Email Protection

Guía rápida de configuración

Contenidos

1. Prólogo

¿A quién está dirigida esta guía?

Iconos

1.1. Introducción

Esta guía contiene información para la puesta en marcha del servicio y configuración básica del producto Panda Email Protection.

1.2. ¿A quién está dirigida esta guía?

Esta documentación está preparada para el personal técnico que configura el servicio de protección para el correo corporativo desde:

El departamento de IT de la empresa que desea implementar un servicio de correo seguro a los usuarios de la red.

El proveedor de servicios gestionados (MSP) que ofrece el servicio de correo seguro a sus cuentas de clientes.

1.3. Iconos

En esta guía aparecen los siguientes iconos:

Información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consejo importante de cara a un uso correcto de las opciones de Panda Email Protection

2. Introducción a Email Protection

2.1. Introducción a Email Protection

Panda Email Protection es una solución de seguridad Cloud para el correo electrónico. Los servicios Cloud permiten centrarte en tu negocio, liberándote de las tareas de gestión y de los costes operativos de las soluciones de seguridad tradicionales. Email Protection consta de un sistema multicapas que combina distintos filtros y mecanismos de protección que emplean tanto tecnologías propias (Panda Email Protection PROACTIVE, Listas de Confianza...) como tecnologías estándar (reputación de IPs, RBLs, listas blancas y negras, greylists, traffic shaping...) para asegurar la máxima efectividad. Mediante la eliminación de spam, virus y phishing - empleando más de diez filtros diferentes -, no sólo se reduce la carga del servidor de correo electrónico, sino que también disminuyen los problemas de productividad relacionados al tiempo dedicado a la eliminación del spam.

Email Protection posee una interfaz intuitiva y de fácil configuración que permitirá al administrador poner en funcionamiento rápidamente los elementos de protección necesarios para la seguridad de la empresa.

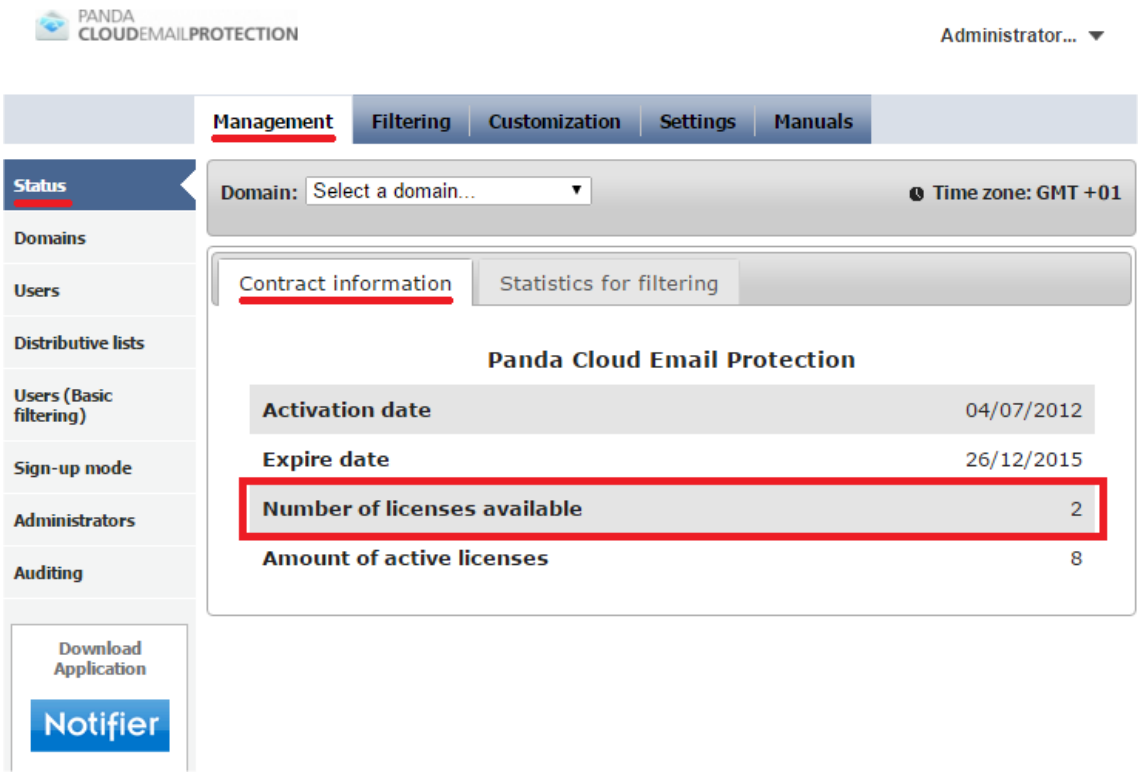
2.2. Algunas de las funcionalidades de Email Protection son:

- Configuración centralizada
- Fácil administración
- Antispam multicapas
- Backup de correo entrante
- Alta de usuarios:
- Manualmente
- Importación desde archivo
- LDAP call out con descubrimiento de Alias
- SMTP call out
- Delegación de administración por dominio
- Log de correos con posibilidad de abrir los correos, agregar remitentes/IP's a lista blanca/negra, clasificar correos como Válido/Spam
- Listas de Confianza por usuario
- Filtros personalizados
- Aplicación de notificación informativa de correos en cuarentena

3. Modelo de licenciamiento

3.1. Modelo de licenciamiento

Panda Email Protection es un producto que se contrata en modo servicio, de esta manera cada buzón de correo que será protegido por la solución consumirá una licencia de las contratadas para el producto. Se puede comprobar el estado en todo momento de las licencias disponibles en el Menú Gestión, Estado, Estado de subscripción.



Para el cómputo de licencias necesarias se deben de considerar las siguientes excepciones:

Dominios alias

En el caso de tener dado de alta un dominio (por ejemplo 'pandatest.com') con usuarios ya creados (consumiendo licencias en el sistema) y de tener un dominio que sea un alias a este dominios (por ejemplo 'pandatest.es'), se puede configurar este dominio como un alias y por tanto todos los usuarios presentes en el dominio principal estarán implícitamente configurados en el dominio de alias sin que estos usuarios del dominio alias consuman una licencia adicional.

3.2. Cuentas de correo alias

Cada licencia permite proteger hasta 5 cuentas de alias asociadas al buzón principal que consume licencia en el sistema. Para que el sistema pueda reconocer estas cuentas de alias cubiertas bajo la licencia asociada al buzón principal, es necesario que estas direcciones de

correo alias se encuentren configuradas correctamente como tales en el sistema. La configuración de los buzones de alias se puede hacer manualmente (sección 4.1.2.1) o bien mediante el método de configuración automática de usuarios por LDAP (sección 4.1.2.4) siempre que se haya activado la opción Activar descubrimiento de alias. El descubrimiento automático de cuentas de alias no estará disponible si se selecciona la opción de provisión automática por SMTP, por lo que se recomienda el alta automática por LDAP siempre que exista un número considerable de cuentas de correo de alias en la organización.

En el caso de que se tengan buzones protegidos que sean alias de otros buzones principales y no haya configurado estos buzones en Email Protection como usuarios alias, estas cuentas consumirán una licencia. En este caso será necesaria la revisión de la configuración de estos buzones en Email Protection.

4. Configuración inicial de la cuenta Email Protection

Configuración de filtrado de correo entrante

Configuración de filtrado de correo saliente

Configuración de registros SPF en el DNS

4.1. Configuración inicial de la cuenta Email Protection

Esta guía recoge los pasos iniciales de configuración necesarios para poder proteger los dominios de correo electrónico de la empresa y a todos sus usuarios. Toda la configuración detalla de esta guía se realiza desde la consola de administración. El acceso a la consola de administración habrá sido facilitado al administrador junto con este manual de configuración rápida (URL de acceso: https://mep.pandasecurity.com/admin/) y dispondrá de unas credenciales únicas de acceso a la interfaz de gestión.

