

CONSALUD S.A.

Reporte Herramienta “mailcleaner”

Francisco Abarca

17/01/2019

Reporte descriptivo sobre el funcionamiento, estado y posibles configuraciones de la herramienta “mailcleaner”, la cual monitorea el estado del servicio de correo y su seguridad.

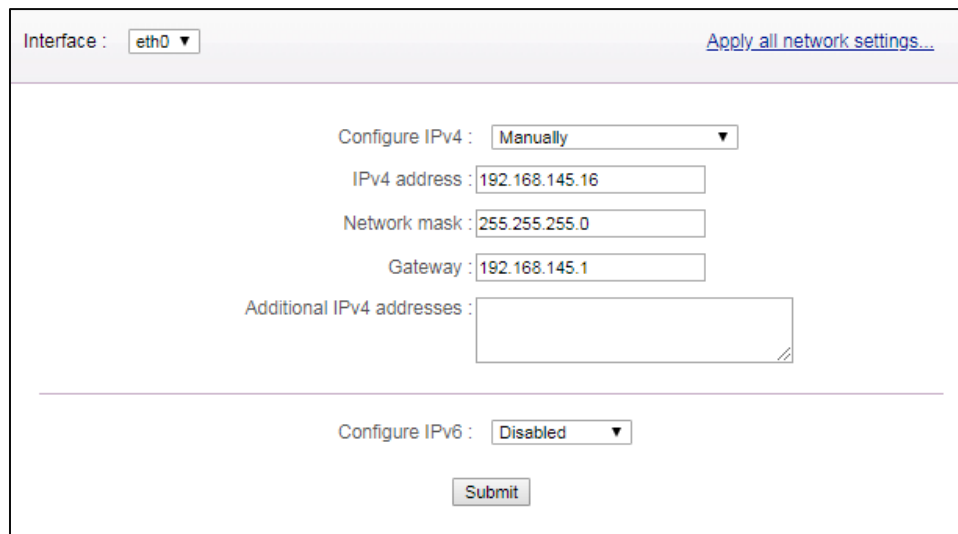
Contenido

Sistema Base	3
Ajuste de Redes.....	3
Ajustes de DNS	3
Localización	4
Hora y Fecha.....	4
Proxies	5
Registro	5
Ajustes Generales.....	6
Predeterminados.....	6
Compañía	6
Cuarentenas	7
Tareas Periódicas	7
Logging del Sistema.....	8
Archivado	8
Dominios	9
SMTP (Simple Mail Transfer Protocol)	10
SMTP Checks	10
Control de Conexiones	11
Control de Recursos	12
TLS (Transport Security Layer)/SSL (Secure Socket Layer)	13
Greylisting (Lista gris)	14
DKIM (DomainKeys Identified Mail)	14
Anti-Spam.....	15
Ajustes Globales	15
Módulos Anti-Spam.....	16
TrustedSources.....	16
Spamc	17
PreRBLs.....	18
NiceBayes	19
UriRBLs	19

Configuración

Ajuste de Redes

Menú en el cual, mediante la selección de una interfaz (red o inalámbrica), es posible configurar su IPv4, tanto manual o seleccionar su configuración automática, en caso de configuración manual tenemos la dirección, la máscara de red, la puerta de enlace (gateway) y direcciones adicionales en caso de ser necesario. Además, tenemos la posibilidad de configurar el IPv6.



Interface : eth0 ▼ [Apply all network settings...](#)

Configure IPv4 : Manually ▼

IPv4 address :

Network mask :

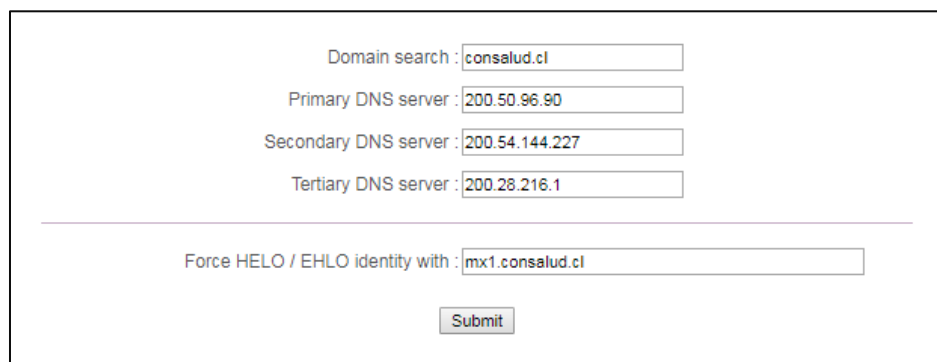
Gateway :

