

Antispam API



OXILION

INTERNET. OBVIOUS!

www.oxilion.nl

Dit document beschrijft de werking van de Antispam API van Oxilion. In dit document wordt eveneens beschreven hoe de webinterface in gebruik kan worden genomen.

Bedrijf: Oxilion B.V.
Auteur: Dennis Wijnberg - d.wijnberg@oxilion.nl
Versie: 0.2
API versie: 1.2

Inleiding

De API voor de antispam dienst van Oxilion is primair gericht op integratie van de antispam diensten in de bestaande configuratie van de klant. Met de API kunt u alle veelvoorkomende zaken automatiseren en de user interface aanpassen aan uw eigen wensen. Uw klanten zien dus nooit dat u onderliggend gebruik maakt van onze oplossing.

Bij de API wordt een user interface geleverd die dient als hulpmiddel om een eigen layout aan te koppelen of om direct te implementeren. Deze userinterface is volledig open source. De licentie waaronder deze code valt is GNU GPLv3. Uitbreidingen zijn daarom ook meer dan welkom. Meer informatie over de userinterface is verderop in dit document te vinden.

De applicatie wordt door de community onderhouden en wordt “as-it-is” geleverd door Oxilion.

Inhoudsopgave

Contents

Functieoverzicht van de API	3
Communicatie met de API.....	5
Vereisten	5
Authenticatie.....	5
Installatie.....	6
Authenticatie.....	6
MySQL configuratie	6
Koppeling met uw bestaande database.....	6
Aanpassen aan huisstijl	8

Funcctieoverzicht van de API

De API is gebouwd op basis van SOAP. Er is een WSDL document waaruit de functionaliteit is te distilleren. Dit document beschrijft de API-versie zoals aangegeven op het voorblad. De functionaliteit is gemakshalve in onderstaande tabel uitgewerkt.

Method	Argumenten	Response
addDomain	Domain String Server String Doelserver Port Integer SMTP poortnummer Voegt een domeinnaam toe aan het antispamcluster. De e-mail wordt afgeleverd op het poortnummer van de bij Server aangegeven hostname of IP.	Boolean
addWBEmail	From String [iets@]domein.nl To String [iets@]domein.nl List String w of b Voegt een domeinnaam of emailadres toe aan de white- of blacklist van een gebruiker	Boolean
configureDelivery	Domain String Server String Doelserver Port Integer SMTP poortnummer Wijzig de afleverinstellingen van een domein.	Boolean
configureDomain	Domain String Spam Boolean BadHeader Boolean Virus Boolean BadFile Boolean Bepaalt de instellingen voor een domeinnaam. Per onderdeel kan de scanning worden ingeschakeld of uitgeschakeld.	Boolean
getAddresses	Domain String Geeft alle adressen terug waarvoor de laatste 30 dagen e-mail is ontvangen binnen de domeinnaam.	Array
getDomains	Geen argumenten. Geeft een array met domeinen terug waarop deze account rechten heeft.	Array
getWBList	Account String [iets@]domein.nl	Array(from String to String wb String)

Method	Argumenten	Respons
getQuarantaine	Account String [iets@]domein.nl Geeft een array terug met alle spam voor deze account van de afgelopen 30 dagen. Let op! Een account kan een e-mailadres of een domeinnaam zijn.	Array (from String to String subject String type String time String smtp_resp String spam_level String mail_id String secret_id String)
releaseMail	mail_id String Uniek ID secret_id String Beveiligingswaarde To String Afleveradres Levert een tegengehouden e-mail alsnog af. Let op! Bij het releasen wordt de e-mail niet verwijderd.	Boolean
deleteMail	mail_id String Uniek ID secret_id String Beveiligingswaarde To String Afleveradres Verwijdert een tegengehouden e-mail expliciet uit de antispam. Expliciet verwijderen is geen verplichting. Een bericht wordt na 30 dagen automatisch verwijderd.	Boolean
removeDomain	Domain String Verwijdert een domeinnaam uit de antispam. Zorg ervoor dat de MX-records al zijn aangepast en de TTL verlopen voordat u een domein verwijderd.	Boolean
removeWBEmail	From String To String Verwijdert een domein of emailadres voor een bepaalde user uit de white of blacklist.	Boolean

Communicatie met de API

De communicatie met onze API gaat op basis van een WSDL document. In deze WSDL staat de volledige webservice beschreven.

Vereisten

Om gebruik te kunnen maken van onze API hebben wij een voorbeeld meegeleverd. Ondanks dat er vanuit elke programmeertaal een verbinding kan worden gemaakt met de webservice, is ons voorbeeld uitgewerkt in PHP. Vereist/Gewenst hiervoor is:

- PHP 5.x Getest met 5.2.10
 - with-openssl
 - with-mysqli (Alleen voor de userinterface)
 - enable-sockets
 - enable-soap

- jQuery UI > 1.7 Getest met 1.7.2, meegeleverd, (Alleen voor de userinterface)

Authenticatie

Op basis van het Oxilion klantnummer en wachtwoord kan de cliëntapplicatie (zoals meegeleverde code) de verbinding opzetten met onze API. Op basis hiervan dient u een authenticatieheader mee te sturen. In het vereenvoudigde voorbeeld ziet u snel hoe u dit kunt doen.

Installatie

Om gebruik te maken van de meegeleverde user interface moet het configuratiebestand worden aangepast. Dit bestand heet *config.php* en is te vinden in de root van de applicatie.

Dit bestand dient aan te worden gepast aan de gewenste configuratie voor een soepele integratie met het bestaande systeem.