⚠ ***La URL de acceso a la consola de administración puede variar y no corresponder con la especificada en este documento. Por favor, revisa el correo de bienvenida al servicio que te ha sido enviado a la dirección de contacto suministrada en el momento en que se generó el acceso.***

La configuración inicial aquí descrita es obligatoria para indicarle a Email Protection los dominios que serán protegidos por la solución, así como los buzones de los usuarios finales que serán filtrados.

La configuración inicial recogida en estos puntos (sección 3.1) es obligatoria ya que de no completarla correctamente y apuntar sus registros MX en su DNS a nuestra solución de filtrado sin completar los pasos detallados en esta guía resultarán en un rechazo de los correos entrantes y salientes de la organización con un código de error permanente, teniendo como resultado final que esos correos nunca serán entregados a sus destinatarios finales.

La configuración detallada en la sección configuración de correo saliente (3.2) es opcional en caso de que se desee que Email Protection realice el filtrado de los correos salientes de la organización, al igual que la configuración detallada en la sección de configuración de seguridad (3.1.5).

4.2. Configuración de filtrado de correo entrante con Email Protection

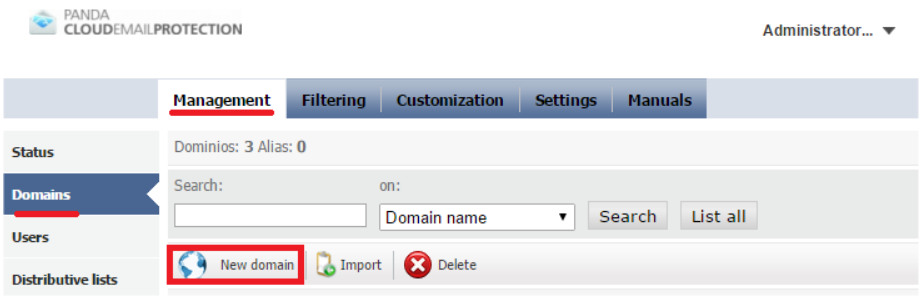
La configuración inicial de la solución Email Protection de Panda Security consiste en varios pasos que deben seguirse en este orden:

- Configuración del dominio o dominios a proteger en la plataforma.
- Configuración de las cuentas de correo de la organización que serán protegidas por la plataforma.
- Personalización inicial de la plataforma, en caso de que se desee cambiar el aspecto de la interfaz y las comunicaciones a las cuentas de correo que serán protegidas.
- Redirección de los registros MX de los dominios protegidos hacia la solución de Panda Security.

A continuación describiremos con detalle como completar cada uno de estos pasos.

Configuración de dominios

El primer paso de configuración consiste en indicar el dominio o los dominios que serán protegidos por la plataforma. Esta configuración se realiza en el Menú Gestión, Dominios. Para cada dominio de correo que se desee proteger por la plataforma Email Protection se debe pulsar Crear dominio:



La información a introducir por dominio a proteger es la siguiente:

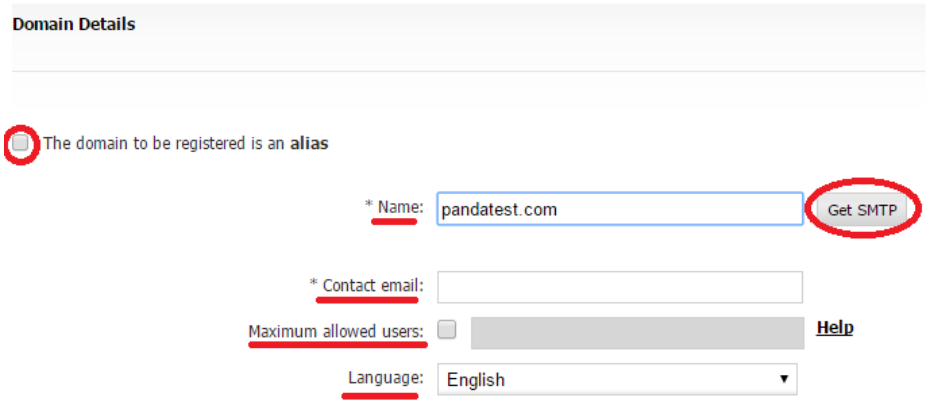
Marca la casilla El dominio a dar de alta es un alias si el dominio que estás configurando es un dominio de alias de otro dominio que ya haya configurado en el sistema.

Es necesario introducir el nombre del dominio a proteger de la organización (por ejemplo 'pandatest.com').

Es necesario introducir un correo electrónico de contacto donde se enviarán las notificaciones relacionadas con ese dominio (como por ejemplo el proceso de sincronización de usuarios o si se ha alcanzado el máximo número de licencias permitidas para ese dominio).

Se puede limitar el número de licencias que serán utilizadas por ese dominio del número total de licencias disponibles en el producto (máximo).

Se puede seleccionar un idioma predeterminado por dominio. Todas las notificaciones a usuarios protegidos por la solución en este dominio así como su interfaz de gestión de usuario final se encontrarán en el idioma seleccionado.



A continuación debes de configurar el nombre de host o la dirección IP donde Panda Email Protection deberá realizar la entrega de los correos una vez realizado el filtrado. Esta dirección será la dirección actual donde se encuentra tu servidor de correo. Si para este dominio aún no se ha realizado la redirección de los registros MX en el DNS, el botón Obtener SMTP rellenará los campos Host MX de forma automática. Asegúrate de que este campo este apuntando al servidor de correo donde se encuentran los buzones que serán protegidos por la solución.

La solución permite configurar varios servidores donde serán entregados los correos una vez filtrados, con distinta prioridad. Asegúrate de que el campo Prioridad tiene un valor distinto de 0 y ten en cuenta que el host MX con mayor prioridad será el que tenga el número más bajo.

Una vez configurados los host MX de destino, asegúrate de comprobar la conectividad SMTP entre la plataforma de filtrado Email Protection y sus servidores de correo utilizando el botón Comprobar SMTP.

De existir algún problema en la conectividad, asegúrate de que los centros de datos de Panda Email Protection pueden establecer comunicación SMTP con sus servidores de correo. El direccionamiento de nuestros centros de datos comprende los siguientes rangos:

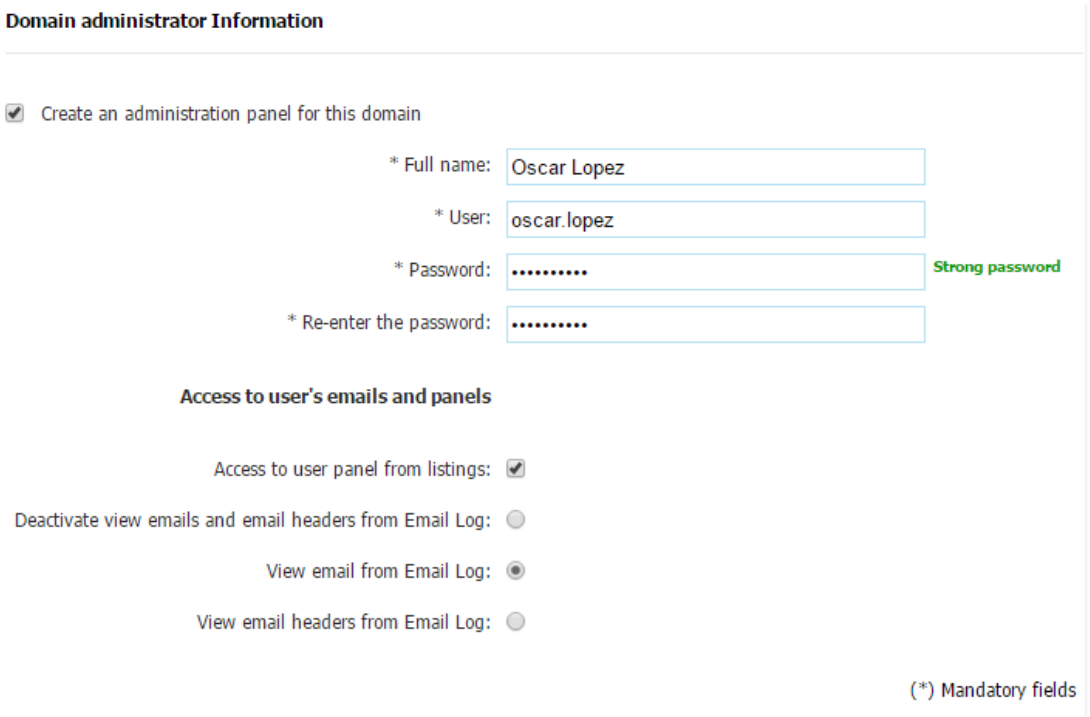
188.94.13.128/25

92.54.22.0/24

92.54.27.0/24

> ⚠ ***El rango de direccionamiento especificado en este documento puede variar. El rango de direccionamiento actualizado está reflejado en la consola de administración bajo la sección Manuales, Información de Configuración.***