Additional IPv4 addresses :

Configure IPv6 : Disabled ▼

Ajustes de DNS

En este menú, tenemos la búsqueda del DNS (registro A), y la definición del DNS primario, secundario y terciario. La identidad con la cual se identifica puede ser forzada e ingresada manualmente.



Domain search :

Primary DNS server :

Secondary DNS server :

Tertiary DNS server :

Force HELO / EHLO identity with :

Localización

Acá configuramos la zona del sistema con dos filtros, Continente y ciudad más cercana.

Continent :

Nearest city :

Submit

current local time is : Jan 17, 2019 12:34:28 PM ([set up...](#))

Hora y Fecha

Sección en la cual podemos proveer un servidor NTP del cual obtendremos nuestros datos horarios, o bien hacerlo de manera manual.

Setup time and date automatically :

Use time server : ☒

NTP server :

Save and sync now

Setup time and date manually :

Date :

Time : : :

↺

Set time and date

current local zone is : America - Santiago ([set up...](#))

Proxies

Esta pestaña posibilita la opción de configurar un proxy, tanto para el protocolo HTTP como para el protocolo de los mensajes (SMTP).

HTTP proxy :

SMTP proxy :

Registro

Sección en donde podemos verificar el estado de registro del sistema, y en caso de vencimiento o fin del término de la licencia renovarla.

Reseller ID :

Reseller password :

Client ID :

System is **registered**

Ajustes Generales

Predeterminados

En esta sección podemos elegir opciones tales como, el idioma de la interfaz, el dominio por defecto, la dirección de correo para el soporte como el sistema, además de las direcciones para la notificación de falsos positivos o negativos.

User GUI language : English ▼

Default domain : consalud.cl ▼

Display domain selector : ☒

Support address :

System mail sender address :

False negative reporting address :

False positive reporting address :

Compañía

Lugar en donde van las configuraciones sobre el nombre de la compañía, nombre de contacto y dirección de correo del contacto.

Company name :

Contact name :

Contact email address :

Cuarentenas

Acá están las opciones de tiempo que mantendrán la existencia de archivos en cuarentena para su posterior eliminación y/o examinación. Hay dos tipos de retenciones que se pueden configurar, retención de spam (en días), y tiempo de retención de contenido peligroso, en días también.

Spam retention time :

Dangerous content retention time :

Tareas Periódicas

En este menú están las configuraciones para las tareas programadas, las cuales se dividen en diarias, semanales y mensuales. Para cada una hay que elegir una hora, un día de la semana y un día del mes respectivamente.

Daily tasks run at :

Weekly tasks run on :

Monthly tasks run at day :

Logging del Sistema

En esta pestaña podemos habilitar un log del sistema (syslog) con su respectivo server para recopilar información.

Use syslog logging : ☐

Syslog server :

Submit

Archivado

Tenemos la opción de habilitar un archivado externo el cual es configurable al seleccionarlo en donde debemos proveer un servidor objetivo.

Archiving mode :

Submit

Dominios

Acá podemos configurar las opciones globales de nuestros dominios, como los correos del administrador, en caso de falla o falsos negativos/positivos y el encargado de soporte.

En esta ventana también podemos revisar los dominios ya configurados y añadir nuevos, ya sean con las variables definidas anteriormente (ajustes de dominio globales) o alguno en particular de los que ya tenemos.

