- Company name
- Country/Region
- Type of company



**Note**

The Activation Code should be the same Activation Code used when configuring your MTA to access Email Reputation Services. Trend Micro will send an email message to the address filled out in the form. This message provides your user name, password, and a URL to click to activate the account.

---

4. Click Sign up.
- 

## Request Trial Account

If you have not purchased the service and just want to try out the service, you can request for a trial activation code.

After you register for the trial service, Trend Micro sends you an activation code email with instructions for configuring your MTA. This activation code will be valid only during the evaluation period. You will need to obtain a new activation code when you purchase the service.

---

### Procedure

1. Open your browser to the following URL:

<https://www.ers.trendmicro.com>

2. Click the **Sign up** link below the Logon fields.

The **Create Account** page displays.

3. Click the **Request a trial activation code** link.

The **Email Security Advanced Free 30-Day Trial** page displays.

4. Complete the form to get your free trial.
5. Return to the **Create Account** page.

6. Specify the trial Activation Code and the required information to sign up your Email Reputation Services account.
- 

## Configuring Your MTA

The next step is to configure your MTA to perform the appropriate DNS queries for the type of Email Reputation Services to which you subscribed:

- **Standard:** Reject connections with a 550 level error code (“connection refused”).Your MTA returns this error code to the server initiating the connection because the IP address is in the Standard Reputation database as a known spammer.
- **Advanced:** After querying the standard and dynamic reputation databases, your MTA returns a temporarily deny connection 450 level error code (“server temporarily unavailable, please retry”) if the IP address is in the dynamic reputation database.

Legitimate email servers that may have compromised hosts that are temporarily sending spam may be listed in the dynamic reputation database. If the connection request is from a legitimate email server, it will requeue and try sending the message later. This process will cause a short delay in mail delivery until the listing expires but will not permanently block the email.

Some servers may have additional options for handling questionable IP connections. These options include throttling or routing messages for more detailed scanning.

For detailed configuration and set-up options, refer to your product manuals and/or technical support organization. You can also refer to: <https://success.trendmicro.com/>

## Logging Onto the Console

Email Reputation Services is part of the Trend Micro Smart Protection Network.

---

## Procedure

1. Open your browser to the following URL:

<https://www.ers.trendmicro.com>

2. Type your User name or Email address, and Password.
3. Click **Log On**.

Trend Micro Email Reputation Services portal displays.

---



### Tip

Trend Micro recommends changing your password after you log on for the first time.

Refer to *Changing Account Details on page 4-14*.

---

## Forgot Password

If you forgot your password and cannot log on to the service, you can reset your password.

---

## Procedure

1. Open your browser to the following URL:

<https://www.ers.trendmicro.com>

2. Click the **Forgot your password?** link below the Password field.
3. Type your email address. You should receive an email message from Trend Micro.
4. Click the link in the email.

The **Reset Your Password** screen appears.

5. Type your new password twice.

**6. Click Update.**

---



# Chapter 4

## Using the Administrative Console

After you create an Trend Micro™ Email Reputation Services account, log on to the administrative console and begin configuring your settings.

- *[Email Reputation Services Console on page 4-2](#)*
- *[IP Reputation on page 4-4](#)*
- *[Managing the Policy on page 4-7](#)*
- *[Administration on page 4-14](#)*

## Email Reputation Services Console

The large map and accompanying chart on this screen display spam statistics gathered from data centers worldwide.

From this dashboard, you can:

- View the Global Spam Threat statistics, refer to [Global Spam Threats on page 4-2](#).
- View Your Network statistics, refer to [Your Network on page 4-3](#).

**Note**

You can only view Your Network statistics from the dashboard after you have logged on.

---

- Look up an IP address reputation, refer to [Look Up IP Addresses on page 4-4](#).
- Nominate an IP address to the Global Approved List database, refer to [Global Approved List on page 4-5](#).
- Click the link to Global spam news, which features the latest notable spam attacks showcasing screenshots and solution details for Trend Micro users.

## Global Spam Threats

You can see two kinds of statistics from this tab:

---

**Procedure**

- Global Spam Threat statistics, by country

The darker the color, the higher the spam rate of a country. Trend Micro computes the spam rate from the email messages that pass through its network, and the spam blocked by Email Reputation Services.

To view more information, you can:

- Mouse-over a given country and a balloon icon will appear showing the current statistics.
- Use the left-side slider to zoom in or out of the map for a closer look.
- Click the Home icon to revert to the original size.
- Click and drag to reposition the map or the chart information.
- A visual chart of spam data

The Spam index shows the current spam trends derived from monitoring the volume of spam sent to Email Reputation servers all over the world.