En este punto puedes completar la configuración del dominio que será protegido o bien puedes definir en este punto un Administrador de Dominio. Este administrador de dominio tendrá unas credenciales de acceso a consola de administración (https://mep.pandasecurity.com/admin/) donde únicamente podrá realizar cambios de configuración para el dominio configurado:



Una vez completada la configuración del dominio, guárdala y procede con el siguiente paso de la configuración: dar de alta los usuarios (buzones de correo) que serán protegidos por la solución.

Configuración de buzones de correo a proteger

Debido al modo de funcionamiento de Panda Email Protection, es necesario configurar todos los buzones que serán protegidos por la plataforma. De no realizar la configuración de los buzones a proteger (bien de forma manual o automática), se procederá a un rechazo permanente de los correos entrantes y salientes de la organización si Email Protection se encuentra procesando correo de tus dominios.

La configuración de los buzones que serán protegidos puede hacerse de varias formas:

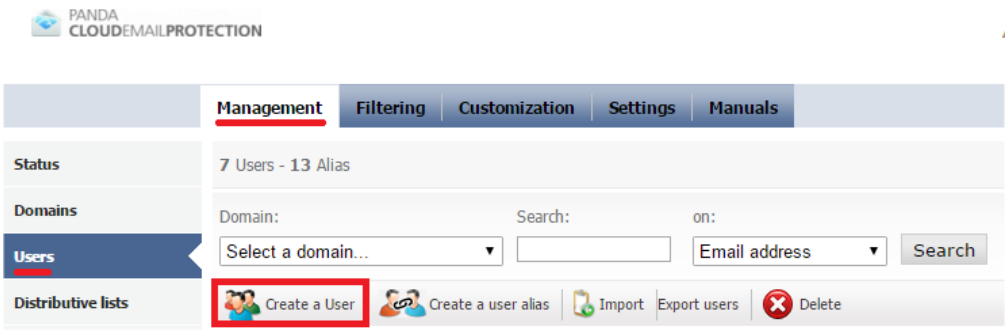
- Manual: Dando de alta manualmente los buzones (o alias de los buzones) individualmente. Importando los usuarios de una lista (en formato TXT o CSV).
- Automática: Se deberá configurar el dominio protegido por la solución mediante uno de los mecanismos de alta automática disponibles: SMTP o LDAP.

La configuración de usuarios por cualquiera de estos métodos no es excluyente: Se pueden configurar manualmente ciertos buzones y activar el alta automática de ciertos usuarios. Ambos mecanismos pueden coexistir.

Configuración manual de usuarios

Los buzones de correo que serán protegidos por la plataforma pueden configurarse manualmente en la consola de administración desde el Menú Gestión, Usuarios. Desde este menú se pueden crear usuarios correspondientes a direcciones de correo principales o direcciones de correo alias asociadas a otro buzón principal ya configurado en la plataforma.

Para la creación de usuarios correspondientes a direcciones de correo principales se debe pulsar en Crear Usuario:



Se debe proporcionar la siguiente información mínima para la creación de un usuario:

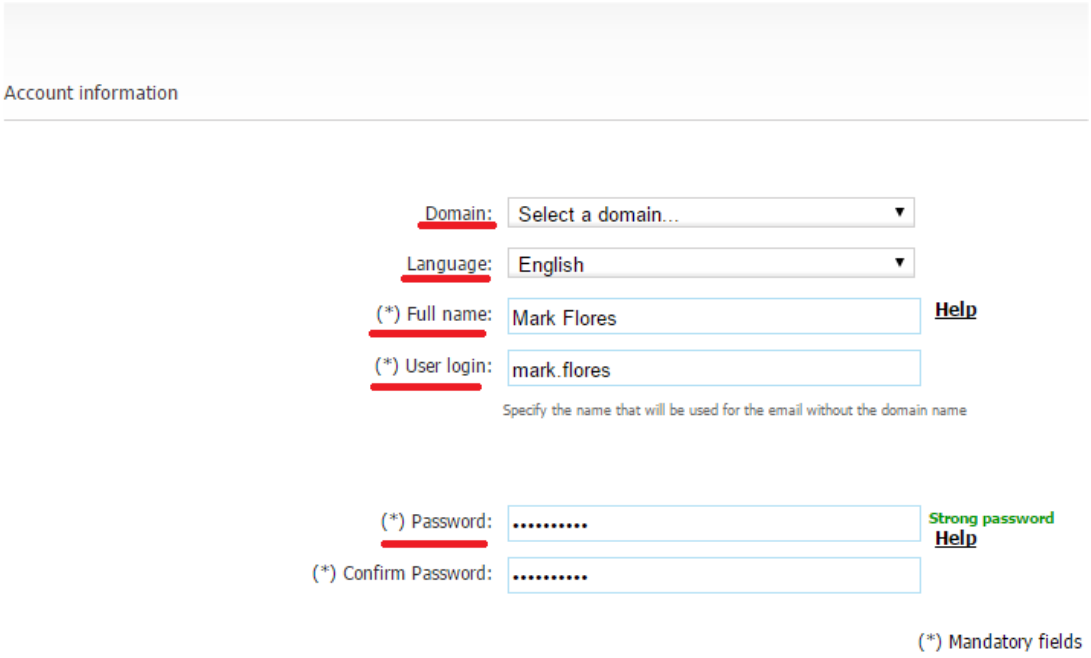
Dominio: Se seleccionará el dominio donde estará el buzón principal del usuario a proteger.

Idioma: Idioma predeterminado. El idioma principal de su interfaz de administración así como todas las comunicaciones se realizarán en este idioma. Por defecto se configurará el definido al crear el dominio a proteger.

Nombre y Apellidos: Esta información será meramente administrativa asociada al buzón que se crea en la plataforma, para poder listar a los usuarios por su nombre y apellido.

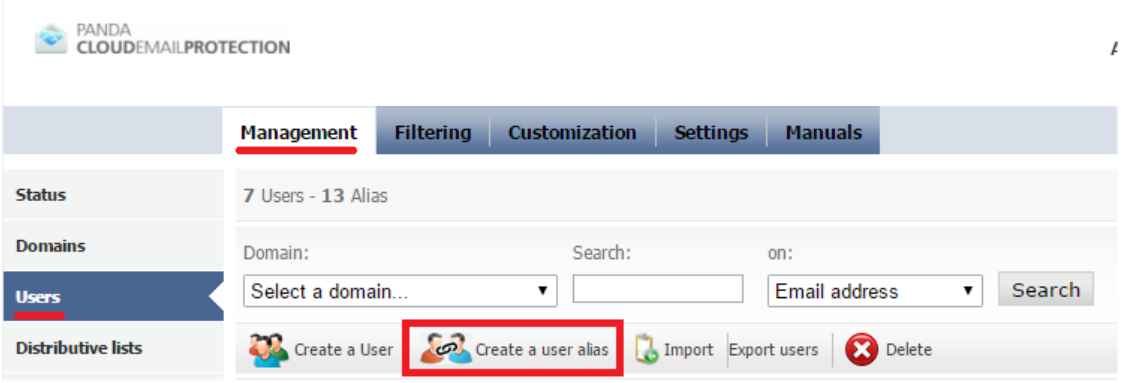
Login del usuario: Esta será la dirección de correo asociada al usuario en el dominio que se protege. Se debe especificar únicamente el nombre del buzón, sin el dominio al que pertenece.

