

Anti-Spam

- [Anti-Spam configuratie door Dustin](#)
- [Anti-Spam Whitelist/Blacklist aanpassen als gebruiker](#)
- [Anti-Spam zelf configureren](#)

Anti-Spam configuratie door Dustin

De servicedesk van Dustin kan voor u de configuratie van het spamfilter inregelen. Hieronder kunt u lezen welke informatie wij van u nodig hebben om dit snel en succesvol uit te kunnen voeren. De servicedesk van Dustin past standaard geen zaken in uw IT-omgeving aan. Desgewenst kan dit alsnog door ons worden uitgevoerd op nacalculatie.

Hetgeen wat u zelf nog zal moeten configureren/wijzigen

- Ten behoeve van de synchronisatie tussen uw Active-Directory en onze spamfilter, dient er een serviceaccount beschikbaar te zijn met leesrechten tot de gebruikers account in Active-Directory.
- LDAPS-verkeer dient te worden toegestaan op de firewall. (Poort 636)
- Uw relay connector / smart host configuratie dient te worden aangepast zodat uw email via onze spamfilter zal worden uitgestuurd. De gegevens om het SPF-record en de relay connector / smart host te configureren zult u ook van ons ontvangen.

Wat doet Dustin voor u?

- De betreffende domeinnamen plaatsen in het spamfilter.
- Verdere domeinconfiguratie wordt ingesteld.
- Met onze ondersteuning worden voor uw domein(en) uw zogenaamde MX en SPF-records aangepast.
- Wij maken een beheerdersaccount aan waarmee u uw eigen domein(en) in ons spamfilter kan beheren/configureren.

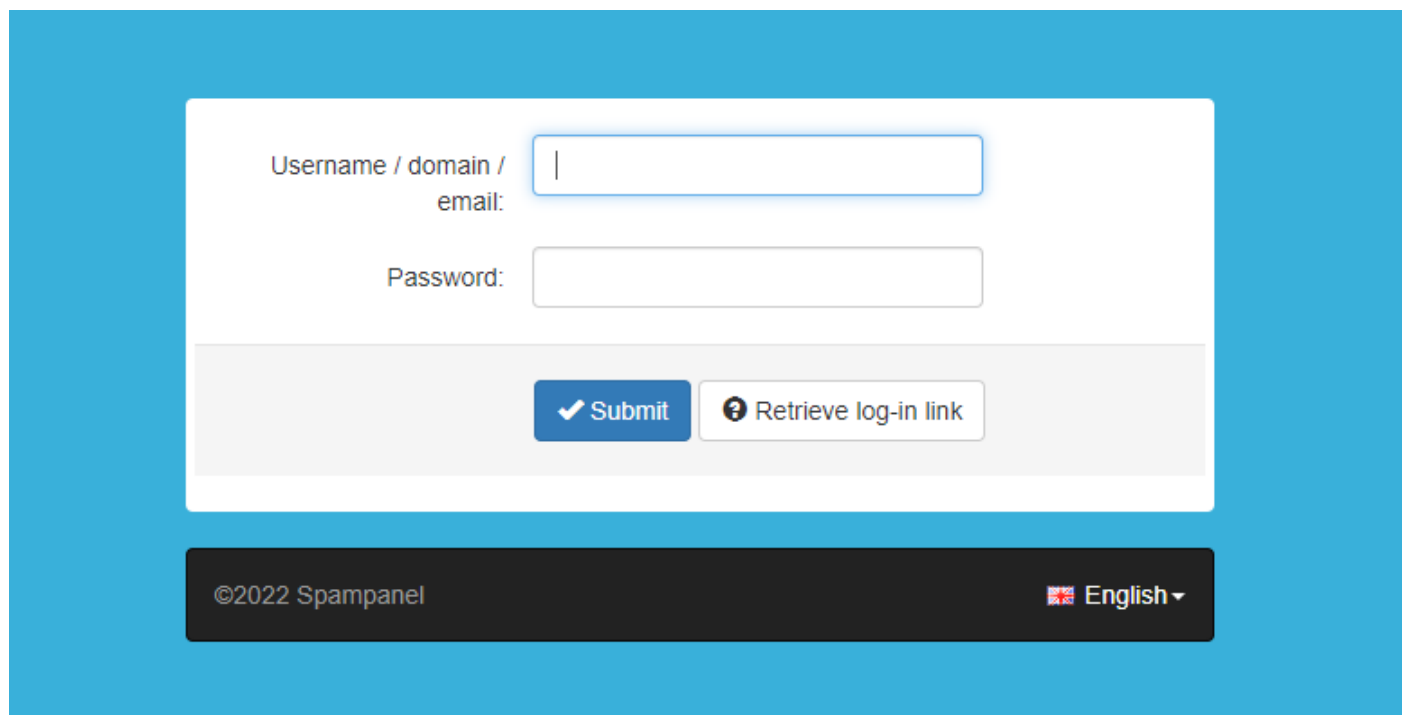
Welke Informatie hebben wij van u nodig?

