

Acronis

PRODUCTO #5

EMAIL

SECURITY



Acronis
EMAIL SECURITY
GOOGLE
WORKSPACE



Requisitos previos

Antes de continuar con la configuración, verifique que ha leído y comprende la siguiente información

Licencias necesarias

Se requiere una licencia de seguridad avanzada del correo electrónico para habilitar la funcionalidad en Acronis Cyber Protect.

La seguridad avanzada de correo electrónico se licencia mediante el buzón de correo. No se cobra por los buzones de correo compartidos.

Privilegios de usuario necesarios

Los usuarios con rol de administrador de empresa o de administrador de protección pueden gestionar la seguridad avanzada del correo electrónico. Otros roles de usuario no tienen acceso a él.

Información general sobre la configuración

Para habilitar la seguridad avanzada de correo electrónico con Perception Point, debe seguir estos pasos.

1. Proporcione y vuelva a configurar los registros MX.
2. Añada las direcciones IP de Perception Point a la lista de direcciones IP seguras en la configuración de su servidor de correo electrónico.
3. Configure el correo electrónico y Perception Point para habilitar la solución.
4. Habilite la seguridad avanzada de correo electrónico en el portal de administración de Acronis Cyber Cloud.

Información general del proceso de incorporación

1. Habilite la seguridad avanzada de correo electrónico en el portal de administración de un inquilino específico
2. Compruebe que la persona que va a gestionar la seguridad avanzada de correo electrónico para el inquilino tenga derechos de administrador empresarial o de protección.
3. Abra la consola de servicio de Acronis Cyber Cloud, acceda a seguridad de correo electrónico y siga las instrucciones que se muestren en pantalla.

Configurar el registro MX

Configurar el registro MX

En el proveedor de red, cambie el registro MX a:

- Para ubicaciones de EE. UU.: inbound-smtp.us-east-1.amazonaws.com
- Para ubicaciones de la UE: inbound-smtp.eu-west-1.amazonaws.com

Verifique su dominio en Perception Point

1. Copie el valor del registro TXT en la sección de configuración de su cuenta.
2. Diríjase a su proveedor de red y añada el registro TXT.

Nota

Al añadir un registro es posible que pasen hasta 72 horas para que el proveedor de red aplique el cambio. Contacte con support@perception-point.io cuando se haya añadido el registro.

3. En la sección **Configuración**, localice la fila **Verificación de registro TXT** y haga clic en **Verificar** en la derecha.

TXT RECORD NAME	amazonses.amazonaws.com
TXT RECORD VALUE	amazonses.amazonaws.com
TXT RECORD VERIFICATION	🕒 PENDING... ✓ VERIFY
SMTP PORT	25
SMTP SERVERS	amazonses.amazonaws.com

En esta sección

- › Resolución de problemas de verificación de dominio en Perception Point

Verifique su dominio en Perception Point > Resolución de problemas de verificación de dominio en Perception Point

Resolución de problemas de verificación de dominio en Perception Point

Al añadir un registro es posible que pasen hasta 72 horas para que el proveedor de red aplique el cambio. Si el estado de verificación del dominio sigue pendiente después de eso, pruebe lo siguiente.

- Compruebe si el TXT aparece como registro público en <https://mxtoolbox.com/TXTLookup.aspx>.
 - Si no aparece, compruebe si el registro incluye un nombre de dominio duplicado. Por ejemplo, la unidad `_amazonses[.]yourdomain[.]com[.]yourdomain[.]com`. Si está duplicado, modifique el nombre del registro TXT a `_amazonses` y vuelva a enviarlo a su proveedor de servicio.
- Verifique que el valor y el nombre de registro coinciden con el de Perception Point.
- En la sección **Configuración**, localice **TXT Record Verification** y haga clic en **Verificar** en la derecha. Puede continuar una vez que el estado cambie de **Pendiente** a **Verificar**.