Contraseña: Es obligatorio asignar una contraseña al usuario para su interfaz de gestión de usuario final.



En el ejemplo anterior hemos dado de alta el siguiente buzón de un usuario que protegerá la plataforma: 'mark.flores@pandatest.com'. Una vez introducidos los datos debemos guardar la configuración de este usuario.

Para la configuración de una dirección de correo alias asociada a una cuenta de correo principal, deberemos pulsar Crear Usuario, Alias desde el Menú Gestión, Usuarios.



Para poder crear un usuario alias, es necesario proporcionar la siguiente información:

Dominio en el que se creará el alias: Es el dominio que tendrá la cuenta de alias. No es necesario que sea el mismo dominio en el que reside la cuenta principal de la que es alias.

Dominio principal: Dominio donde se encuentra la cuenta principal asociada a la cuenta de alias que se está creando.

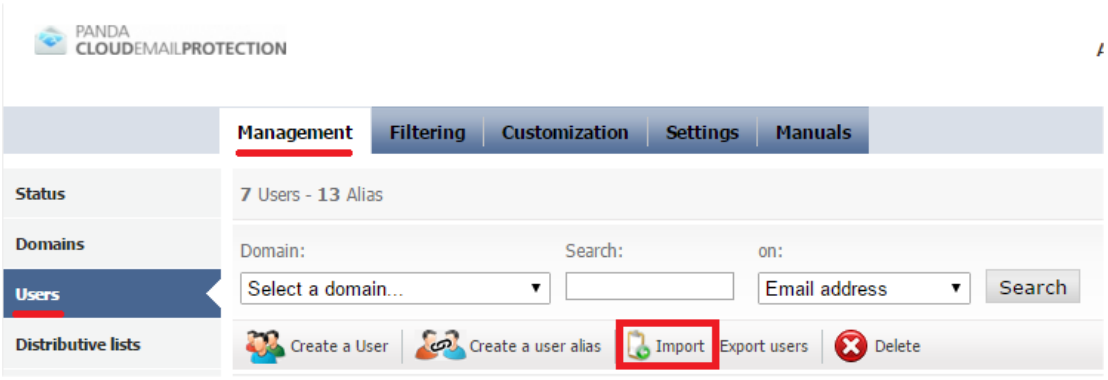
Alias: El nombre de la cuenta de alias que se protegerá, sin '@' ni dominio.

Cuenta principal: Se seleccionará una cuenta principal anteriormente provisionada en la plataforma.

Una vez introducidos los datos, debemos Guardar la configuración del usuario alias.

Configuración de usuarios importando listas

La plataforma Email Protection permite la creación manual de usuarios importando los usuarios desde un fichero. Esto se realiza desde el Menú Gestión, Usuarios. Desde aquí, pulsaremos Importar.



Antes de realizar la importación deberemos preparar un fichero que contenga los nombres de los buzones (y alias) a proteger. El archivo puede ser tanto un .csv como un .txt con el formato siguiente:

- Nombre y apellido, Dirección de Correo, Contraseña.
- Nombre y apellido, Dirección de Correo.
- Nombre y apellido, Dirección de Correo, Contraseña, lista de direcciones alias separados por coma.

Tanto la contraseña como los posibles alias asociados a un buzón principal son opcionales. Si no se especifica una contraseña, el sistema generará una de forma aleatoria cuando se importe el usuario. De especificarse las contraseñas recomendamos el siguiente criterio a la hora de crear una contraseña segura para los usuarios:

- Letras minúsculas y mayúsculas de "a" a "z", exceptuando "ñ".
- Números del 0 a 9.
- Símbolos permitidos: _ . –
- Longitud mínima de 8 caracteres y máxima de 64 caracteres.

La dirección de correo en el fichero puede especificarse de 2 formas:

- Incluyendo el dominio al que pertenece el buzón. En este caso un ejemplo de la lista sería:

  Miguel Sanchez, mzanchez@ejemplo.com, aras249gt

  Andrés López, alopez@ejemplo.com, 32kios5d

  Andrés López, alopez@ejemplo.com, alopez.alias1@ejemplo.com, alopez.alias2@ejemplo.com

- Sin incluir el dominio al que pertenece el buzón. En este caso un ejemplo de la lista sería:

  Miguel Sanchez, mzanchez, aras249gt

  Andrés López, alopez, 32kios5d Andrés López, alopez

  Andrés López, alopez, alopez.alias1, alopez.alias2

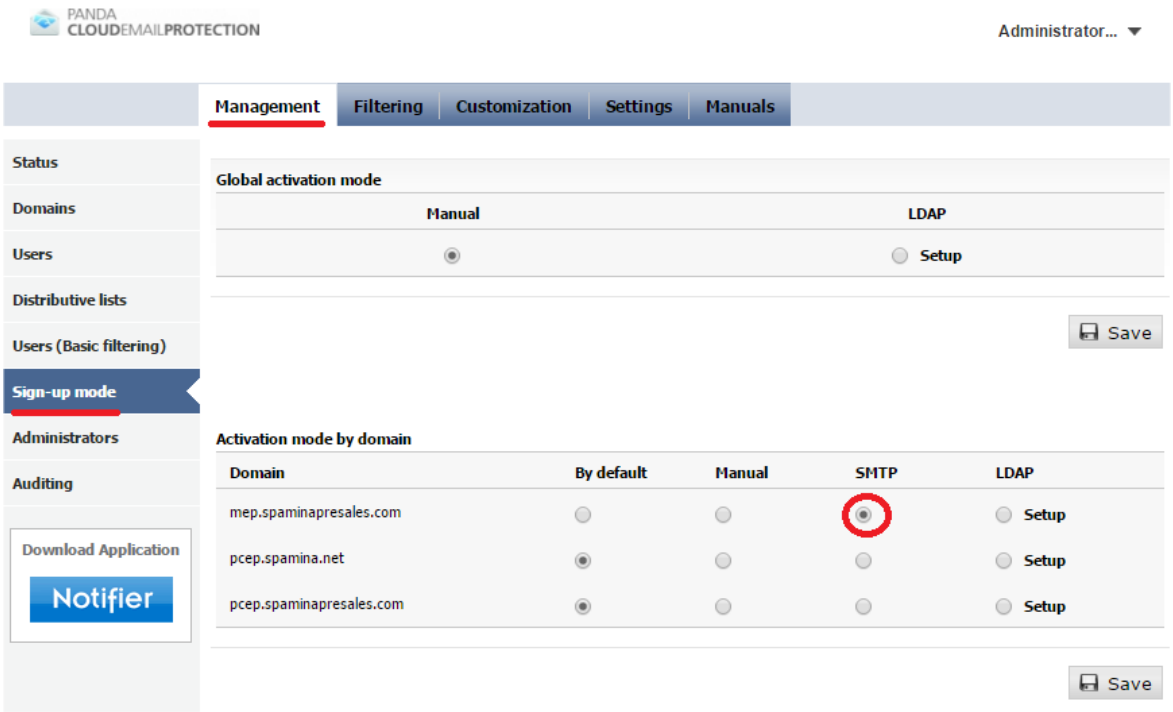
⚠ ***Es muy importante realizar la importación correctamente dependiendo de si la lista de buzones a importar contiene el dominio o si no se especifica el dominio. Si se especifica el domino en la lista a importar, es esencial dejar en blanco el campo 'Dominio:' en el menú de importación, de lo contrario fallará el proceso.***

Una vez seleccionado el archivo a importar y teniendo en cuenta las consideraciones anteriores, pulsaremos Importar. La importación de usuarios no se realizará de forma inmediata, sino que puede tardar varios minutos dependiendo del tamaño de la lista. El sistema enviará un correo electrónico al administrador de la cuenta con el resultado del proceso de importación.