- Distinguished Name (DN) van de LDAP-service account die **lees** toegang heeft tot alle gebruikersinformatie.
- De betreffende domeinnamen waarvoor u onze dienst wilt gebruiken.
- Het IP-adres waarop u uw e-mail ontvangt.
- Het IP-adres waarvan u uw e-mail verzend richting onze spamfilter.
- De inloggegevens van uw domein hosting partij, zodat wij de DNS-instellingen kunnen aanpassen.

Indien u deze gegevens aan ons hebt toegezonden, zullen wij dit verwerken en ontvangt u van ons uw beheerders account.

Anti-Spam Whitelist/Blacklist aanpassen als gebruiker

Log in op het spamfilter via: <https://master.antispamcloud.com>

The image shows a login interface for an anti-spam system. It features a white login box centered on a blue background. The box contains two input fields: 'Username / domain / email:' and 'Password:'. Below these fields are two buttons: a blue 'Submit' button with a checkmark icon and a white 'Retrieve log-in link' button with a question mark icon. At the bottom of the interface, there is a black footer bar containing the copyright notice '©2022 Spampanel' on the left and a language selector 'English' with a dropdown arrow on the right.

Username / domain / email:

Password:

©2022 Spampanel English ▾

Klik op de tab **Protection -> Sender allow list -incoming**.

U kunt nu hier uw persoonlijke **whitelist/blacklist** door op Add sender to allow list toevoegen en het gewenste adres in te voeren en op **save**

Logged in as [redacted] Email User

Dashboard

Reporting

Email Scout Reports - incoming

Email Scout Reports - outgoing

Protection report

Incoming

Train messages

Protection

Logs - incoming

Logs - outgoing

Delivery issue log - incoming

Sender allow list - incoming

Sender block list - incoming

Spam quarantine

Sender allow list [redacted]

If you wish to receive mail from a particular sender regardless of the message content, you should add it to the allow list.

- You have the option to check only the "envelope" sender, the sender address that is in the "From" header.
- To add all addresses at a domain to the allow list, add the domain name without a leading "@" (e.g. for .nl, add nl).
- To add an entire top-level domain to the allow list, use *** as a wildcard (e.g. for anything from .nl, add ***.nl).

+ Add sender to allow list Import senders from CSV Export senders as CSV

Query Rules

Address contains

+ New rule

Group results by:

Choose column

No results found

Add sender to allow list

Sender Flag

Apply to Envelope Sender Apply to From: Address Apply to both

Address *

Cancel Save

Dit zelfde geldt voor het blokkeren. Hier kunt u voor te recht bij Protection -> sender block list - incoming

Anti-Spam zelf configureren

Het is uiteraard ook mogelijk om zelf de gehele configuratie uit te voeren. Hieronder kunt u de informatie vinden om dit snel en succesvol uit te kunnen voeren.

Hetgeen wat u zelf kunt configureren/wijzigen

- Ten behoeve van de synchronisatie tussen uw Active-Directory en onze spamfilter, dient er een serviceaccount beschikbaar te zijn met leesrechten tot de gebruikers account in Active-Directory.
- LDAPS-verkeer dient te worden toegestaan op de firewall. (Poort 636)
- Uw relay connector / smart host configuratie dient te worden aangepast zodat uw email via onze spamfilter zal worden uitgestuurd. De gegevens om het SPF-record en de relay connector / smart host te configureren zult u ook van ons ontvangen.
- Het aanpassen van uw zogenaamde MX-records zodat het e-mailverkeer voor de betreffende domeinen via onze spamfilter wordt verstuurd.
- U kunt uw SPF-record aanpassen zodat wij in de DNS kunnen registreren namens welke server of IP-adressen e-mails verstuurd mogen worden vanaf een bepaald domein.
- Het configureren van uw domein(en) in onze spamfilter zoals de IP-configuratie, Single Sign-on en LDAP-configuratie.

Wat doet Dustin voor u?

- De betreffende domeinnamen plaatsen in het spamfilter.
- Wij maken een beheerdersaccount aan waarmee u uw eigen domein(en) in onze spamfilter kan beheren/configureren.

Welke Informatie hebben wij van u nodig?

- De betreffende domeinnamen waarvoor u onze dienst wilt gebruiken.
- Het IP-adres waarvan u uw e-mail verzend richting onze spamfilter.

Indien u deze gegevens aan ons hebt toegezonden, zullen wij dit verwerken en ontvangt u van ons uw beheerders account met daarbij de benodigde gegevens om de configuratie zelf uit te kunnen voeren.