TXT RECORD NAME	<code>_amazonses[.]yourdomain[.]com</code>	
TXT RECORD VALUE	<code>"v=spf1 include:_amazonses[.]yourdomain[.]com ~all" [.]yourdomain[.]com</code>	
TXT RECORD VERIFICATION	🕒 PENDING...	✓ VERIFY
SMTP PORT	25	
SMTP SERVERS	<code>[.]yourdomain[.]com [.]yourdomain[.]com</code>	✎ EDIT

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Cree un grupo de G-suite y configure un servidor

Debe configurar un servidor de escaneo de Perception Point al que se dirigirán los correos electrónicos.

1. Vaya a admin.google.com > **aplicaciones** > **Google Workspace** > **Gmail** > **servidores**.
2. Haga clic en **añadir ruta**.
 - **Nombre:** Análisis de Perception Point
 - **Nombre del servidor:**
 - Para ubicaciones de EE. UU.: `inbound-smtp.us-east-1.amazonaws.com`
 - Para ubicaciones de la UE: `inbound-smtp.eu-west-1.amazonaws.com`
 - Borre la opción **realizar búsqueda MX en el servidor**.
 - Verifique que se ha seleccionado **Solicitar transporte seguro (TLS)**.
 - Verifique que se ha seleccionado **Solicitar certificado CA firmado**.

La configuración debería tener el siguiente aspecto.

Edit mail route ✕

[Help](#)

Perception Point Scanner

1. Specify email server

Single host ▾

inbound-smtp.us-east-1.amazonav : 25 ⓘ

2. Options

- Perform MX lookup on host
- Require secure transport (TLS)
- Require CA signed certificate

[CANCEL](#) [SAVE](#)

3. Haga clic en **Guardar**.

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Dirige correos electrónicos entrantes a Perception Point

1. Vaya a admin.google.com > **aplicaciones** > **Google Workspace** > **Gmail** > **Cumplimiento normativo**.
2. Desplácese hasta Cumplimiento normativo y haga clic en Configurar.
Si ya tiene una norma de cumplimiento normativo de contenido, haga clic en **añadir otra**.
 - **Nombre (descripción corta):** Regla de redirección de Perception Point
 - **Mensajes de correo electrónico afectados:**
 - Seleccionar entrada
 - Seleccionar interno: recibiendo
3. En **Añadir expresiones que describen el contenido que desea buscar en cada mensaje**
 - Elija en la primera lista desplegable: «Si TODOS estos coinciden con el mensaje»
 - Haga clic en **añadir**
 - Coincidencia de contenido avanzada
 - **Ubicación:** Encabezado + Cuerpo
 - **Tipo de coincidencia:** No contiene texto
 - **Contenido:** X-PERCEPTION-POINT-ROUTING: AQWEDSFQ
Perception Point genera el campo Contenido: para cada organización por separado.
4. En **Hacer lo siguiente si las expresiones coinciden:** seleccione **modificar mensaje**.
5. Seleccione **Añadir X-Gm-Original-al encabezado** y **Añadir encabezados X-Gm-Spam y X-Gm-Phishy**.
6. Seleccione **Añadir encabezados personalizados** y añada el valor del **Contenido** generado anteriormente.
 - **Encabezado:** X-PERCEPTION-POINT-ROUTING
 - **Valor:** AQWEDSFQ

7. Seleccione **Cambiar ruta**, y, de forma opcional, **Redirigir también el correo no deseado**.
8. Seleccione desde el menú desplegable **Análisis de Perception Point**.
9. En la parte inferior del diálogo, haga clic en **mostrar opciones**.
 - a. En **filtro de sobre**, seleccione **afectar solo a destinatarios específicos del sobre** e introduzca su dominio o grupo de correos electrónicos concreto.
10. Haga clic en **Añadir configuración**.
11. Haga clic en **Guardar**.