You can filter the spam trends by clicking Week, Month, or Year.

---

## Your Network

After you've logged in, you can see two kinds of statistics from this tab:

---

### Procedure

- Spam statistics for your network

To view the current statistics for your network on the map, the flashing globe “MY ERS” icon for a given country. A panel displays with the name of the country.

To view more information, you can:

- Mouse-over a given country and a balloon icon will appear showing the current statistics.
- Use the left-side slider to zoom in or out of the map for a closer look.
- Click the Home icon to revert to the original size.

- Click and drag to reposition the map or the chart information.
- A visual chart of all email messages your network received and blocked

Email Reputation Services protects against known and unknown sources of spam by blocking spam messages at the SMTP connection level. When a mail server attempts to connect to an MTA that is protected by Email Reputation Services, your DNS resolver queries the Email Reputation Services lists using the criteria associated with your account.

If Email Reputation Services reports that the mail server is listed on one of the Email Reputation Services reputation lists, then that connection attempt is added to the “Blocked Spam messages” number.

You can filter the spam trends by clicking Day, Week, or Month.

---

## IP Reputation

In this section, you can:

- Look up IP addresses (refer to [Look Up IP Addresses on page 4-4](#))
- Nominate an IP address to the Global Approved List (refer to [Global Approved List on page 4-5](#))

### Look Up IP Addresses

If you suspect that your IP address is being blocked by Email Reputation Services, please look up the full IP address and determine which database it is listed in.



**Note**

This lookup tool is based on IP addresses and does not use host or domain names.

---

To look up an IP address:

---

## Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
2. Go to **IP Reputation > Lookup**.
3. Type the IP address.
4. Click **Check**.

Depending on the results, you can do one of the following:

- If the IP address is not in one of the Email Reputation Services databases, the IP address comes from a reputable source. You can ask Trend Micro to add this IP address to the Global Approved List (refer to *Global Approved List on page 4-5*).
- If it is unlisted but you think the IP address sends spam and you doubt the integrity of the IP address, you can block the IP address from your network (refer to *Blocked Lists on page 4-9*).
- If it is listed, you can request to temporarily remove it from the Global Blocked List.

---

## Global Approved List

Trend Micro maintains several databases that are either approved or blocked IP addressed, based on their behavior. One such database is the Global Approved List. IP addresses in this list are IP addresses that have been authenticated and are known to come from approved senders. IP addresses in this list are automatically approved and pass through the network.

While Trend Micro maintains this database, you can also nominate your IP address to be added to this list. Trend Micro will then conduct their investigation and determine if the IP address you nominated should indeed be a part of this database.

To nominate an IP address to the Global Approved List:

---

## Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
2. Go to **IP Reputation > Global Approved List**.
3. Read through the Global Approved List description. If you agree, click **I Understand and Agree**.



### Note

Provide all the necessary information on each of the following tabs to ensure that Trend Micro can conduct a full investigation. You may also be asked to provide more information if the provided information are not enough.

---

4. From the **Mail Transfer Agent** tab:
  - To add one (1) or (2) entries:
    - a. Provide the following:
      - IP
      - FQDN
      - Email domain name
      - Company name
      - Country/Region
      - Type of company
    - b. To add another entry, click **Add an entry**.
  - To add more Mail Transfer Agent entries:
    - a. Download a sample CSV file.
    - b. Provide the necessary information and save the file.

- c. Import the file to the site.
5. From the **HELO/EHLO Checking** tab:
  - To add one (1) or two (2) entries, provide the HELO/EHLO string. You can also click **Add an entry** to add another string.
  - To add more HELO/EHLO string entries:
    - a. Download a sample CSV file.
    - b. Provide the necessary information and save the file.
    - c. Import the file to the site.
6. From the **Contact Information** tab, provide your email address, first and last name.
7. Click **Nominate**.

Trend Micro will investigate and determine if the IP address can be added to the Global Approved List. If the IP address does not fulfill the criteria to be added to the Global Blocked List, you can still add the IP address to your internal Approved lists ([Approved Lists on page 4-8](#)).

---

## Managing the Policy

In the Policy section you can:

- Create an Approved Sender list to always receive email messages from certain trusted countries and IP addresses.
- Create a Blocked Sender list to always block email messages from certain countries and IP addresses.
- Adjust Dynamic Reputation settings.

You can define the lists by individual IPv4 or IPv6 IP addresses, or by country.