Domain default settings

General ▾ [Next step >>](#)

System mail sender address :

False negative reporting address :

False positive reporting address :

Support name :

Support email :

Domain default settings

New domain ➕

Domain specific settings

Domain search

Results: 3

consalud.cl

consalud.net

iconsalud.cl

Domain name :

Use default values from:

consalud.cl

General ▾ [Next step >>](#)

Aliases :

System mail sender address :

False negative reporting address :

False positive reporting address :

Support name :

Support email :

SMTP (Simple Mail Transfer Protocol)

SMTP Checks

Dentro de esta pestaña podemos controlar el funcionamiento del protocolo de transferencia de los correos, ya sea verificando el dominio, forzando la sincronización del protocolo, hacer timeout a la verificación del recipiente, filtrar DNS con una o varias bases de datos a seleccionar, hacer una lista blanca sobre hosts, modificar el timeout para la verificación con la base de datos, entre otras opciones.

Verify sender domain : ☐

Force SMTP protocol synchronisation : ☒

Recipient verification timeout : seconds [Clear cache now...](#)

Allow hosts with MX that point to IP addresses : ☐

Reject wrong SPF (fail result) : ☐

Reject invalid reverse DNS : ☐

Honor DMARC reject policy : ☐

Check connecting hosts against RBLs : ☒

bl.spamcop.net

☐ dnsbl-3.uceprotect.net

☐ ips.backscatterer.org

☐ ix.dnsbl.manitu.net

☐ sip-inv.mailcleaner.net

☐ iprbl.mailcleaner.net

☐ b.barracudacentral.org

☐ dnsbl.sorbs.net

☐ zen.spamhaus.org

☐ dnsbl-2.uceprotect.net

☒ dnsbl-1.uceprotect.net

☐ sip24-inv.mailcleaner.net

Don't check these hosts :

200.100.0.0/24

190.96.85.163

clinicalosandes.cl

x-data.cl

sendgrid.net

RBL checks timeout : seconds

Scan relayed (outgoing) messages for viruses : ☒

Mask IP address of relayed host on port 587 : ☐

Masquerade relayed HELO with sender domain : ☐

Enable reporting to DMARC domains : ☐

Submit

Control de Conexiones

Desde acá tenemos las opciones delimitar a quién aceptamos/rechazamos dentro del protocolo sea por IP como por dominio/direcciones, también tenemos la opción de bloquear ciertos destinatarios.

Allow connection from hosts : *

Allow external relaying for these hosts :

172.20.2.214
172.20.10.55
172.20.10.164
172.20.10.162

Allow relaying from unknown domains : ☒

Reject relaying to these external domains :

Reject connection from these hosts :

85.0.136.243

Reject these senders addresses :

*@onemail.cl
*@googlegroups.com
*@melter.com.mx
*@iqelite.com
*@sybil.com.mx

Reject these authenticated users :

Reject these recipient addresses :

Submit

Control de Recursos

En esta sección determinamos cuantos recursos se entregan, pudiendo limitar la cantidad de conexiones simultáneas, la máxima cantidad de mensajes por conexión, negar conexiones si estas superan cierta carga, el tamaño máximo por mensaje, cada cuanto son los reintentos de envío y límites por host.

SMTP session timeout : seconds

Maximum simultaneous connections :

overall :
per external host :
per trusted host :
Maxium messages per connection :

Reserved connections for relaying hosts :
Refuse untrusted connections if load is higher than :
Global maximum message size : KB
Add Reply-To address to error messages :

Sending retries : every up to

Enable per host rate limit : ☐

Enable per trusted host rate limit : ☐

Submit

TLS (Transport Security Layer)/SSL (Secure Socket Layer)

Acá podemos habilitar las opciones sobre los certificados e ingresar las claves correspondientes.

Enable SSL/TLS : ☒

Forbid unencrypted SMTP authentication : ☐

Enable obsolete SMTPS port 465 : ☐

Encoded SSL certificate :
-----BEGIN CERTIFICATE-----
MIIDNzCCAqCgAwIBAgIJAiz+d3IfXnn8MA0GC SqGS1b3DQ
EBBAUAMHExCzAJBgNV
BAYTAkNIMQ0wCwYDVQQIEWRXYXVkmREwDwYDVQQH
EwhMYXVzYW5uZTEUMBIGA1UE
ChMLTWFFpbENsZWFuZlZlZDAsBgNVBAstC01haWxDbG
VhbmVYMRQwEgYDVQQDEwtt
✓ certificate is valid