Configuración automática de usuarios por SMTP

La plataforma de filtrado de correo Email Protection permite realizar la configuración automática de usuarios por SMTP. Mediante este mecanismo de provisión, los usuarios que no se encuentren provisionados en el sistema se irán configurando automáticamente conforme se reciba correo dirigido a esos buzones de correo protegidos.

La configuración de provisión automática por SMTP se selecciona por dominio configurado en la plataforma desde el Menú Gestión, Modo de Alta. Se deberá marcar el modo de alta del dominio por SMTP como sigue:



A continuación deberemos guardar la configuración. Al guardar la configuración se solicitará la introducción de un usuario existente en el dominio. Se debe introducir un usuario que exista en el dominio que se está protegiendo.

Esta comprobación tiene por objeto verificar que el servidor de correo es apto para la provisión de usuarios por SMTP. Si la comprobación falla al introducir un usuario existente en el dominio que se está protegiendo es posible que su servidor no sea apto para la provisión automática de usuarios por SMTP.

La causa más habitual de este fallo es que su servidor de correo no sea capaz de rechazar direcciones de correo no existentes en la organización. En Microsoft Exchange esta funcionalidad se conoce como 'Recipient Validation' y debe estar habilitada para que este método de provisión funcione correctamente.

⚠ ***El sistema no le permitirá configurar el modo de alta automática por SMTP en caso de fallo en la comprobación anterior.***

Una vez configurado el modo de alta por SMTP, el sistema irá creando los usuarios de forma automática en el momento en que la plataforma Email Protection reciba un correo dirigido a un usuario que no haya sido dado de alta anteriormente.

El alta automática por SMTP provisionará todas las direcciones de correo de la organización como buzones principales. Esto es un factor importante a tener en cuenta de cara al cómputo de licencias que serán utilizadas en la organización. En caso de que la organización tenga varias direcciones alias de correo electrónico, es recomendable configurar el sistema para que realice las altas automáticas por LDAP activando el descubrimiento de alias.

Configuración automática de usuarios por LDAP (Active Directory)

Otro mecanismo de provisión automática de usuarios consiste en realizar consultas por LDAP contra el servidor de directorio de su organización. Este es el mecanismo de provisión de usuarios automático recomendado para organizaciones de medio o gran tamaño en número de buzones a proteger.

El alta por LDAP incluye la funcionalidad de detectar y asociar automáticamente buzones de correo alias a buzones principales.

La configuración de alta automática por LDAP puede configurarse de forma global o por dominio. Recomendamos la configuración Global de LDAP si todos los dominios que serán protegidos por la solución dependen de un mismo controlador de dominio o servicio de directorio LDAP. Configura el alta por LDAP en dominios independientes si la organización dispone de varios servidores de directorio independientes por dominio.

Los requisitos para poder configurar el alta por LDAP son los siguientes:

- La nube de Panda Security debe poder acceder a su servicio de directorio (Active Directory / Lotus / LDAP) en una dirección pública o mediante un nombre completo de host visible desde internet.
- Las consultas se pueden hacer por LDAP o LDAPS.
- Se pueden hacer consultas anónimas, aunque lo más recomendable es crear un usuario dedicado para las consultas LDAP.

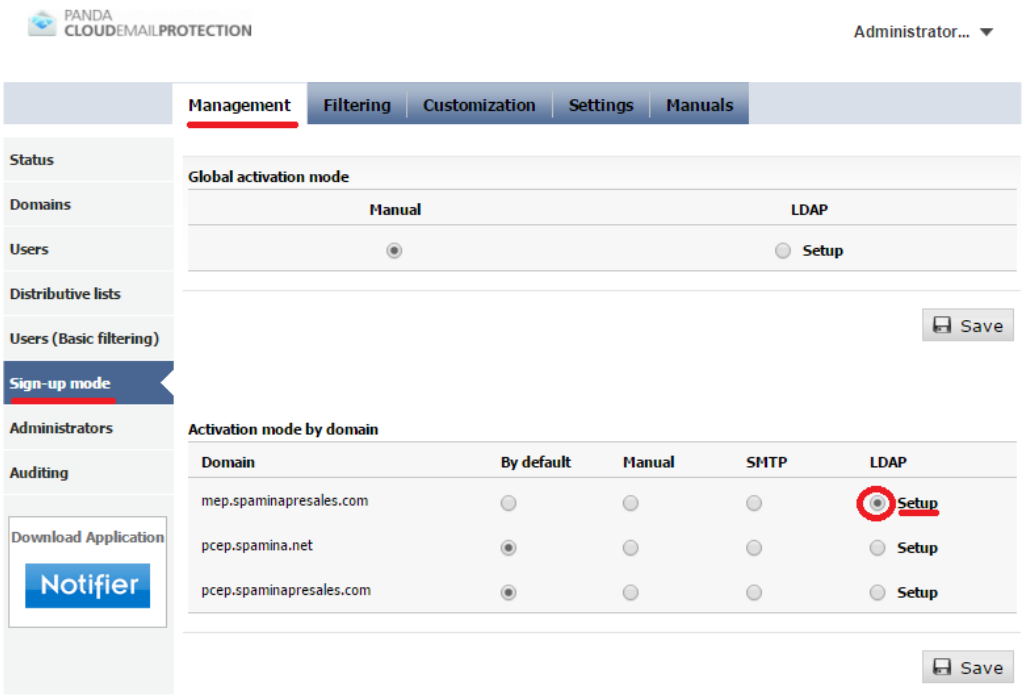
El rango de direccionamiento desde el que se lanzarán las consultas LDAP contra su servicio de directorio es el siguiente:

- 188.94.13.128/25
- 92.54.22.0/24
- 92.54.27.0/24

El rango de direccionamiento especificado en este documento puede variar. El rango de direccionamiento actualizado está reflejado en su consola de administración bajo la sección Manuales, Información de Configuración.

En el caso específico de integración con un servicio de Directorio Activo, será necesario crear un usuario perteneciente al grupo de usuarios de dominio y obtener las credenciales de ese usuario. Ejecuta las siguientes acciones previas en el controlador de dominio de la organización:

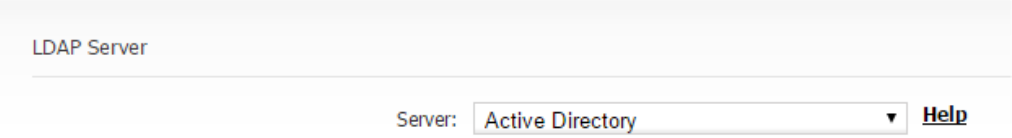
- Crea un usuario perteneciente al grupo 'Usuarios de Dominio'.
- La contraseña del usuario debe contener únicamente caracteres alfanuméricos y los símbolos '_' y '-'. Se recomienda no utilizar otros caracteres.
- Indica que el usuario no debe cambiar la contraseña y que la contraseña nunca expire.
- Una vez creado el usuario, se debe obtener la ruta Distinguised Name del usuario. Para ello, abre una ventana de comandos desde el controlador de dominio y ejecuta el siguiente comando:
- dsquery.exe user –name [USUARIO]
- Por ejemplo, en el caso de que el usuario creado en el sistema para las consultas LDAP se llame 'panda', el comando a ejecutar y su respuesta será lo siguiente:
- dsquery.exe user –name pandaCN=panda,CN=Computers,DC=dctest,DC=local
- El usuario de consulta a configurar en el sistema será lo devuelto por el comando: 'CN=panda,CN=Computers,DC=dctest,DC=local'
- Una vez obtenida esta información, se puede realizar la configuración del alta por LDAP en el sistema desde el Menú Gestión, Modo de Alta, seleccionando Configurar y después haciendo clic en Configurar.



A continuación se explica la configuración a introducir basándonos en el caso de que estemos configurando la integración con un controlador de dominio Microsoft Active Directory:

- Servidor LDAP

Active Directory. En caso de disponer de otro servicio de directorio, especifícalo aquí.