## Approved Lists

Approved lists allow messages from approved senders to bypass IP-level filtering. The Approved lists are not applied to your MTA, but you can set up additional approved or blocked senders, or perform additional filtering at your MTA. The trade-off for bypassing IP filtering is the additional resources that are needed to process, filter, and store the higher levels of spam messages that would otherwise have been blocked.

In the case of a standard reputation (Known Spam Source List) service lookup, the order of the evaluation hierarchy is:

1. Approved IP
2. Blocked IP
3. Approved country
4. Blocked country

For dynamic reputation (QIL) service lookup, the customer-defined “blocked policy lists” (IP, Country) are ignored and only the Approved lists are checked. Otherwise, the order of policy lookup (first IP, then country) is the same as for standard reputation (Known Spam Source List) service.

Avoid specifying overlapping CIDR ranges in the Approved and Block lists because the Block list might take priority over the Approved list.

To add to the Approved list:

---

### Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
2. Click **Policy > Approved Lists**.
3. Select the country and click **Add >**. The name of the chosen country should move to the right frame.

**WARNING!**

Be very selective when adding a country as you might also be adding known spammers to the approved list.

---

4. Specify the IPv4 or IPv6 address and click Add >. The IP address should move to the right frame.

When specifying the IP address, you can use either of the following:

- Standard IPv4 format: 123.123.123.123
- IPv4 IP address range in CIDR notation: 123.123.123.123/24

**Note**

Avoid specifying the same CIDR range in the Approved and Blocked lists, as unexpected results might occur. If required, the approved CIDR range must be less than or equal to the blocked CIDR range.

For example, avoid specifying 172.31.15.164/30 in the Approved list and 172.31.15.164/31 in the Blocked list

---

- Standard IPv6 format:
  - 2001:0db7:85a3:0000:0000:8a2e:0370:7334
  - 2001:db7:85a3:0:0:8a2e:370:7334
  - 2001:db7:85a3::8a2e:370:7334

5. Click **Save**.
- 

## Blocked Lists

Blocked lists stop messages from the blocked senders, bypassing IP-level filtering. The Blocked lists are not applied to your MTA, but you can set up additional blocked or approved senders, or perform additional filtering at your MTA. The trade-off for bypassing IP filtering are the additional resources that are needed to process, filter, and store the higher levels of

spam messages that would otherwise have been blocked. When using the Blocked lists, you may experience lower overall spam catch rates.

In the case of a standard reputation (Known Spam Source List) service lookup, the order of the evaluation hierarchy is:

1. Approved IP
2. Blocked IP
3. Approved country
4. Blocked country

For dynamic reputation (QIL) service lookup, the customer-defined “blocked policy lists” (IP, Country) are ignored; only the Approved lists are checked. Otherwise, the order of policy lookup (first IP, then country) is the same as for standard reputation (Known Spam Source List) service.

To add to the Blocked list:

---

### Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
2. Click **Policy > Blocked Lists**.
3. Select the country and click **Add >**. The name of the chosen country should move to the right frame.
4. Specify the IPv4 or IPv6 address and click **Add >**. The IP address should move to the right frame.

When specifying the IP address, you can use either of the following:

- Standard IPv4 format: 123.123.123.123
- IPv4 IP address range in CIDR notation: 123.123.123.123/24

**Note**

Avoid specifying the same CIDR range in the Approved and Blocked lists, as unexpected results might occur. If required, the approved CIDR range must be less than or equal to the blocked CIDR range.

For example, avoid specifying 172.31.15.164/30 in the Approved list and 172.31.15.164/31 in the Blocked list

---

- Standard IPv6 format:
  - 2001:0db7:85a3:0000:0000:8a2e:0370:7334
  - 2001:db7:85a3:0:0:8a2e:370:7334
  - 2001:db7:85a3::8a2e:370:7334

**5. Click Save.**

---

## Reputation Settings

You can choose which lists to enable from those that make up the Standard Reputation database. By default, all lists are enabled. The default setting is the most effective combination for reducing spam levels, and it meets the needs of most customers. You can also use the dynamic reputation slider to adjust how aggressively Email Reputation Services blocks email connections.

---

**WARNING!**

If you disable some lists from the Standard database, you may see an increase in the amount of spam messages that reach your internal mail server for additional content filtering.

---

## Standard Reputation Services Database

The Standard Reputation Services includes a database with the following lists:

- The **Known Spam Source List** is a list of IP addresses of mail servers that are known to be sources of spam.