Encoded SSL private key :
-----BEGIN RSA PRIVATE KEY-----
MIICXAlBAABgQCuxqlsCHei5Xd+PbPm9HEDSKALXd+nH
REYmtNR9db3fo7I9wRx
6UtSahX6Nc3JuEYDdu+2tzX+PeiharAO+O+ZQgpUaapj4Nk
LEh3Hdx3L46qt2y0y
hgURyFzSsQQBVQQhS/jsRkwqc/wai9DXTIJmzrhWzWZAKfD
NY8ExY5hyVQIDAQAB

Force encryption to these hosts :

Force encryption from these hosts :

Force encryption to these external domains :

Force encryption from these external domains :

Submit

Greylisting (Lista gris)

Esta sección nos habilita el uso de la lista gris dentro del sistema, la cual rechazará temporalmente cualquier correo desde un dominio/remitente el cual no reconozca, también tenemos un filtro para colocar dominios para que no entren en esta lista.

Allowed retry interval : between seconds and seconds

Records expiration : seconds

Avoid greylisting for these domains :

vtr.cl

winpack.cl

manantial.com

entelchile.net

colbun.cl

DKIM (DomainKeys Identified Mail)

DKIM, es un método de autenticación de correos destinado para detectar direcciones de remitentes falsificados, esto es muy útil contra el phishing. Aquí podemos generar y colocar las llaves necesarias para el método, así como el dominio del DKIM.

Default DKIM domain :

Default DKIM selector :

Default private key :

[Generate new private key...](#)

Domain, selector and/or private key are currently not set or not saved.

Ajustes Globales

Dentro de esta pestaña tenemos los ajustes generales sobre las herramientas anti-spam, tanto la configuración de la lista blanca, negra y la de avisos. También tenemos una pequeña sección al inicio con nuestras IP/Redes confiadas.

Nuestras listas son modificables y los elementos pueden ser retirados/deshabilitados/agregados a placer del administrador.

Trusted IPs/Networks :

Enable access to whitelists : ☒

Ignore whitelist in tag mode : ☐

☐ *@soprole.cl
soprole.cl

☐ *@transbank.cl
transbank.cl

☐ *@bancoestado.cl
bancoestado.cl

☐ *@sarrapropiedades.cl
sarrapropiedades.cl

☐ *@bauform.cl
bauform.cl

☐ *@fastmed.cl

Add an address to the white list

Address :

Comment :

< Add element

Disable, enable or removed address from the list

Enable/Disable selected elements

Remove selected elements

Enable access to warnlists : ☐

Enable access to blacklists : ☐

Submit

Módulos Anti-Spam

TrustedSources

Este módulo cuando está habilitado administra las listas blancas y añade filtros propios de bases de datos en el internet. También se pueden modificar las variables de tiempo que puede tomar y tamaño máximo del mensaje, además tenemos la opción de añadir servidores SMTP conocidos desde acá.

Enable module : ☒

Module is decisive : ☒

Position in filter chain : ▼

Maximum check time : seconds

Maximum message size : bytes

Enable all trusted path detection : ☒

Trust SPF validation on these domains :

Known good authenticated SMTP servers :

Authenticated SMTP servers search string :

Use these DNS lists : ☒ iprwl.mailcleaner.net (IP addresses whitelist)
☐ list.dnswl.org (IP addresses whitelist)
☒ trustedspf.mailcleaner.net. (Domains with good SPF)
☒ list.eduwhitelist.net (IP addresses whitelist)

Submit

Spamc

Este módulo es similar al anterior pero enfocado al spam, en donde filtra mediante bases de datos DNSBL (Domain Name System-based Blackhole List) o RBL (Real-time Blackhole List), enfocadas a DNS o URI (Uniform Resource Identifier).

Enable module : ☒

Module is decisive : ☒

Position in filter chain :

Maximum check time : seconds

Maximum message size : bytes

Use statistical filter : ☒

Enable text recognition in images : ☒

Enable image format/size detection : ☒

Enable PDF format detection : ☒

Enable botnet detection : ☒

Honor DMARC quarantine policy : ☐

Enable RBLs controls : ☒ timeout : seconds

Using these DNS RBLs : ☒ bl.spamcop.net
☐ dnsbl-3.uceprotect.net
☐ ips.backscatterer.org
☐ ix.dnsbl.manitu.net
☒ iprwl.mailcleaner.net
☐ sip-inv.mailcleaner.net
☒ iprbl.mailcleaner.net
☒ list.dnswl.org
☒ b.barracudacentral.org
☒ list.eduwhitelist.net
☐ dnsbl.sorbs.net
☐ zen.spamhaus.org
☐ dnsbl-2.uceprotect.net
☐ dnsbl-1.uceprotect.net
☐ sip24-inv.mailcleaner.net

Using these URI RBLs : ☒ uribl.mailcleaner.net.
☐ dbl.spamhaus.org
☒ multi.uribl.com.
☐ uri-inv.mailcleaner.net.
☐ multi.surbl.org.

