

INTRODUCCION

Mailcfg es un panel de control para la gestión del servidor de correo mediante una interfaz html. El sistema permite acceso a mantenimiento-modificaciones desde tres niveles:

- Nivel de usuario. Cada titular de una cuenta de correo, puede cambiar los parametros de funcionamiento correspondientes a su cuenta. Precisa una contraseña de acceso que proveerá el administrador.
- Nivel de Administrador de dominio. Puesto que en un host puede haber multiples dominios, en la administración del correo se repite esta estructura.

El administrador de dominio, puede acceder a las configuraciones de usuario.

- Nivel de configurador del servidor. Algunos parámetros importantes que afectan al funcionamiento global del sistema de correo pueden gestionarse desde aquí. A este nivel, se tiene acceso a todas las opciones inferiores.

En su conjunto, este sistema de correo permite:

- Crear cuentas de correo pop3 e imap.
- Accesos mediante conexiones planas, SSL y STARTTLS.
- Establecimiento de contraseñas planas, o encriptadas (MD5 y NTLM)
- Redireccionamiento de cuentas
- Filtros de entrada mediante listas blancas y listas negras.
- Autoresponders, globales, o limitados a las listas blancas.
- Control del spam de salida mediante limitadores por hora / dia y més.
- Filtros de entrada opcionales para SPF, y varios servidores de listas negras (bl).
- Estadística de uso actualizada cada pocos minutos.

CUENTAS DE USUARIO

Para acceder al mantenimiento de una cuenta de usuario, la dirección url de acceso, será normalmente `http://mail.domain.tld` o `http://mail2.domain.tld`. Normalmente para acceder a esta opción precisará una contraseña de acceso web que será suministrada por el administrador.

Una vez dentro, debe indicar la cuenta de correo y la clave de acceso (de esas cuentas) para acceder a la configuración de usuario.

MANTENIMIENTO DE CUENTAS DE USUARIO

En esta pantalla podrá modificar la contraseña de acceso, la redirección de cuenta y un mensaje de autorespuesta.

Para modificar la contraseña esta debe ser introducida dos veces. La contraseña debe de tener al menos ocho dígitos.

Todo el correo destinado a esta cuenta podrá redireccionarse a otra del mismo dominio, o de otro otro dominio y servidor, introduciendo la dirección de destino deseada en la casilla "Redireccionar a".

Para generar un mensaje de autorespuesta, se puede cumplimentar la caja de texto disponible. Se recomienda utilizar esta opción solamente con listas blancas activadas, para evitar confirmaciones no deseadas de correo activo (Por ejemplo un spammer al recibir esta autorespuesta, tendrá la confirmación de que la cuenta se utiliza, y seguramente potenciará el spam a esta cuenta).

Cuando utilice esta opción debe de tener muy en cuenta los siguientes puntos.

- Si la lista blanca no está activa, la autorespuesta se dirigirá a todo correo recibido, con el reforzamiento del spam consecuente.

- Si la lista blanca está activa, solo los usuarios en esta lista recibirán la autorespuesta. Esta es la recomendación de uso normal.

- Las respuestas se gestionan por remitente y día. Esta es una forma de evitar el rebote inmediato, que si al otro lado existe otra autorespuesta, puede dar lugar al bloqueo del servidor por un loop sin fin. Esto quiere decir que como máximo se responde una vez al día al mismo remitente.

RESUMEN DE CONFIGURACION DE CUENTA DE USUARIO

Esta pantalla le permitirá consultar la configuración que debe poner en su ordenador o dispositivo móvil.

En general se recomienda utilizar una conexión segura bien sea STARTTLS o SSL. cuando se establece una conexión segura todos los datos se transmiten encriptados incluido la contraseña por lo que no es preciso utilizar contraseñas encriptadas en conexiones seguras, pero si compatible.

Muchos dispositivos móviles y algunos programas modernos como Outlook o Thunderbird, gestionan de forma inteligente la creación de una nueva cuenta. Esto es perfectamente válido y en general sencillo. No obstante en muchos casos si se quiere configurar una cuenta pop normalmente es necesario indicarlo manualmente.

Cuando dé de alta una cuenta que sólo se va a utilizar en un dispositivo puede usar el protocolo IMAP. Sin embargo compartir cuentas IMAP puede dar problemas con muchos programas cliente de correo. Si por el contrario quiere utilizar cuentas POP3 compartidas es muy importante que no quede marcada la casilla eliminar en el servidor cuando elimine el correo y marcar la casilla eliminar en el servidor al cabo de N días.