- The **Dial-up User List (DUL)** is a list of dynamically assigned IP addresses, or those with an Acceptable Use Policy (AUP) that prohibits public mail servers. Most entries are maintained in cooperation with the ISP owning the network space. IP addresses in this list should not be sending email directly but should be using the mail servers of their ISP.
- The **Emerging Threat List (ETL)** includes IP addresses of mail servers involved in active ransomware, malware, or other email threat campaigns.

For the Standard section:

- You can enable or disable the lookup of selected lists by using the check boxes.
  - Select the check box to enable the list.
  - Clear the check box to turn off the list. The Email Reputation Services system will skip that list during a lookup request.
- Click the **Save** button to save new settings.

## Dynamic Reputation Slider

Use the dynamic reputation slider to set blocking levels as follows:

- **More aggressive:** If too much spam is reaching your network, select a more aggressive setting. However, this setting might also block connections from legitimate email senders.
- **Less aggressive:** If legitimate email is being blocked, select a less aggressive setting.

**Tip**

Trend Micro recommends that you make changes to the Dynamic Settings carefully and in small increments. You can then fine-tune your settings by measuring the increased amount of spam and legitimate messages received and making additional small changes.

If you are receiving many spam messages and want to block as many as possible, use the most aggressive level. If this setting blocks too many legitimate messages, you can reduce this setting by one level and evaluate it based on the resulting proportion of spam messages received.

---

## Configuring Reputation Settings

To configure reputation settings:

---

### Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
2. Go to **Policy > Reputation Settings**.
3. Enable or disable one of the Standard Reputation Services list.
4. Under **Advanced Reputation Service**, move the slider to one of the following points:
  - **Level 4:** The most aggressive setting. If Email Reputation Services detects even a single spam message from a sender IP address, it adds the sender address into the dynamic reputation database. The length of time that the IP address stays in the database depends on whether Email Reputation Services detects additional spam from the sender.
  - **Level 3:** A moderately aggressive setting. Email Reputation Services allows a small volume of spam from senders with a good rating. However, if Email Reputation Services detects an increase in spam beyond the allowable threshold from such a sender, it adds the sender to the dynamic reputation database. The length of time that

the IP address stays in the database depends on whether Email Reputation Services detects additional spam from the sender. The length of time may be extended up to maximum as in Level 4.

- **Level 2:** A moderately tolerant setting. Email Reputation Services allows a larger volume of spam from a sender with a good rating. However, if Email Reputation Services detects an increase in spam above the allowable threshold from such a sender, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database is generally shorter than the time for level 3.
- **Level 1:** The least aggressive setting. Email Reputation Services allows the same amount of spam from a sender with a good rating, as in level 2. The length of time that an IP address stays in the database is shorter, in general, than that for level 2.

5. Click **Save**.

---

## Administration

In the Administration section, you can do the following:

- Change the administrative console user name and password
- Change the Activation Code

### Changing Account Details

You can change your account ID email address and password. To protect your account, Trend Micro recommends changing the password regularly. The password must be between eight (8) and thirty-two (32) alphanumeric characters.

### Changing the Account ID

To change the account ID:

---

### Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
  2. Go to **Administration** > **Account Details**.
  3. Click the **Account ID** tab.
  4. Type the new Account ID twice.
  5. Type your password.
  6. Click **Update**.
- 

### Changing the Password

To change the password:

---

#### Procedure

1. Open the following URL:  
<https://www.ers.trendmicro.com>
  2. Go to **Administration** > **Account Details**.
  3. Click the **Password** tab.
  4. Type the old password once and the new password twice.
  5. Click **Update**.
- 

### Changing the Activation Code

To upgrade, reactivate, or continue using your service, provide the new Activation Code you received from Trend Micro on the license screen. If your new Activation Code validates correctly, then it will be saved and used immediately.

To change your Activation Code, type your new Activation Code and then click **Activate**.

# Chapter 5

## Getting Help

This chapter describes how to get additional help for issues that may arise and how to contact support.

- *Frequently Asked Questions (FAQs) on page 5-2*
- *Getting Help with the Administrative Console on page 5-3*
- *Contacting Trend Micro on page 5-4*
- *Documentation Feedback on page 5-6*

## Frequently Asked Questions (FAQs)

- [\*Why Were You Referred To This Website? on page 5-2\*](#)
- [\*Why is My IP Listed in the Known Spam Source List? on page 5-2\*](#)
- [\*Why is My IP Listed in DUL? on page 5-2\*](#)
- [\*Why is My IP Listed in ETL? on page 5-3\*](#)
- [\*Why is My IP Listed in QIL? on page 5-3\*](#)
- [\*Why Did I Receive A Bounced Email But The IP Address Is Not On Any Blocked List? on page 5-3\*](#)

### Why Were You Referred To This Website?

Most people find this website after they receive a bounced email telling them that their mail was rejected and refers them to this site. If you received an email referring you to Trend Micro Email Reputation Services, it is most likely because the IP address used by your mail server has been blocked.