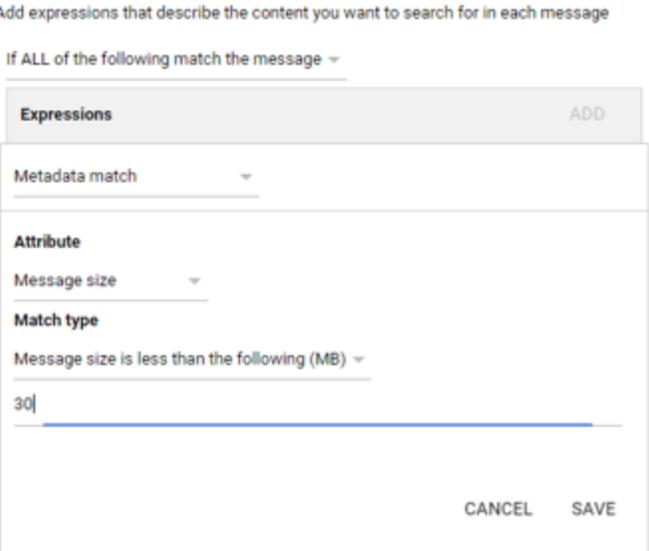
Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Configurar los límites de tamaño del correo electrónico en G Suite

1. Vaya a admin.google.com > **aplicaciones** > **Google Workspace** > **Gmail** > **Cumplimiento normativo**.
2. En Cumplimiento normativo de contenido, edite la sección de **expresiones** y añada una nueva:
 - Coincidencia de metadatos
 - **Atributo:** Tamaño del mensaje
 - **Tipo de coincidencia:** El tamaño del mensaje es inferior al siguiente (MB)
 - **30**

La configuración debería tener el siguiente aspecto:



2. Add expressions that describe the content you want to search for in each message

If ALL of the following match the message ▾

Expressions ADD

Metadata match ▾

Attribute

Message size ▾

Match type

Message size is less than the following (MB) ▾

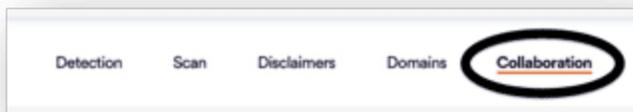
30|

CANCEL SAVE

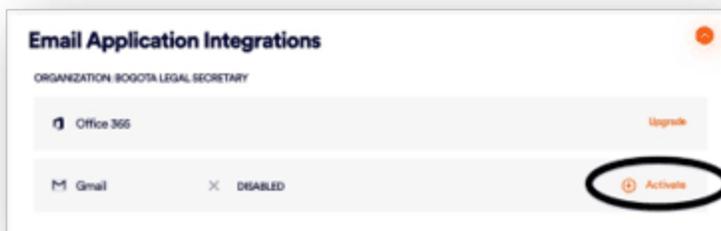
3. Guarde los cambios.

Active la aplicación de remedio de Microsoft 365

1. Inicie sesión en su cuenta de Perception Point X-Ray xray.perception-point.io.
2. En la parte superior derecha, vaya a su nombre de usuario y seleccione **Configuración > Colaboración**.



3. En **Integraciones de aplicación de correo electrónico > Gmail** haga clic en **Activar**.



Se abrirá una nueva pestaña en el navegador solicitando que inicie sesión en Gmail.

4. Use las credenciales de un administrador global para iniciar sesión, revisar los permisos solicitados y aprobar.

Acronis

**EMAIL
SECURITY M365**



Requisitos previos

Antes de continuar con la configuración, verifique que ha leído y comprende la siguiente información

Licencias necesarias

Se requiere una licencia de seguridad avanzada del correo electrónico para habilitar la funcionalidad en Acronis Cyber Protect.

La seguridad avanzada de correo electrónico se licencia mediante el buzón de correo. No se cobra por los buzones de correo compartidos.

Privilegios de usuario necesarios

Los usuarios con rol de administrador de empresa o de administrador de protección pueden gestionar la seguridad avanzada del correo electrónico. Otros roles de usuario no tienen acceso a él.

Información general sobre la configuración

Para habilitar la seguridad avanzada de correo electrónico con Perception Point, debe seguir estos pasos.