LISTAS BLANCAS Y NEGRAS

Aquí se configuran las listas blancas y negras. Cada lista puede estar completada pero estará desactivada si la casilla correspondiente así lo indica.

Las listas son un medio de filtrado del correo de entrada y se gestionan de la siguiente forma:

En primer lugar para cada correo entrante se comprueba si la dirección del remitente está en la lista negra. En caso afirmativo el correo entrante se ignora.

En caso contrario se comprueba la lista blanca. Si el remitente aparece en dicha lista el correo es aceptado. En caso contrario el correo se rechaza y opcionalmente se puede enviar un correo al remitente con las instrucciones necesarias para ser desbloqueado. Por defecto tras una instalación limpia este mensaje no se envía y debe prepararse de forma personalizada para cada instalación con las indicaciones oportunas.

La sintaxis para cumplimentar las listas debe especificar una coincidencia por línea, y puede ser una cuenta completa o un dominio. En este caso se recomienda anteponer el símbolo @.

ADMINISTRACION DE DOMINIO

La administración de cuentas de correo de un dominio permite añadir nuevas cuentas mantenerlas y eliminarlas. También permite efectuar redirecciones de cualquiera de estas cuentas.

Para acceder a este mantenimiento introduzcan el nombre del dominio y la contraseña de acceso.

Una vez aceptadas sus credenciales tendrá acceso a:

1. Mantenimiento de cuentas de usuario del dominio.
2. Mantenimiento de redirecciones de dominio.
3. Modificación de la contraseña de acceso.

CUENTAS DE DOMINIO

En esta opción podrá añadir cuentas o cambiar tanto el nombre de la cuenta como la clave de acceso. Por motivos de seguridad las claves no se muestran en pantalla, pero sin embargo por operatividad se pueden ver momentáneamente pulsando el botón del ratón sobre la casilla de la contraseña.

Para añadir una nueva cuenta debe indicar tanto el nombre de usuario como la contraseña. A este nivel las contraseñas no tienen limitaciones pero se recomienda utilizar contraseñas de seis o más dígitos que no tengan ninguna relación con el nombre de usuario y que no sean demasiado simples.

No debe equivocarse y pensar que no hay nada interesante detrás de esta cuenta de correo o de aquella y que por tanto no habrá interés por parte de nadie en hackearla. La realidad es que la mayoría de los robos de contraseñas que se producen en los últimos años no tienen como objetivo la obtención de datos sino el acceso a una pasarela abierta para envío masivo de spam.

Para eliminar una cuenta simplemente elimine el nombre de usuario y confirme la modificación mediante el botón grabar cuentas.

REDIRECCION DE CORREO

Mediante esta utilidad podrá redireccionar cuentas de correo. La redirección consiste en reconducir el destinatario de un determinado correo. Se pueden redirigir tanto las cuentas que tengan buzón propio como otras que no tengan. Esto quiere decir que un nombre de usuario puede estar solamente en cuentas de dominio, puede estar solamente en redirecciones o puede estar simultáneamente en ambos. En este último caso la redirección se impone ante el buzón, pero en el momento que se anula la redirección vuelve a estar activo el buzón.

Por supuesto las redirecciones siempre deben de corresponder al dominio que se está gestionando pero el destino puede ser cualquier dirección válida de correo.

CAMBIO DE CONTRASEÑA

Mediante esta opción podrá modificar la contraseña de acceso a este mantenimiento (mantenimiento de dominios).

CONFIGURACION DEL HOST

Si dispone de un servidor dedicado podrá acceder a este grupo de utilidades que permiten personalizar el funcionamiento global del servidor de correo.

Mediante estas utilidades podrá:

1. Añadir o eliminar nuevos dominios de correo.
2. Establecer manualmente filtros de entrada que le permitirán bloquear desde una Dirección de correo hasta un TLD (dominios top level) completo.
3. Establecer los límites máximos de envío por cuenta así como los filtros SPF y black lists.
4. Tendrá acceso a una estadística con los últimos datos disponibles de utilización.

ADMINISTRADOR DE DOMINIOS

Esta opción le permitirá añadir, modificar o eliminar dominios de correo. En la persiana desplegable de la parte superior del panel dispondrá de la lista de dominios en uso actualmente. Al seleccionar uno de estos dominios preexistentes tendrá la opción a modificar los datos o anular totalmente el dominio.

Para crear un nuevo dominio seleccione NEW en dicho desplegable cumplimente los datos y presione el botón nuevo.

FILTROS DE ENTRADA GLOBALES

Esta utilidad le permitirá explotar el filtro interno del propio servidor para eliminar correo indeseado. Aunque esta opción está orientada principalmente a limitar acceso por dominios, su potente sistema de edición regex, permite ir mucho más allá, permitiendo aplicar esta avanzada sintaxis para dominios TLD o para otros objetivos.