### Why is My IP Listed in the Known Spam Source List?

Your IP is listed in the Known Spam Source List because we received spam mail from this IP address. There was no action taken when we reported this issue to your ISP.

### Why is My IP Listed in DUL?

Your IP is listed in DUL because it is not defined in rDNS as static. Please contact your ISP to correctly define your IP address.

## Why is My IP Listed in ETL?

Your IP may be involved in active ransomware, malware, or other email threat campaigns.

## Why is My IP Listed in QIL?

Your IP is listed in QIL because they were recently involved in sending spam mail.

## Why Did I Receive A Bounced Email But The IP Address Is Not On Any Blocked List?

You may have given your local IP instead of the one your ISP provided. Please contact your ISP to give you the correct IP address. Or you can also check the bounced mail message and headers for a line that looks similar to this:

---

### Procedure

- 550 Service unavailable; Client host [127.0.0.2] blocked using Trend Micro RBL+.

Please see [https://www.ers.trendmicro.com/reputations/index?ip\\_address=127.0.0.2](https://www.ers.trendmicro.com/reputations/index?ip_address=127.0.0.2)

---

The IP address you would want to check, in this case, is 127.0.0.2.

## Getting Help with the Administrative Console

For detailed information about working with the administrative console, see the help files. You can access page-level help for a particular screen by clicking the help icon near the upper-right corner of each screen.

## Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	<a href="https://www.trendmicro.com">https://www.trendmicro.com</a>
Email address	<a href="mailto:support@trendmicro.com">support@trendmicro.com</a>

- Worldwide support offices:  
<https://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:  
<https://docs.trendmicro.com>

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent

- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

## Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

---

### Procedure

1. Go to <https://success.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



#### Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/smb-new-request>

---

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

---

## Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

## Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://www.ers.trendmicro.com/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<https://success.trendmicro.com/solution/1112106>

## Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<https://docs.trendmicro.com/en-us/survey.aspx>

# Appendix A

## Glossary

## Dynamic Reputation Database (QIL)

The Dynamic Reputation Database or Quick IP List is a highly dynamic list and uses advanced detection techniques for attacks caused by botnets (zombie networks, SMTP malware, spyware). IP addresses are added and removed quickly due to the nature of the threat.

## Dial-up User List (DUL)

Dial-up User List (DUL) includes IP addresses in dynamic ranges identified by ISPs. Most legitimate mail sources have static IP addresses.

## Emerging Threat List (ETL)

The **Emerging Threat List (ETL)** includes IP addresses of mail servers involved in active ransomware, malware, or other email threat campaigns.

## False Positive

A false positive occurs when an email sender is incorrectly labeled a spammer. If you subscribed to the advanced version of Email Reputation Services, you can adjust how strict Email Reputation Services is with servers attempting to establish email connections with your network.

If you select a setting that is too strict, you could block connections from senders trying to deliver legitimate email.

## Global Approved List

The Global Approved List includes legitimate mail sources collected by Email Reputation Sources and the Threat Protection Network.

## HTTP

Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.

## HTTPS

Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.

## IP

"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

## Known Spam Source List

The Known Spam Source List includes IP addresses historically associated with sending spam.

## Marketing Message List

The Marketing Message List (MML), also known as Graymail, includes legitimate mail sources historically known to send extensive marketing messages.

## Phish Attack

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix to avoid account termination. The email will include a URL to a Web site that looks exactly like the real thing. It is simple to copy a legitimate email and a legitimate Web site but then change the so-called backend, which receives the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as a logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any Web site you suspect to be a phishing site. See [Sending Suspicious Content to Trend Micro on page 5-5](#) for more information.

## Ping

Ping is a utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the computer with the specified IP address is online or not.

## SOCKS 4

SOCKS 4 is a TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers

outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.

## TCP

Transmission Control Protocol (TCP) is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.



# Index

## **D**

documentation feedback, 5-6

## **S**

support

    resolve issues faster, 5-4





**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A.  
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736  
Email: support@trendmicro.com

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: EREM09072/200812