1. Proporcione y vuelva a configurar los registros MX.
2. Añada las direcciones IP de Perception Point a la lista de direcciones IP seguras en la configuración de su servidor de correo electrónico.
3. Configure el correo electrónico y Perception Point para habilitar la solución.
4. Habilite la seguridad avanzada de correo electrónico en el portal de administración de Acronis Cyber Cloud.

Información general del proceso de incorporación

1. Habilite la seguridad avanzada de correo electrónico en el portal de administración de un inquilino específico
2. Compruebe que la persona que va a gestionar la seguridad avanzada de correo electrónico para el inquilino tenga derechos de administrador empresarial o de protección.
3. Abra la consola de servicio de Acronis Cyber Cloud, acceda a seguridad de correo electrónico y siga las instrucciones que se muestren en pantalla.

Configurar el registro MX

Configurar el registro MX

En el proveedor de red, cambie el registro MX a:

- Para ubicaciones de EE. UU.: inbound-smtp.us-east-1.amazonaws.com
- Para ubicaciones de la UE: inbound-smtp.eu-west-1.amazonaws.com

Verifique su dominio en Perception Point

1. Copie el valor del registro TXT en la sección de configuración de su cuenta.
2. Diríjase a su proveedor de red y añada el registro TXT.

Nota

Al añadir un registro es posible que pasen hasta 72 horas para que el proveedor de red aplique el cambio. Contacte con support@perception-point.io cuando se haya añadido el registro.

3. En la sección **Configuración**, localice la fila **Verificación de registro TXT** y haga clic en **Verificar** en la derecha.

TXT RECORD NAME	amazonses.com	
TXT RECORD VALUE	amazonses.com	
TXT RECORD VERIFICATION	PENDING...	✓ VERIFY
SMTP PORT	25	
SMTP SERVERS	amazonses.com	✎ EDIT

En esta sección

- › Resolución de problemas de verificación de dominio en Perception Point

Verifique su dominio en Perception Point > Resolución de problemas de verificación de dominio en Perception Point

Resolución de problemas de verificación de dominio en Perception Point

Al añadir un registro es posible que pasen hasta 72 horas para que el proveedor de red aplique el cambio. Si el estado de verificación del dominio sigue pendiente después de eso, pruebe lo siguiente.

- Compruebe si el TXT aparece como registro público en <https://mxtoolbox.com/TXTLookup.aspx>.
 - Si no aparece, compruebe si el registro incluye un nombre de dominio duplicado. Por ejemplo, la unidad `_amazonses[.]yourdomain[.]com[.]yourdomain[.]com`. Si está duplicado, modifique el nombre del registro TXT a `_amazonses` y vuelva a enviarlo a su proveedor de servicio.
- Verifique que el valor y el nombre de registro coinciden con el de Perception Point.
- En la sección **Configuración**, localice **TXT Record Verification** y haga clic en **Verificar** en la derecha. Puede continuar una vez que el estado cambie de **Pendiente** a **Verificar**.

TXT RECORD NAME	<code>_amazonses[.]yourdomain[.]com</code>	
TXT RECORD VALUE	<code>"v=spf1 include:_amazonses[.]yourdomain[.]com ~all" [.]yourdomain[.]com</code>	
TXT RECORD VERIFICATION	⌚ PENDING...	✓ VERIFY
SMTP PORT	25	
SMTP SERVERS	<code>[.]yourdomain[.]com [.]yourdomain[.]com</code>	✎ EDIT

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Añadir a la lista de direcciones IP seguras aquellas que usa Perception Point

1. Vaya a Administrador de Exchange > **Protección** > **Filtro de conexión** > **Editar opciones predeterminadas** > **Direcciones IP permitidas**.
2. Dependiendo de su ubicación, añada las siguientes direcciones IP a la lista **Direcciones IP permitidas**.