Si no utilizamos la sintaxis regex, el sistema filtrará cualquier coincidencia con cualquiera de las líneas que aparezcan en el panel desplegable. Este manejo es muy sencillo pero conviene tener presente que la coincidencia puede no ser exactamente la que esperamos. Por ejemplo imaginemos que queremos bloquear un dominio denominado test.com. Si añadimos la línea test.com tal cual, bloquearemos cualquier correo en el que se encuentre esta coincidencia por ejemplo:

- test.comercial@gmail.com
- juan.lopez@mastest.com
- usuario@test.com

Este inconveniente puede ser subsanado simplemente añadiendo '@' delante del dominio.

Sin embargo si queremos bloquear cuentas concretas seguramente nos veremos obligados a utilizar regex. El siguiente ejemplo sirve como ilustración, y en él se bloquea la cuenta john@test.com.

- j.john@test.com también usuario del mismo servidor será bloqueado
- john@test.com funcionaria perfectamente.

Entre otras cosas la sintaxis regex permite indicar inicio y final de la coincidencia. Para indicar inicio usaremos la combinación de caracteres ^. Mientras que para indicar final utilizaremos la combinación de caracteres \$

Además para poder determinar qué la sintaxis utilizada es regex todo el conjunto debe ir entre caracteres '/'. Aplicando esta sintaxis el ejemplo que veíamos anteriormente podría limitarse con toda precisión mediante las expresiones:

- /.john@test.com/ (Valida)
- /.john@test.com\$/ (Mejor aún)

CONTROL DE SPAM (ENVIO Y RECEPCION)

Ahora veamos cómo tener más control sobre el envío y la recepción de correos. La primera sección de esta opción le permite establecer los límites de envío de correo para cada cuenta de usuario por hora, día y mes.

Estos límites deben de ser manejados con extrema precaución pues es la salvaguardia para evitar el lanzamiento masivo de spam tanto motivado por robo de contraseñas, por cualquier tipo de virus en los ordenadores de los usuarios o por cualquier otra razón.

En este sentido es importante saber que con las tecnologías modernas actuales una sola cuenta hackeada puede enviar hasta 10000 correos por hora, cantidad más que suficiente para que muchos servidores de listas negras detecten la actividad de este servidor como spammer.

En la parte inferior tenemos la posibilidad de activar o desactivar el filtro de entrada SPF, así como varios filtros correspondientes a servidores de listas negras. Normalmente se recomienda utilizar siempre el filtro SPF, y en cuanto a las listas negras puede evaluar cuáles le interesan en función de:

- spamhaus. Lista negra de carácter moderado muy reconocida entre los administradores de correo.

- spamcop. Es una lista negra moderada que ha funcionado durante muchos años.

- sorbs. Es una de las listas más apreciadas de internet, aunque en algunas ocasiones ha incluido a gmail como servidor de mala reputación lo cual puede hacer que dejemos de recibir algunos correos.

- barracuda. Es una de las listas más exigentes de internet. Incluir esta lista como filtro asegura un nivel de spam mínimo aunque podrían perderse correos.

ESTADÍSTICAS

La estadística del sistema de correo le permitirá comprobar los siguientes datos por e mail y día:

- Pop3_: número de conexiones POP3 realizadas
- Imap_: número de conexiones IMAP realizadas
- Sent: número de correos enviados
- Bounc: número de envíos rechazados (bounced)
- Defer: número de envíos postpuestos (deferred)
- Queue: número de envíos en espera (queued)
- PSent: reservado
- Reser: reserva
- Rejec: número de envíos rechazados (reject)
- BList: número de correos de entrada bloqueados por listas negras
- NoSPF: número de correos de entrada bloqueados por incumplir criterio SPF
- LostC: número de conexiones interrumpidas.

APENDICE

Proceso en tiempo real: smtpfilter

1. Spam out control

2. Incomming mail:

2.1 Check blacklist. Founded -> drop

2.2 Check whitelist. Not found -> response with policy explanation (Delayed)

2.3 Sent to recipient.

2.4 Check autoresponder. -> Send response to sender

Proceso diferido: maillog

1. Lock control.

ID: ctladdr=user@domain.tld -> counter -> lock if exceed

2. Response not whiitelist.

ID: response to=sender from=user@domain.tld not whitelisted -> send if not
previously done

3. Autoresponse.

ID: response to=sender from=user@domain.tld autoresponse

ID: warning: Subject from -> send if not sent already