Configuratie-item	Mogelijkheden									
Authenticatie										
USER	Het mijn.oxilion.nl klantnummer									
PASS	Het mijn.oxilion.nl wachtwoord									
MySQL configuratie										
DB_HOST	De MySQL databaseserver. De server moet verbindingen accepteren voor DB_USER/DB_PASS vanaf het IP-adres waar de applicatie draait.									
DB_USER	De MySQL gebruikersnaam.									
DB_PASS	Het MySQL wachtwoord voor DB_USER.									
DB_NAME	De MySQL databasenaam.									
Koppeling met uw bestaande database										
USER_TABLE	De tabel waar de cliëntapplicatie de gebruikersgegevens vandaan moet halen.									
USER_USERFIELD	De veldnaam van de "gebruikersnamen". Dit kan een klantnummer, gebruikersnaam, e-mailadres enz. zijn uit de bestaande administratie c.q. website.									
USER_PASSFIELD	De veldnaam van het "wachtwoord".									
ACCOUNT_TABLE	De tabel waar de rechten op domeinen/accounts worden bepaald. Deze tabel moet ten minste de velden: userId, domain en address hebben. Waarbij de waarden van userId een verwijzing zijn naar USER_USERFIELD. Om een gebruiker toegang te geven tot een hele domeinnaam dient domain ingevuld te worden (example.com) en address leeg te zijn. Om een gebruiker toegang te geven tot slechts één account of slechts een deel van de accounts, moet er per e-mailadres een record bestaan waar de domain is ingevuld (example.com) en bij address het corresponderende adres. Voorbeeldpopulatie: Tabel: gebruikers <table><thead><tr><th>klantnr</th><th>naam</th><th>wachtwoord</th></tr></thead><tbody><tr><td>1</td><td>Tess Bakker</td><td>g9pxH^f</td></tr><tr><td>2</td><td>Maura Jansen</td><td>d9nk*dM</td></tr></tbody></table>	klantnr	naam	wachtwoord	1	Tess Bakker	g9pxH^f	2	Maura Jansen	d9nk*dM
klantnr	naam	wachtwoord								
1	Tess Bakker	g9pxH^f								
2	Maura Jansen	d9nk*dM								

	<p><i>(Zie volgende pagina)</i></p> <p>Tabel: accounts</p> <table border="1"> <thead> <tr> <th>userId</th> <th>domain</th> <th>address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>example.com</td> <td>tess@example.com</td> </tr> <tr> <td>1</td> <td>example.com</td> <td>suse@example.com</td> </tr> <tr> <td>1</td> <td>another.org</td> <td></td> </tr> <tr> <td>2</td> <td>another.org</td> <td>maura@another.org</td> </tr> </tbody> </table> <p>Tess Bakker heeft dus rechten op tess@example.com, suse@example.com en alles binnen de domeinnaam another.org. Maura Jansen heeft alleen recht op maura@another.org</p>	userId	domain	address	1	example.com	tess@example.com	1	example.com	suse@example.com	1	another.org		2	another.org	maura@another.org
userId	domain	address														
1	example.com	tess@example.com														
1	example.com	suse@example.com														
1	another.org															
2	another.org	maura@another.org														
ABSOLUTE_URL	De absolute URL, met eindslash, waar de applicatie zich bevindt.															
LIVE	Bepaalt of er code-foutmeldingen worden getoond aan de gebruiker.															
	Mogelijke waarden: true/false Let op! Geen aanhalingstekens.															

Aanpassen aan huisstijl

Om de applicatie aan de gewenste huisstijl aan te kunnen passen staat de PHP-code los van de HTML en is er gebruik gemaakt van templates. Deze staan hieronder uitgelegd.

index.htm	<p>Overkoepelende template waarin de achtergrond, de title en de verwijzingen naar CSS en javascript staan opgenomen.</p> <p>Placeholders: {MAIN} Wordt altijd vervangen door de inhoud van home.htm (ingelogd) of login.htm (niet ingelogd).</p>
home.htm	<p>De template waar de lijst met domeinnamen in komt te staan.</p> <p>Placeholders: {ACCESS} Wordt vervangen door een aantal iteraties van de home_access_line.htm template.</p>
login.htm	<p>In deze template staat het inlogscherf.</p>
home_access_line.htm	<p>Deze template wordt gebruikt voor elke domeinnaam waarin de ingelogde gebruiker rechten heeft.</p> <p>Placeholders: {DOMAIN} De betreffende domeinnaam. {AANTAL} Het aantal e-mailadressen dat bekend is voor deze domeinnaam. {USERS} Wordt voor elke e-mailadres een keer vervangen door home_access_spam_line.htm.</p>
home_access_spam_line.htm	<p>Dit zijn de uiteindelijke regels met spam die je ziet.</p> <p>Placeholders: {FROM} Waar de e-mail vandaan komt. {SUBJECT} Onderwerp van de e-mail. {TYPE} Waarom de e-mail is tegengehouden. {TIME} Wanneer de e-mail is verstuurd. {ADDRESS} Het betreffende e-mailadres {ID} Het unieke mail_id {KEY} De sleutel bij mail_id genaamd secret_id</p>
home_access_spam.htm	<p>De kop voor elk e-mailadres met spam.</p> <p>Placeholders: {ADDRESS} Het betreffende e-mailadres. {LINES} Voor iedere spam e-mail de inhoud van home_access_spam_line.htm.</p>
home_access_nospam.html	<p>De koptekst voor elk e-mailadres zonder spam.</p> <p>Placeholder: {ADDRESS} Het betreffende e-mailadres.</p>
respons.htm	<p>De info/foutmeldingen die vanuit de applicatie komen.</p> <p>Placeholder: {RESULT} Het resultaat. Mogelijke waarden: info/error. {MSG} Het daadwerkelijke bericht.</p>