Para ubicaciones de EE. UU.	Para ubicaciones de la UE
<ul style="list-style-type: none">• 3.81.182.154	99.81.216.78
<ul style="list-style-type: none">• 3.93.155.149	<ul style="list-style-type: none">• 34.249.190.60
<ul style="list-style-type: none">• 3.95.118.12	<ul style="list-style-type: none">• 108.128.137.108
<ul style="list-style-type: none">• 3.95.142.181	<ul style="list-style-type: none">• 99.80.189.20
<ul style="list-style-type: none">• 54.227.64.76	

3. Seleccione **Habilitar lista de direcciones IP seguras** y haga clic en **Guardar**.

Office 365 Admin <https://outlook.office365.com/epc/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=7b2c2986-28d8-2306-dd67-0...>

Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection**
- advanced threats
- mail flow
- mobile
- public folders
- unified messaging
- hybrid

Default

general

▶ connection filtering

IP Allow list
Always accept messages from the following IP addresses.

+ ✎ -

Allowed IP Address
54.204.57.41
34.192.31.89
34.192.37.108
54.77.126.91/32

IP Block list
Always block messages from the following IP addresses.

+ ✎ -

Blocked IP Address

Enable safe list

Save Cancel

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Crear un conector desde Microsoft 365 hasta Perception Point

1. Administrador de Exchange → flujo de correo → conectores → <crear nuevo conector>
 - **De:** Office 365
 - **Para:** Organización del partner
 - **Nombre:** Análisis de Perception Point
2. Seleccione **Solo cuando tenga una regla de transporte configurada que redirija los mensajes a este conector.**
3. Seleccione **Enrutar correos electrónicos a través de los servidores inteligentes** y añada el siguiente SES FQDN de Amazon dependiendo de su ubicación:
 - Para ubicaciones de EE. UU.: `inbound-smtp.us-east-1.amazonaws.com`
 - Para ubicaciones de la UE: `inbound-smtp.eu-west-1.amazonaws.com`
4. Deje la configuración TLS predeterminada.
5. Use el siguiente correo electrónico en la pantalla de validación:
`noreply@perception-point.io`
6. Haga clic en **Guardar**.

La siguiente imagen muestra el resultado esperado.

Exchange admin center

dashboard recipients permissions compliance management organization protection advanced threats **mail flow** mobile public folders unified messaging hybrid

rules message trace url trace accepted domains remote domains **connectors**

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?ActivityCorrelationID=...

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:

To:

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For outbound email, it refers to...

Next Cancel

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Crear un conector desde Microsoft 365 hasta Perception Point

1. Administrador de Exchange → flujo de correo → conectores → <crear nuevo conector>
 - **De:** Office 365
 - **Para:** Organización del partner
 - **Nombre:** Análisis de Perception Point
2. Seleccione **Solo cuando tenga una regla de transporte configurada que redirija los mensajes a este conector.**
3. Seleccione **Enrutar correos electrónicos a través de los servidores inteligentes** y añada el siguiente SES FQDN de Amazon dependiendo de su ubicación:
 - Para ubicaciones de EE. UU.: `inbound-smtp.us-east-1.amazonaws.com`
 - Para ubicaciones de la UE: `inbound-smtp.eu-west-1.amazonaws.com`
4. Deje la configuración TLS predeterminada.
5. Use el siguiente correo electrónico en la pantalla de validación:
`noreply@perception-point.io`
6. Haga clic en **Guardar**.

La siguiente imagen muestra el resultado esperado.

Exchange admin center

dashboard recipients permissions compliance management organization protection advanced threats **mail flow** mobile public folders unified messaging hybrid

rules message trace url trace accepted domains remote domains **connectors**

New Connector - Google Chrome

Secure | https://outlook.office365.com/ep/Connectors/ConnectorSelection.aspx?ActivityCorrelationID=...

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector. [Learn more](#)

From:

To:

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For outbound email, it refers to...

