Email Anti-Malware

Administrator Guide

Email Anti-Malware Administrator Guide

Documentation version: 1.0

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support** > **Contact us**.

Contents

Chapter 1

Introduction to Anti-Malware

This chapter includes the following topics:

About Anti-Malware

Anti-Malware re-routes your inbound email and outbound email through the detection infrastructure. Multiple scanners, including the Skeptic™ scanner, scan the emails before they pass on to the final destination. Skeptic uses predictive technology to identify and stop new virus and malware outbreaks as they occur and before virus signatures are available. (A virus signature is a unique string of bits that defines a specific computer virus. The signature is then used to detect instances of the virus.) Polling for signature updates is performed automatically every 10 minutes. Instant updates are carried out in the event of a new outbreak.

If an email is free of malware, it is delivered to the intended recipient. If malware is detected, the email is quarantined. Any email that is found to be infected is quarantined for 30 days. Blocked malware notifications are generated automatically, and can be configured to be sent to the intended recipient and up to 5 Administrators. The service has no discernible effect on email delivery times.

Use the portal to configure Anti-Malware to your requirements.

About detecting malicious URL links

Link Following offers protection against malicious URL links within emails. Such links differ from email malware threats because the user performs a direct action to follow the link to a malicious website. Skeptic actively follows links in emails and checks the destination website for malware or other types of potentially harmful content in real time. When a link is confirmed as malicious, a signature is created. Any further emails that contain a confirmed malicious link are treated as being infected with malware and are quarantined.

Note: To benefit from a real-time solution to protect your organization from web-based malware threats, inquire about Web Security.

Configuring Anti-Malware

This chapter includes the following topics:

Defining global or domain-specific settings

You can configure the Anti-Malware settings globally for all domains, or you can configure custom settings for an individual domain. Typically, you use the global settings to configure the Anti-Malware service and then make fewer changes for individual domains.

If you make changes to the settings for an individual domain, you cannot then change the settings for that domain back to global settings.

To apply settings globally, or to a specific domain

1. Select **Services** > **Email Services** > **Anti-Malware**.
2. On the **Anti-Malware** page, do one of the following:
   - To specify global settings, select **Global Settings** from the drop-down list.
     The settings in the page are editable. The changes that you make are applied to all of your domains, unless a particular domain already has custom settings.
   - To specify custom settings for a domain, select the domain from the **Global Settings** drop-down list.
     When you select a specific domain to work with, the name of the domain is displayed as a heading.

The fields in the page are editable and inherit the global settings, until you make a change. The changes you make are applied only to the selected domain.

Configuring Anti-Malware Alert Settings

Alert settings define how administrators and recipients are notified when email messages contain suspected malware. You configure Anti-Malware alert settings on the **Services > Anti-Malware > Alert Settings** tab.

Table 2-1 Anti-Malware alert settings

Settings	Description	More information
Email addresses	Define the address from which alerts are sent, and the administrator addresses that receive alerts	See "Configuring sender and administrator email addresses for alerts" on page 9.
Blocked Malware Alert	Enable alerts for Administrators and recipients when malware is detected and email is quarantined, and define the messages that they receive.	See "Configuring blocked malware alerts" on page 10.
Detected Malware Alert	Enable alerts for Administrators and recipients when malware is detected after email is delivered, and define the messages that they receive.	See "Configuring detected malware alerts" on page 11.

See "Defining global or domain-specific settings" on page 8.

Configuring sender and administrator email addresses for alerts

The sender email address is the address from which Anti-Malware alerts are sent. You can use the default email address of alerts@notifications.messagelabs.com, or you can enter a custom email address that is on your mail system.

All administrator email addresses receive the alerts that are configured for administrators. You can specify up to 5 administrator email addresses.

To define sender and administrator email addresses

1. Select **Services** > **Email Services** > **Anti-Malware**.
2. On the **Alert Settings** tab, **Email Addresses** section, either accept the default address or enter a different **Sender Email** address.
3. Under **Administrator Email**, enter an Anti-Malware Administrator's email address and click **Add**.
4. Repeat step 3 for each additional administrator that you want to notify.
5. At the bottom of the tab, click **Save**.

Configuring blocked malware alerts

The Anti-Malware service sends a blocked malware alert when an incoming or outgoing email message is quarantined because the message contains suspected malware.