- Conexión

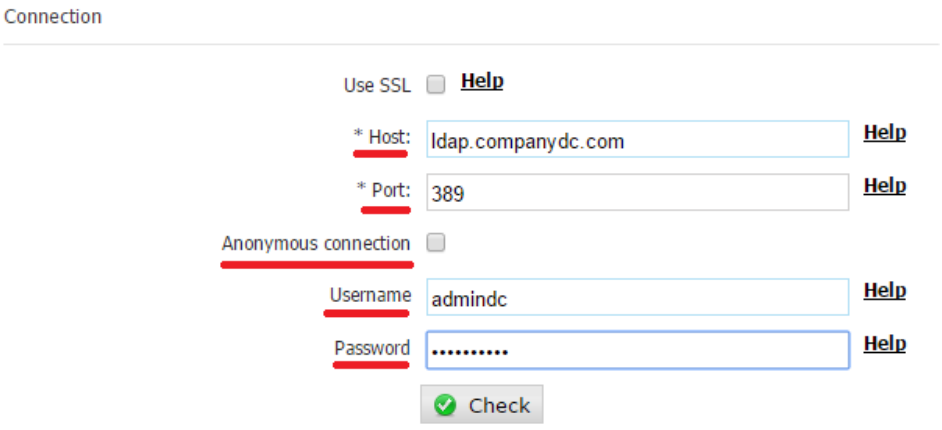
Host: IP o FQDN del servicio para poder acceder a su controlador de dominio. Debe ser accesible desde las IPs de la nube de Panda.

Puerto: 389 (por defecto)

Conexión Anónima: [Desmarcado] Los controladores de Dominio de Microsoft no permiten las consultas de usuarios de forma anónima. Desmárquelo.

Nombre de Usuario: Se deberá introducir la ruta CN obtenida al usuario mediante el comando ejecutado anteriormente en el controlador de dominio, en este caso: CN=spamina,CN=Computers,DC=dctest,DC=local

Contraseña: Se debe especificar la contraseña asignada al usuario que se utilizará para las consultas.



Una vez introducidos los valores correctos, pulsa el botón de verificar. El sistema indicará si la conexión y autenticación con el sistema de directorio se ha podido realizar correctamente. De existir un fallo, por favor revisa que la conectividad desde las IPs de la nube de Panda Security en el puerto asignado y las credenciales del usuario son correctas.

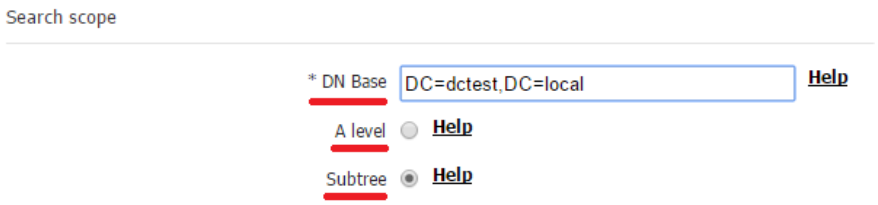
- Alcance de la búsqueda

DN Base: Punto en la estructura LDAP donde comenzará a buscarse usuarios.

Se recomienda configurar un punto de búsqueda lo más próximo a la raíz para poder así encontrar a todos los usuarios de la organización, independientemente de si se encuentran en distintas unidades organizativas. La ruta de búsqueda base puede obtenerse a partir del CN del usuario utilizado para las consultas. En el caso de Directorio Activo se pueden coger la parte del CN del usuario que comienza por DC, para el caso anterior sería: *DC=dctest,DC=local*

Un Nivel: Selecciona esta opción si todos los usuarios de la organización se encuentran en el punto donde se especifica la búsqueda.

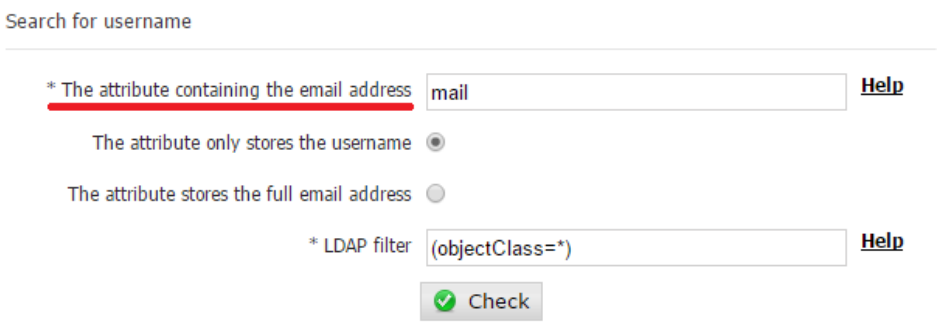
Subárbol: Selecciona esta opción si deseas que realicemos una búsqueda a este nivel y niveles superiores en la estructura LDAP en búsqueda de los usuarios. Habitualmente esto es lo recomendado cuando se especifica un DN Base próximo a la raíz.



En el ejemplo propuesto anteriormente marcaremos la búsqueda en Subárbol, para permitir que se encuentren los usuarios en niveles superiores a la ruta indicada.

- Búsqueda del nombre de usuario

Al seleccionar el tipo de servicio de directorio adecuado (Active Directory / Open LDAP / Lotus Domino), estos campos se completarán automáticamente. En caso de configurar un servicio de Directorio Activo, suele ser necesario indicar que El atributo almacena la dirección de correo electrónico completa



A continuación prueba mediante el botón Verificar que la configuración es la adecuada para el servicio de directorio. Se le pedirá al administrador que introduzca una dirección electrónica principal (no un alias) de su organización y el sistema comprobará si la puede localizar realizando una consulta, comprobando por tanto que la configuración de esta sección es correcta.

En caso de no encontrarse la dirección introducida, asegúrate de revisar la configuración de esta sección y contrastar los atributos aquí introducidos con el administrador de dominio para verificar los campos donde se encuentran las direcciones de correo de los usuarios en el servicio de directorio.

- Búsqueda de Alias

Esta es la funcionalidad más interesante que proporciona el alta de usuarios por LDAP frente al SMTP: el descubrimiento de las cuentas de alias. Se recomienda activarlo para el alta por LDAP.

Atributo que contiene el Alias: proxyaddresses. En la mayoría de las instalaciones de directorio activo + Exchange, proxyaddresses es el atributo que se debe configurar aquí.

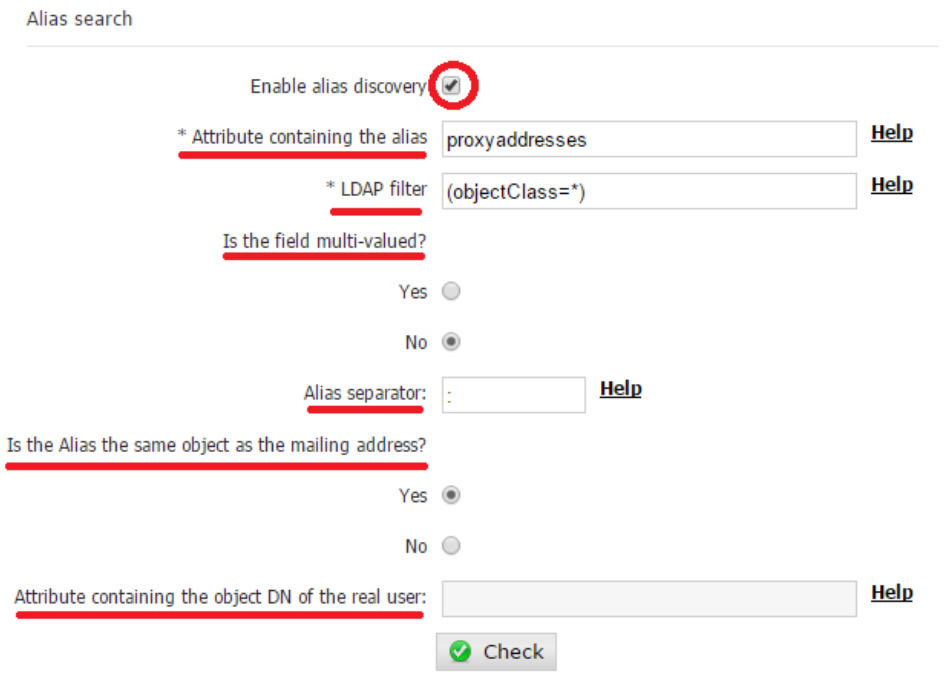
Filtro LDAP: (objectClass=*) Se pueden especificar filtros específicos si se desea para restringir la búsqueda únicamente a ciertos usuarios.