Next Cancel

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

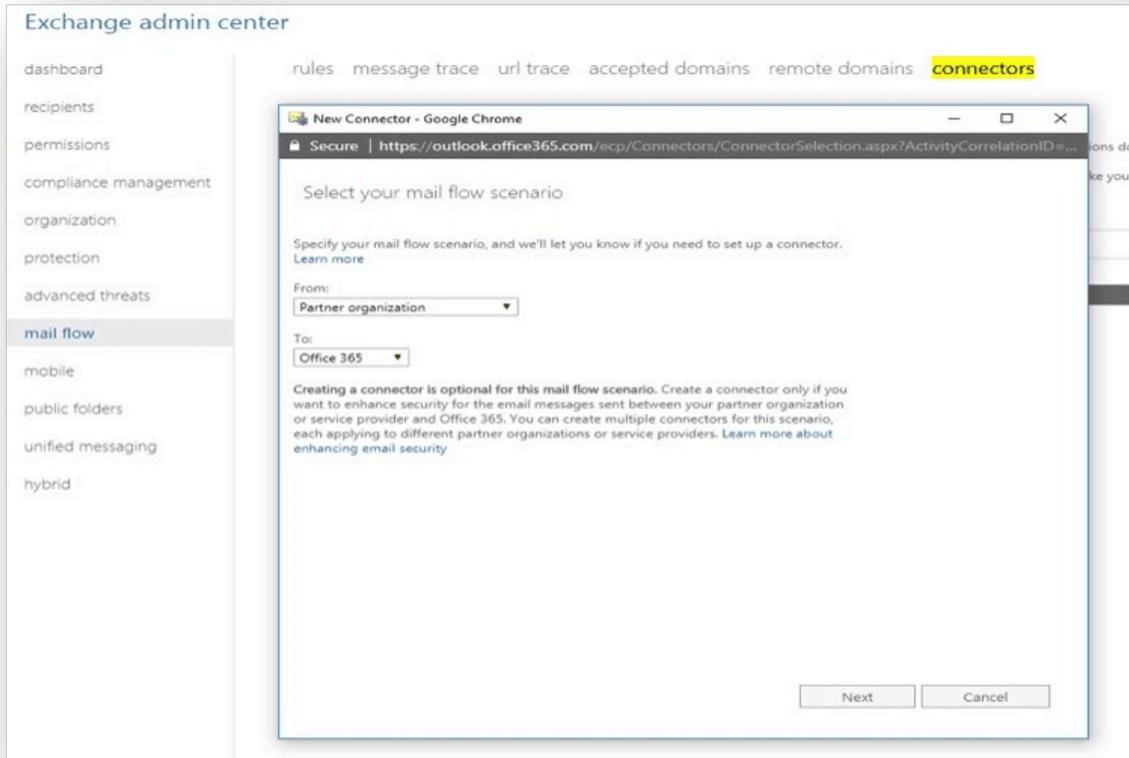
Crear un conector desde Perception Point hasta Microsoft 365

1. Administrador de Exchange → flujo de correo → conectores → <crear nuevo conector>
 - **De:** Office 365
 - **Para:** Organización del partner
 - **Nombre:** Desactive la limitación de IP desde el conector de Perception Point
2. Seleccione **Usar la dirección IP del remitente** y añada las siguientes direcciones IP dependiendo de su ubicación:

Para ubicaciones de EE. UU.	Para ubicaciones de la UE
<ul style="list-style-type: none">• 3.81.182.154• 3.93.155.149• 3.95.118.12• 3.95.142.181• 54.227.64.76	<ul style="list-style-type: none">• 99.81.216.78• 34.249.190.60• 108.128.137.108• 99.80.189.20

3. Deje la configuración TLS predeterminada.
4. Haga clic en **Guardar**.

La siguiente imagen muestra el resultado esperado.



Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Crear una regla de enrutamiento en Microsoft 365

1. En **Administrador de Exchange > Flujo de correo > Reglas > Crear una nueva regla**.
2. En la parte inferior del diálogo, haga clic en **Más opciones**.
3. En **Nombre**, escriba Regla de redirección de Perception Point.
4. Seleccione **Aplicar esta regla si**.
5. Seleccione **El destinatario es > El dominio es**.
6. Añada todos los usuarios, grupos o dominios que quiera enrutar a través de Perception Point.
7. Haga clic en **Añadir condición**.
8. Seleccione **El remitente > es externo/interno**.
9. Seleccione **Fuera de la organización**.
10. Seleccione **Hacer lo siguiente > Redirigir el mensaje a > El siguiente conector > seleccione el conector de Perception Point que ha creado**.
11. Seleccione **Excepto si > Añadir excepción > El remitente... > Tiene la dirección IP en alguno de estos intervalos o coincide por completo con ellos**:

Para ubicaciones de EE. UU.	Para ubicaciones de la UE
<ul style="list-style-type: none">• 3.81.182.154	99.81.216.78
<ul style="list-style-type: none">• 3.93.155.149	<ul style="list-style-type: none">• 34.249.190.60
<ul style="list-style-type: none">• 3.95.118.12	<ul style="list-style-type: none">• 108.128.137.108
<ul style="list-style-type: none">• 3.95.142.181	<ul style="list-style-type: none">• 99.80.189.20
<ul style="list-style-type: none">• 54.227.64.76	

12. Seleccione **Añadir excepción > El mensaje... > tiene un tamaño mayor o igual a > añada un tamaño límite de 30 000 KB**.

13. La regla de enrutamiento debe tener la menor prioridad de todas
 - a. Para las reglas de bloqueo existentes, establezca «Dejar de procesar más reglas».
 - b. Para las reglas de exención de responsabilidad existentes, añada una excepción para introducir las direcciones IP de Perception Point en la lista blanca.
 - c. Para las reglas de bloqueo de uso de IP existentes, establezca «Dejar de procesar más reglas».

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Crear una regla para spam de confianza alta en Microsoft 365

1. En **Administrador de Exchange > Flujo de correo > Reglas > Crear una nueva regla**.
2. En la parte inferior del diálogo, haga clic en **Más opciones**.
3. En **Nombre**, escriba **Enviar los correos electrónicos de spam de Office 365 a la carpeta de correo no deseado (Alta)**.
4. Seleccione **Aplicar esta regla si**:
 - a. Seleccione **Coincide un encabezado de mensaje**
 - b. El encabezado **X-PP-Forefront-Antispam-Report** coincide con **SCL:9, SCL:8, SCL:7**
5. Seleccione **Hacer lo siguiente > Modificar Propiedades del mensaje > Establecer el nivel de confianza de spam (SCL) en > 9**.

Rule - Google Chrome

https://outlook.office365.com/ecp/RulesEditor/EditTransportRule.aspx?ActivityCorrelationID=994b4d2a-d216-0806-6bc3-19290a2...

Send Office365 spam emails to junk folder

Name:
Send Office365 spam emails to junk folder (High)

*Apply this rule if...
A message header matches...

add condition

*Do the following...
Set the spam confidence level (SCL) to...

add action

Except if...
add exception

Save Cancel

'X-PP-Forefront-Antispam-Report' header matches **'SCL:9'** or **'SCL:8'** or **'SCL:7'**