- **Inbound Alerts** are issued when emails that are addressed to internal users are quarantined because they contain suspected malware.
- **Outbound Alerts** are issued when internal users attempt to send emails that contain suspected malware, and these emails are quarantined.

For each alert, you can specify whether administrators, recipients, or both receive blocked malware alerts.

You can also create custom blocked malware alert messages for inbound and outbound blocked email. Each blocked malware alert should include the Pen number for the quarantined email. The Pen number is a unique reference number that is used to locate and release the email from within the portal.

To configure blocked malware alerts

1. Select **Services** > **Email Services** > **Anti-Malware**.
2. On the **Alert Settings** tab, **Blocked Malware Alert** section, select **Administrators** or **Recipient(s)** as appropriate.
   - Under **Inbound Alerts**, check **Administrators** to send these alerts to all administrator emails that are configured to receive alerts. Check **Recipient(s)** to send alerts to the internal users to which the quarantined emails were addressed.
   - Under **Outbound Alerts**, check **Administrators** to send these alerts to all administrator emails that are configured to receive alerts. Check **Recipient(s)** to send alerts to the internal users who attempted to send the emails that were quarantined.

3 To view the default text for inbound or outbound blocked malware alerts, or to create custom alert messages, click **Edit Alerts**.

4 In the **Blocked Malware Alert Settings** dialog box, when **Default** is selected, you can view, but not edit, the default alert messages.

- To use the default messages, click **Cancel**.
- To customize an alert message, change **Default** to **Custom**. You can now edit the subject line and body text of the selected message or replace the text completely. You can also choose placeholders from the dropdown list to insert variables into the alert emails. These variables are replaced by data before the alerts are sent.

See "About placeholders in malware alerts" on page 12.

5 When you finish editing alerts, click **Save**.

6 At the bottom of the **Alert Settings** tab, click **Save**.

Configuring detected malware alerts

Note: Depending on your organization's configuration, you may not have access to the functionality described here.

The Anti-Malware service sends a detected malware alert when an incoming or outgoing email message is delivered and then is later found to contain suspected malware.

- **Inbound Alerts** are issued when emails that are delivered to internal users are later found to contain suspected malware.
- **Outbound Alerts** are issued when internal users send emails that are later found to contain suspected malware.

For each alert, you can specify whether administrators, recipients, or both receive alerts.

You can also create custom alert messages for inbound and outbound detected malware. Each blocked malware alert should include the Pen number for the quarantined email. The Pen number is a unique reference number that is used to locate and release the email from within the portal.

To configure detected malware alerts

1 Select **Services** > **Email Services** > **Anti-Malware**.

2 On the **Alert Settings** tab, **Detected Malware Alert** section, select **Administrators** or **Recipient(s)** as appropriate.

- Under **Inbound Alerts**, check **Administrators** to send these alerts to all administrator emails that are configured to receive alerts. Check **Recipient(s)** to send alerts to the internal users to which the emails that contained the detected malware were addressed.
- Under **Outbound Alerts**, check **Administrators** to send these alerts to all administrator emails that are configured to receive alerts. Check **Recipient(s)** to send alerts to the internal users who sent the emails that contained the detected malware.

3 To view the default text for inbound or outbound detected malware alerts, or to create custom alert messages, click **Edit Alerts**.

4 In the **Detected Malware Alert Settings** dialog box, when **Default** is selected, you can view, but not edit, the default alert messages.

- To use the default messages, click **Cancel**.
- To customize an alert message, change **Default** to **Custom**. You can now edit the subject line and body text of the selected message or replace the text completely. You can also choose placeholders from the dropdown list to insert variables into the alert emails. These variables are replaced by data before the alerts are sent.

See “About placeholders in malware alerts” on page 12.

5 When you finish editing alerts, click **Save**.

6 At the bottom of the **Alert Settings** tab, click **Save**.

About placeholders in malware alerts

You can insert placeholders to add variables to custom blocked malware alerts or detected malware alerts. The placeholders enable you to provide useful information to Administrators or email recipients. Each placeholder is inserted as a percent character followed by a letter. The placeholder is replaced by the data that it represents before the alert is sent.

Table 2-2 describes the placeholder characters that appear in **Placeholder** menus when you configure custom alerts. Some placeholders are available only for certain types of alerts. Others are available only when the alert is configured for Administrators.