¿El campo es multievaluado?: No

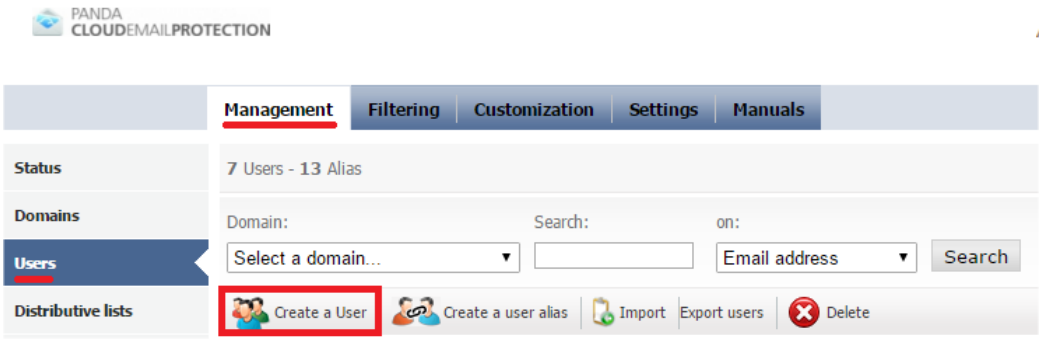
Separador de Alias: Se introducirá ':'

¿El Alias está en el mismo objeto que la dirección de correo? Si

Estos valores son los habituales para un esquema estándar de directorio activo. A continuación se debe realizar la verificación de los valores introducidos. Se deberá introducir una dirección de correo de alias asociada a un usuario y la comprobación deberá devolver la dirección de correo principal encontrada para ese alias. La configuración de esta sección junto con el resultado de la comprobación se muestran a continuación:



Si la comprobación no devuelve correctamente la dirección principal asociada a la dirección de alias introducida, asegúrate de revisar la configuración de esta sección y contrastar los atributos aquí introducidos con el administrador de dominio para comprobar los campos donde se guardan las direcciones de alias en su servicio de directorio.

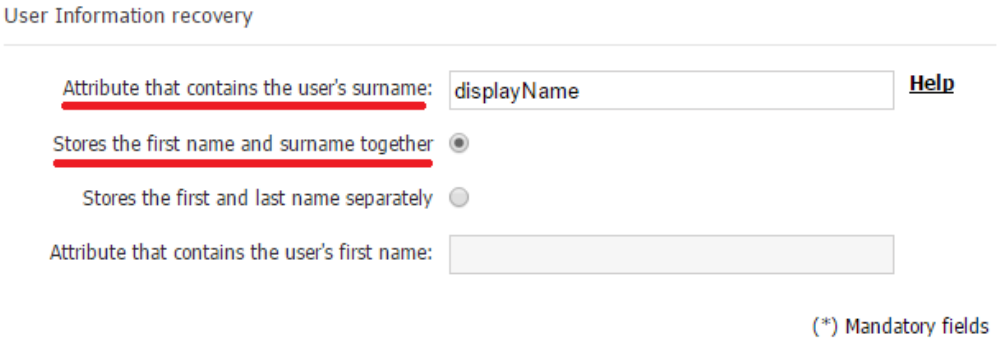


- Recuperación de datos del usuario

Es conveniente especificar al sistema en qué atributos se incluye el nombre y apellidos del usuario, para poder identificarlo más fácilmente cuando se da de alta automáticamente en el sistema. Los valores habituales en esta sección para un controlador de dominio Active Directory son:

Atributo que contiene el apellido del usuario: displayName

Almacena el nombre y apellido juntos: Seleccionado.



Una vez realizada la configuración de LDAP, guarda los cambios.

Ten en cuenta lo siguiente a la hora de introducir toda la configuración necesaria para el alta automática por LDAP:

Debe de poder comprobarse

La conectividad con el controlador de dominio es correcta.

La comprobación de usuarios localiza cuentas de correo correctamente (sección Búsqueda de nombre de usuario)

En caso de activar el descubrimiento de alias, se debe realizar la verificación para comprobar que el sistema localiza las cuentas principales a partir de las direcciones de alias.

En caso de localizar un error, conviene ir guardando la configuración a medida que se vayan superando las comprobaciones (es decir, guardar la configuración y seguir editándola posteriormente según se va progresando.

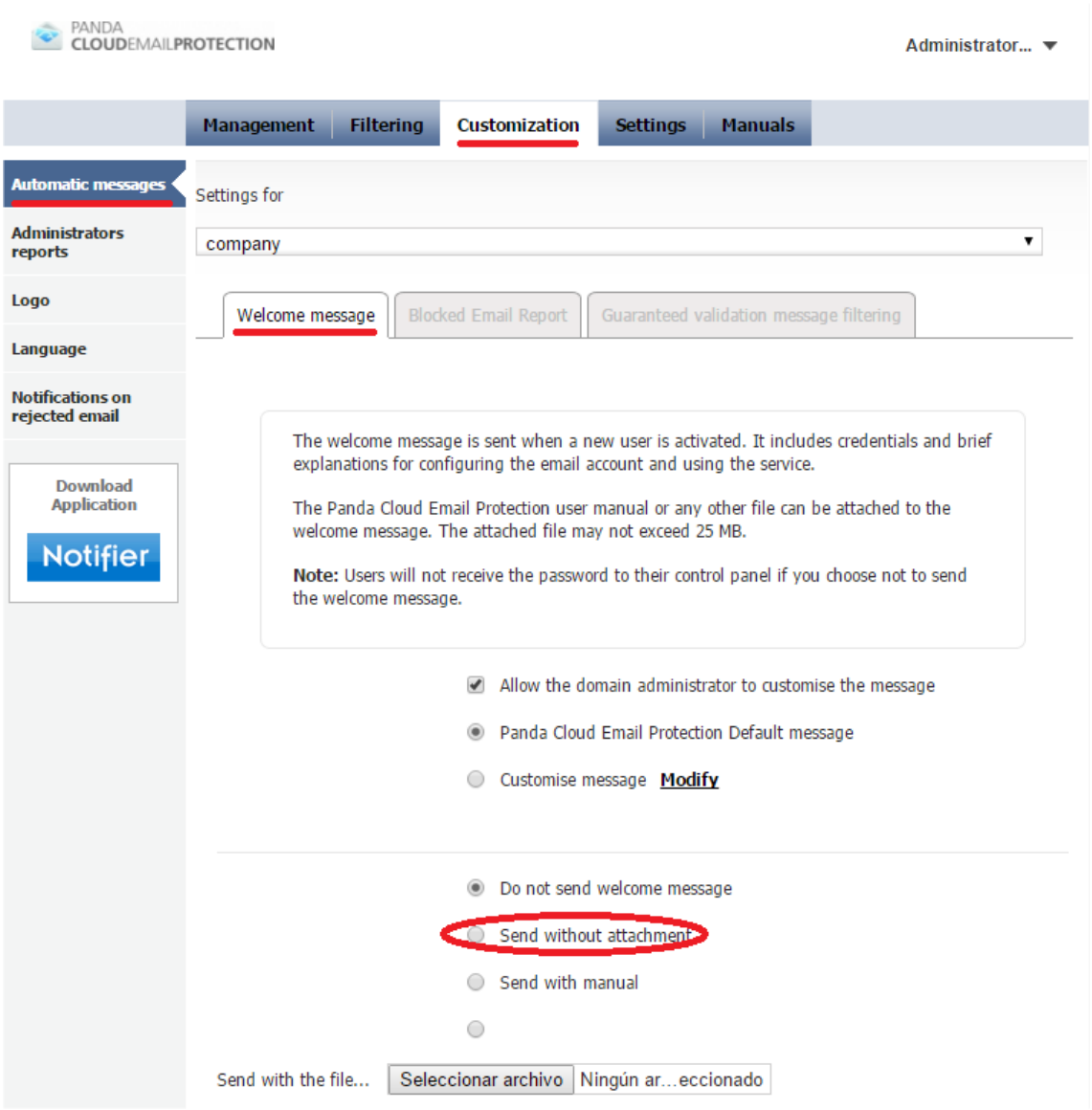
La configuración incluida en esta sección está específicamente orientada a la configuración de un servicio de directorio basado en Active Directory. La configuración aquí indicada puede variar levemente en cada organización, si bien esta configuración está garantizada para funcionar si no se ha modificado el esquema estándar de Active Directory en tu instalación.