Enable DCC control : ☐ timeout : seconds

Enable Razor control : ☐ timeout : seconds

Enable Pyzor control : ☒ timeout : seconds

Enable SPF control : ☒ timeout : seconds

Enable DKIM control : ☒ timeout : seconds

PreRBLs

Módulo idéntico al anterior el cual genera un filtro más complementando al anterior sus opciones son similares, la función es idéntica pero el input de las RBL puede variar atrapando correos que pasaron el filtro anterior.

Enable module : ☒

Module is decisive : ☒

Position in filter chain : ▼

Maximum check time : seconds

Maximum message size : bytes

List hits to be spam : ▼

Using these RBLs : ☒ bl.spamcop.net
☐ dnsbl-3.uceprotect.net
☒ ips.backscatterer.org
☐ ix.dnsbl.manitu.net
☒ sip-inv.mailcleaner.net
☐ iprbl.mailcleaner.net
☐ b.barracudacentral.org
☐ dnsbl.sorbs.net
☒ zen.spamhaus.org
☐ dnsbl-2.uceprotect.net
☐ dnsbl-1.uceprotect.net
☒ sip24-inv.mailcleaner.net

Avoid checking for good SPF : ☐

Don't check these hosts :

Submit

NiceBayes

Este módulo se comunica con bases de datos con modelos estadísticos e información para identificar el spam de una manera más personalizada (la cual debe ser mantenida en base a reglas) similar a smapassasin.

Enable module :	<input checked="" type="checkbox"/>
Module is decisive :	<input checked="" type="checkbox"/>
Position in filter chain :	4 ▼
Maximum check time :	20 seconds
Maximum message size :	500000 bytes

Submit

UriRBLs

Con este módulo hacemos un filtrado mediante URI con las bases de datos seleccionadas, siempre cuando el filtro este habilitado, además de tener bases activas y/o elegidas.

Enable module :	<input checked="" type="checkbox"/>
Module is decisive :	<input checked="" type="checkbox"/>
Position in filter chain :	5 ▼
Maximum check time :	20 seconds
Maximum message size :	500000 bytes

URL hits to be spam :	1 ▼
Using these RBLs :	<input checked="" type="checkbox"/> uribl.mailcleaner.net.
	<input checked="" type="checkbox"/> dbi.spamhaus.org
	<input type="checkbox"/> multi.uribl.com.
	<input type="checkbox"/> uri-inv.mailcleaner.net.
	<input type="checkbox"/> multi.surbl.org.
Resolve URL shorteners :	<input checked="" type="checkbox"/>

Submit

ClamSpam

Este módulo filtra spam con reglas internas provistas por terceros, con las opciones de máximo tiempo de chequeo y máximo largo del mensaje.

Enable module : ☒

Module is decisive : ☒

Position in filter chain : ▼

Maximum check time : seconds

Maximum message size : bytes

Submit

Protección de Contenido

Ajustes Globales

En esta sección podemos configurar la cantidad de adjuntos máximos por mensaje, así como máximo tamaño por archivo adjunto, configuraciones sobre los adjuntos de forma TNEF (Transport Neutral Encapsulation Format), y la utilidad de notificar al administrador en caso de ocurrencias con los archivos adjuntos.

Maximum attachments per message :

Maximum attachment size : bytes ☒ no maximum size

Content control maximum archive depth : ☐ disable content controls in archives

Expand TNEF (winmail.dat) attachments : ☒

Still deliver bad TNEF attachments : ☒

Use decoded TNEF attachments :

Sent notice to administrator : ☒

Administrator address :

Anti-Virus

Acá podemos elegir el comportamiento del antivirus en caso hallar un archivo malicioso, si queremos que haga su trabajo silenciosamente en caso que el virus ya sea conocido y el tiempo que puede demorar el escáner.