Table 2-2 Malware alert placeholders

Placeholder	Description
Date email was sent (%d)	Adds the date that the email was sent. Example: "The email was sent on %d"
Subject line (%t)	Adds the subject line of the email. Example: "An email that is sent to you with the following subject line was blocked: %t"
Plain text section of email body (%p)	Adds the plain text section of the email body. Example: "An email containing the following text has been blocked: %p" To protect confidentiality, this placeholder is not allowed in messages to administrators.
Suspect attachment filenames (%y)	Adds the file names of attachments that contain suspected malware. Example: "An email containing the following attachments has been blocked: %y"
Envelope senders (%e)	Adds the envelope sender of the email. This is the email address of the actual sender, which may be different from the sender that appears on the "From:" line in the email body. Example: "The sender address of the email was: %e"
Message body senders (%s)	Adds the message body senders, that is, the "reply to" address that appears in the email. Example: "The reply to address of the mail was: %s"
Sending server IP address (%S)	Adds the IP address of the server that sent the email. Example: "The sender's IP address was: %S"

Table 2-2 Malware alert placeholders *(continued)*

Placeholder	Description
Envelope recipients (%r)	Adds all recipients, including bcc recipients. Example: "The recipient address of the email was: %r" To protect confidentiality, this placeholder should not be inserted in recipient alerts. Administrators may need to know every recipient, including BCC recipients, to understand the extent of an attack and to determine which systems need remediation when malware is detected after delivery.
Message body recipients (%g)	Adds the recipients that are listed in the TO: and CC: lines of the email. Example: "A messages containing suspected malware was sent to %g."
Message-id (%i)	Adds the Message identification number of the email. Example: "Malware was detected in an email with the following Message ID: %m".
Mail server name (%m)	Adds the name of the mail server that handled the email. Example: "A message that later was found to contain malware was delivered by %m."
Message size (%a)	The size of the message, in KB. Example: "The message size is %a KB."
Max message size (%b)	The **Maximum Message Size** value that is configured on the **Services > Platform > Message Size** tab. Example: "The message exceeds the maximum message size of %b KB."
Rule that detected (%R)	Adds the name of the rule that triggered the detection. Example: "The email is out of compliance with the following rule: %R"

Table 2-2 Malware alert placeholders *(continued)*

Placeholder	Description
Reason text (%E)	Adds the reason text. Example: "The email was blocked for the following reason: %E"
Pen number (%q)	Adds the Pen number of the email. Administrators can enter the Pen number into the **Search** field on the **Malware Release** tab to find and release a quarantined message. Example: "A message that contains suspected malware has been quarantined. If you think that this was done in error, use this number to release the message from quarantine: %q."
Name of virus scanner (%n)	Adds the name of the virus scanner that detected the malware. Example: "An email message that contains suspected malware was detected by Scanner %n".
Output from scanner (%v)	Adds the malware information that is provided by the scanner. Example: ""xyz/99 was detected in file abd.c"
Insert an actual % (%%)	Adds a double % to insert a percent character in the alert message. Example: "To be 100%% certain that blocked malware does not infect your system, do not release email messages from quarantine."

See “Configuring blocked malware alerts” on page 10.

See “Configuring detected malware alerts” on page 11.

Releasing a quarantined email

When Anti-Malware intercepts an infected email, the service stores the email in quarantine, rather than delivering it to the intended recipients. The infected email is stored for up to 30 days before it is deleted. This quarantine period ensures that the malware is isolated and cannot infect the intended recipient’s computer.

Each quarantined email has a unique identifier, which is known as a Pen number. This number is stated in the administrator alerts and recipient alerts that are issued when an email is quarantined.

Note: The Pen number also appears on the **Incident Details** page when the Advanced Threat Protection service is available.

An Administrator can allow an infected email to be released from quarantine and delivered to the intended recipient.

To release an email from quarantine

1. Select **Services** > **Email Services** > **Anti-Malware**.
2. On the **Malware Release** tab, enter the Pen number of the email message.
3. Click **Search**.

   A pop-up window displays details of the quarantined email.
4. Locate the required entry and, in the column to the right, click **Release**.

   A disclaimer displays.
5. Read the disclaimer and then click **Release**.

   The quarantined email is released to the intended recipient(s).