- Personalización de la plataforma

Una vez realizados los pasos anteriores, la plataforma se encuentra lista para comenzar a proteger a los usuarios de los dominios configurados. El siguiente paso es personalizar la plataforma desde el Menú Personalización. Se recomienda considerar la siguiente personalización básica:

Mensaje de bienvenida: En caso de que se haya configurado un mecanismo de alta automática (SMTP o LDAP), la plataforma puede configurarse para enviar un mensaje de bienvenida al usuario en el que se enviarán las credenciales de acceso al usuario al panel de

gestión de usuario final. Si se prefiere notificar a los usuarios finales de la posibilidad de acceder a un panel de control donde pueden gestionar sus prioridades de filtrado y acceder a sus correos de Spam almacenados en la cuarentena del sistema, activa esta opción (deshabilitada por defecto)



Logotipo: El administrador de la empresa puede subir un logotipo personalizado que será mostrado en todas las notificaciones que se envían a los clientes así como en la interfaz de usuario final. Esto puede hacerse desde Personalización, Logotipo:

Las personalizaciones se pueden realizar a nivel global o para alguno de los dominios dados de alta en el sistema. El nivel de personalización se selecciona desde Mostrar configuración de: donde se puede aplicar la configuración seleccionada específicamente por dominio.

Configuración de los registros MX de su DNS

Una vez completados los pasos anteriores, la plataforma está lista para proteger correo entrante de la organización. Para introducir el sistema de filtrado Email Protection en el flujo de entrega de correo de la organización, se debe modificar los registros MX del dominio a proteger. Para cada dominio configurado en la plataforma Email Protection, se deben de cambiar los registros MX apuntando a los siguientes hosts:

- mx01.mep.pandasecurity.com
- mx02.mep.pandasecurity.com

La configuración de los registros MX asociados al servicio Email Protection pueden variar respecto a los indicados en este documento. Los registros MX que se deben de usar asociados a la cuenta se encuentran reflejados en la consola de administración bajo la sección Manuales, Información de Configuración. Por favor, revisa esta sección antes de aplicar los cambios pertinentes en el servicio de DNS.

Se recomienda asignar la misma prioridad a ambos registros MX (por ejemplo '10') para conseguir un balanceo entre ambos hosts.

Panda Security no tiene acceso a los registros MX de los dominios de nuestros clientes. Es responsabilidad del cliente realizar este cambio ya que el registro de los dominios pertenece a los clientes finales de Panda Security. Consulta con el administrador de red o con tu proveedor del servicio de DNS de los dominios para obtener información sobre cómo realizar este cambio.

Una vez realizado el cambio, la plataforma Email Protection comenzará a procesar correo entrante de la organización, procederá al filtrado y a la retención de correo Spam o malicioso y entregará el correo legítimo en el servidor de correo protegido por la solución.

Configuraciones adicionales de seguridad (Firewall)

Una vez realizado el cambio de los registros MX para los dominios protegidos por la solución, es posible asegurar la entrega de correo a la organización restringiendo la entrega de correo a los servidores protegidos por Email Protection únicamente desde las IPs de la nube de Panda Security. Los rangos de IPs que entregarán correo entrante a su organización serán:

- 188.94.13.128/25
- 92.54.22.0/24
- 92.54.27.0/24

El rango de direccionamiento especificado en este documento puede variar. El rango de direccionamiento actualizado está reflejado en su consola de gestión bajo la sección Manuales, Información de Configuración. Esto puede hacerse a nivel del firewall perimetral de la organización o restringiendo la entrega de correo en el servidor de correo.

4.3. Configuración de filtrado de correo saliente con Email Protection

Una vez realizada la configuración de correo entrante, la solución Email Protection puede configurarse para realizar el filtrado de correo saliente de la organización. Este paso es opcional e independiente del correo entrante. No obstante, para la realización correcta de filtrado de correo saliente, se deben haber seguido los pasos de configuración referentes a configuración de dominios y de usuarios descritas con anterioridad.

Para configurar el correo saliente a través de la plataforma Email Protection, se debe de configurar un 'Smart Host' en el servidor de correo de la empresa para que todo el correo sea entregado a la nube de Panda Security. Nuestro sistema procesará el correo saliente, lo filtrará y en caso de tratarse de un correo legítimo, procederá a su entrega a los servidores de correo destino. Consulta la documentación del servidor de correo para obtener más información de configuración de un relay de correo saliente.

A la hora de configurar nuestro sistema de filtrado como 'Smart Host', se debe de utilizar el siguiente nombre de servicio: *smtp.mep.pandasecurity.com*

> ***La configuración del host de servicio a utilizar para envío de correo saliente puede variar respecto al indicado en este documento. El Smart Host que debe ser utilizado en su cuenta aparece reflejado en la consola de administración bajo la sección Manuales, Información de Configuración. Por favor, revisa esta sección antes de aplicar los cambios pertinentes en su servicio de correo electrónico.***

Al realizar la configuración, se debe de configurar nuestro Smart Host con una sesión SMTP autenticada. Utiliza las mismas credenciales (usuario y password) que te han sido proporcionadas para acceder a la consola de administración situada en https://mep.pandasecurity.com/admin/)

4.4. Configuración de registros SPF en su DNS

Tanto si se ha configurado el correo saliente a través de la plataforma Email Protection como si se ha configurado únicamente el servicio para el filtrado de correo entrante a su organización, Panda Security recomienda modificar los registros SPF de sus dominios para incluir el rango de direccionamiento de nuestros centros de datos. En caso de tener correo saliente a través de Panda Security, esta modificación debe llevarse a cabo para evitar que servidores de correo destino rechacen el correo proveniente de la nube de Panda Security tras ser filtrado. Para ello, hay que añadir los siguientes rangos de direcciones IP:

- ip4:188.94.13.128/25
- ip4:92.54.22.0/24
- ip4:92.54.27.0/24

El rango de direccionamiento SPF especificado en este documento puede variar. Por favor, revisa el rango que le corresponde a tu cuenta en la consola de administración bajo en la sección Manuales, Información de Configuración antes de realizar cambios en el servicio de DNS.

Un ejemplo de registro SPF asociado a uno de los dominios sería como sigue: *"v=spf1 ip4:188.94.13.128/25 ip4:92.54.22.0/24 ip4:92.54.27.0/24 ip4: [OTHER CUSTOMER IP ADDRESSES] ~all"*

Se recomienda incluir el rango de direccionamiento de la nube de Panda Security a los registros actuales en el DNS.

5. Información adicional y contacto

Puedes encontrar más información sobre las opciones de configuración y filtrado de nuestro producto en los siguientes enlaces:

- Documentación del panel de administración de Empresa: https://mep.pandasecurity.com/download/manual/es/corp.pdf
- Documentación del panel de administración de Usuario Final: https://mep.pandasecurity.com/download/manual/es/user.pdf

En caso de requerir asistencia técnica, puedes contactar con el área de preventa técnica en: customer.service@pandasecurity.com

Email Protection