Drop known viruses silently ☒

Anti-virus scanners timeout : seconds

Active scanners : ClamAV (daemon)

Control HTML

En este menú podemos elegir que funcionalidades de HTML habilitamos, bloqueamos o desarmamos y si genera un aviso al administrador/log.

IFrame objects :	<input type="text" value="block"/>	<input checked="" type="checkbox"/> silently
Formulars :	<input type="text" value="allow"/>	<input type="checkbox"/> silently
Scripts :	<input type="text" value="allow"/>	<input type="checkbox"/> silently
Codebase objects :	<input type="text" value="block"/>	<input type="checkbox"/> silently
Web Bugs :	<input type="text" value="disarm"/>	<input type="checkbox"/> silently
<input type="button" value="Submit"/>		

Control en el formato de los Mensajes

Similar al menú anterior pero con el enfoque de las funcionalidades y cualidades de los mensajes, según estas habilitamos o no los mensajes.

Maximum attachments per message :	<input type="text" value="200"/>
Maximum attachment size :	<input type="text" value=""/> bytes <input checked="" type="checkbox"/> no maximum size
Content control maximum archive depth :	<input type="text" value="5"/> <input type="checkbox"/> disable content controls in archives
<hr/>	
Expand TNEF (winmail.dat) attachments :	<input checked="" type="checkbox"/>
Still deliver bad TNEF attachments :	<input checked="" type="checkbox"/>
Use decoded TNEF attachments :	<input type="text" value="do nothing but checking content"/>
<hr/>	
Sent notice to administrator :	<input checked="" type="checkbox"/>
Administrator address :	<input type="text" value="juan.serrano@consalud.cl"/>
<input type="button" value="Submit"/>	

Nombre de Archivos Adjuntos

Dentro de esta sección podemos usar expresiones regulares para generar reglas, para filtrar ciertos nombres o extensiones de archivos que consideremos peligrosos.

The screenshot shows the 'Nombre de Archivos Adjuntos' (Filename Attachments) settings window. On the left, there is a list of filename expressions with checkboxes and warning icons:

- ☐ \ws[cfh]\$
Windows Script Host files are dangerous
- ☐ \xmk\$
Microsoft Exchange Shortcuts are dangerous
- ☐ \Z\$ (disabled)
- ☐ \zip\$ (disabled)
- ☐ \s{10,}
A long gap in a name is often used to bypass filters
- ☐ \{[a-hA-H0-9-]{25,}\}
Files containing CLSID's are trying to bypass filters
- ☐ {[a-hA-H0-9-]{25,}}

On the right, there are two panels:

- Add a filename expression to block**
Filename expression :
Comment :
< Add element
- Disable, enable or removed blocked filename**
Enable/Disable selected elements
Remove selected elements

Tipo de Archivos Adjuntos

Este menú es similar al anterior, pero la diferencia es que las reglas están predefinidas y solo se puede activar/desactivar, obteniendo un filtro por tipo de archivos más generalizado.

The screenshot shows the 'Tipo de Archivos Adjuntos' (File Type Attachments) settings window. On the left, there is a list of file types with checkboxes and warning icons:


- ☐ archive (not blocked)
- ☐ AVI (not blocked)
No AVI movies allowed
- ☐ ELF
No programs allowed
- ☐ EPS Binary File Postscript (not blocked)
.eps Postscript
- ☐ executable
No programs allowed
- ☐ MNG (not blocked)
No MNG movies allowed

On the right, there is a panel:


- Disable or enable file type blocking**
Enable/Disable selected elements

Accesos

Esta ventana recopila las opciones de acceso, crear usuarios nuevos para acceder a la herramienta y cambiar contraseñas.



Accesses : Administrators

New administrator 

Administrators specific settings
Administrator search


Results : 2
admin
mailcleaner-support

admin


Password :

Confirm :

Submit



Accesses : Administrators

New administrator 

Administrators specific settings
Administrator search

Results : 2
admin
mailcleaner-support

Administrator name :

Password :

Confirm :

Role : administrator ▼

Submit