

# epati

## Antispam Configuration

Product: Antikor v2 - Next Generation Firewall  
Guides

# Antispam Configuration

In addition to Threshold Score and gray list settings, Antivirus Check, MX Check for SMTP FROM, SPF Check, DKIM Check, DMARC Check, Phishing Check are set here.

## Antispam Configuration

### Threshold Score Settings

Grey List Threshold Score [?](#)

Add Header Threshold Score [?](#)

Rewrite Subject Threshold Score [?](#)

Reject E-mail Threshold Score [?](#)

### Antivirus Check

☒ Active

White List [Reload](#) [Add](#)

#	Status	Source	Description	Transactions
1	Active	lan1	lan1	<a href="#">Edit</a> <a href="#">Delete</a>

[«](#) [<](#) [1](#) [>](#) [»](#)

### MX Check for SMTP FROM

☒ Active

White List [Reload](#) [Add](#)

#	Status	Domain	Description	Transactions
1	Active	domain.tld	domain.tld	<a href="#">Edit</a> <a href="#">Delete</a>

[«](#) [<](#) [1](#) [>](#) [»](#)

### SPF Check

☒ Active

White List [Reload](#) [Add](#)

#	Status	Domain	Description	Transactions
1	Active	domain.tld	domain.tld	<a href="#">Edit</a> <a href="#">Delete</a>

[«](#) [<](#) [1](#) [>](#) [»](#)

## Threshold Score Settings

**Antispam Rules Transaction: “Score”**, it gets minus or plus points according to the specified transaction.

If the rule does not work, the determined score increases. If the specified threshold scores (grey list threshold score, spam header addition threshold score, email subject change threshold score, and definitive spam - rejection threshold score) are exceeded, they are blocked.

Set Action (Reject, Quarantine, Ignore) setting is available for Spam Emails.

## Antivirus Check

It performs antivirus checks on e-mails, except for the sources in the white list. Your trusted sources that you do not want to be checked by antivirus should be whitelisted.

## MX Control for SMTP FROM

It provides MX control for incoming e-mails, thus checking whether the source of the e-mail address is reliable. Trusted domains should be whitelisted.

## SPF control

SPF (Sender Policy Framework) Control is the name given to the records in the DNS records of the domain name that indicate from which IP addresses that domain name sends e-mail. In sending e-mails, it can also be called “authentication (check)” for the sender. Trusted domains should be added to the SPF Control - Whitelist.

Antispam categories can be added from predefined categories as allowed and disabled.

DKIM Check

Active

White List

Refresh

Add

#	Status	Domain	Description	Transactions
1	Active	domain.tld	domain.tld	<div>Edit</div> <div>Delete</div>

< 1 >

DMARC Check

Active

White List

Refresh

Add

#	Status	Domain	Description	Transactions
1	Active	domain.tld	domain.tld	<div>Edit</div> <div>Delete</div>

< 1 >

Grey List Settings

Pause

White List

Refresh

Add

#	Status	Domain	Description	Transactions
1	Active	domain.tld	domain.tld	<div>Edit</div> <div>Delete</div>

< 1 >

Phishing Check

Active

Antispam Categories Management

Edit

Allowed Categories

Haber - Predefined

Blocked Categories

Virus Bulasmig - Predefined

Kimlik An - Predefined

## DKIM Control

DKIM (DomainKeys Identified Mail) Check is an email verification form that adds digital cryptographic signatures to email messages. If a DKIM check is to be made, trusted domains must be added to the white list.

## DMARC Control

DMARC (Domain-Based Message Authentication, Reporting & Conformance) controls how the recipient's email server should handle incoming emails when the sender's address is not defined. When DMARC Check is done, trusted domain names must be added to the white list.

## Gray List Settings

When the graylist settings are active, SMTP will reject the requests the first time because the actual SMTP requests will continue for as long as the sending failed, so it is clear that the SMTP request is not an attack. Trusted domains need to be whitelisted.

## Phishing Control

It controls phishing attacks to be made to e-mail accounts. For e-mail security, Antikor users should activate this feature.

## Antispam Categories Management

Predefined or specified categories can be added here as allowed and disabled. Users are provided with e-mail filtering on a category basis.

**Important Note:** It is recommended that Antikor users activate and use all the settings in Antispam.

ePati Cyber Security Technologies Inc.  
Mersin Universitesi Ciftlikkoy Kampusu  
Teknopark Idari Binasi Kat: 4 No: 411  
Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

[www.epati.com.tr](http://www.epati.com.tr)  
[info@epati.com.tr](mailto:info@epati.com.tr)  
+90 324 361 02 33  
+90 324 361 02 39