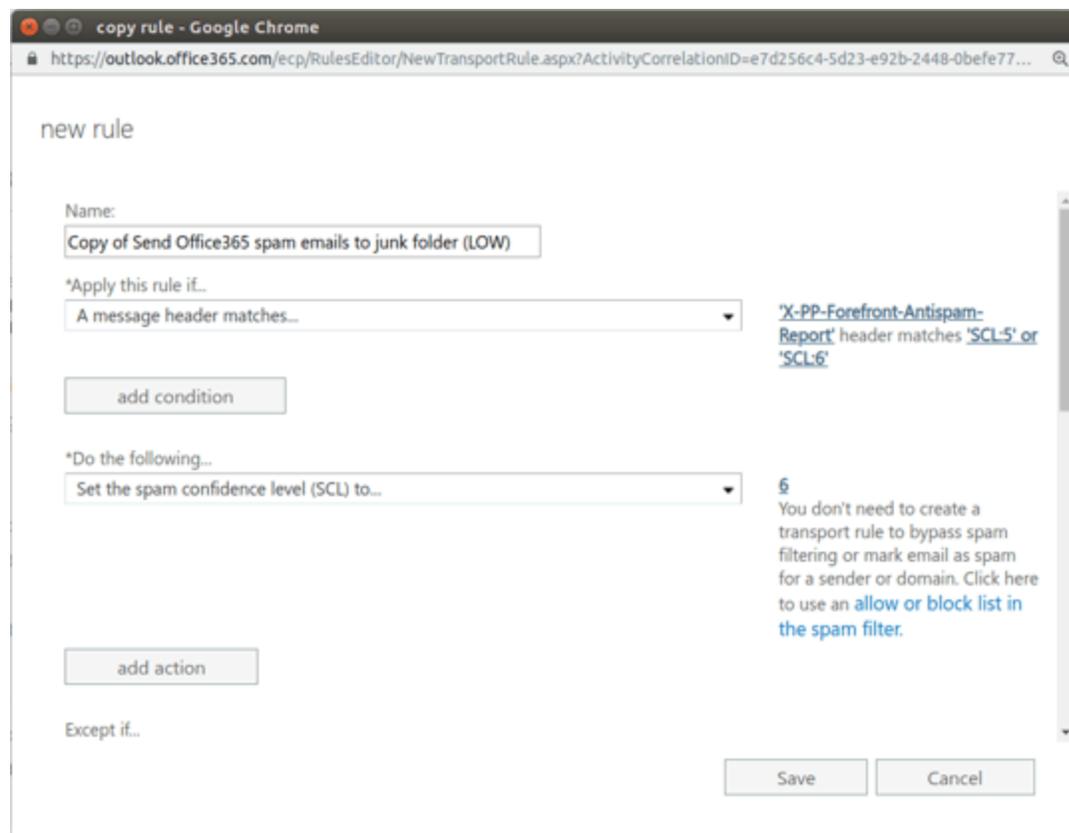
9
You don't need to create a transport rule to bypass spam filtering or mark email as spam for a sender or domain. Click here to use an [allow or block list in the spam filter](#).

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021

Crear una regla para spam de confianza baja en Microsoft 365

1. En **Administrador de Exchange** > **Flujo de correo** > **Reglas** > **Crear una nueva regla**.
2. En la parte inferior del diálogo, haga clic en **Más opciones**.
3. En **Nombre**, escriba **Enviar los correos electrónicos de spam de Office 365 a la carpeta de correo no deseado (Baja)**.
4. Seleccione **Aplicar esta regla si**:
 - a. Seleccione **Coincide un encabezado de mensaje**
 - b. El encabezado **X-PP-Forefront-Antispam-Report** coincide con **SCL:6, SCL:5**
5. Seleccione **Hacer lo siguiente** > **Modificar Propiedades del mensaje** > **Establecer el nivel de confianza de spam (SCL) en** > **6**.



Crear una regla de spam para correos electrónicos de spam en Microsoft 365

1. En **Administrador de Exchange > Flujo de correo > Reglas > Crear una nueva regla**.
2. En la parte inferior del diálogo, haga clic en **Más opciones**.
3. En **Nombre**, escriba **Regla de spam de Perception Point**.
4. Seleccione **Aplicar esta regla si**
 - a. Seleccione **Coincide un encabezado de mensaje**
 - b. **Coincide con estos modelos exactos**
 - i. Seleccione **Introducir texto** > escriba **X-PERCEPTION-POINT-SPAM**
 - ii. Seleccione **Introducir modelos de texto** > escriba **FAIL**
5. Seleccione **Hacer lo siguiente > Modificar Propiedades del mensaje > Establecer el nivel de confianza de spam (SCL) en > 6**.

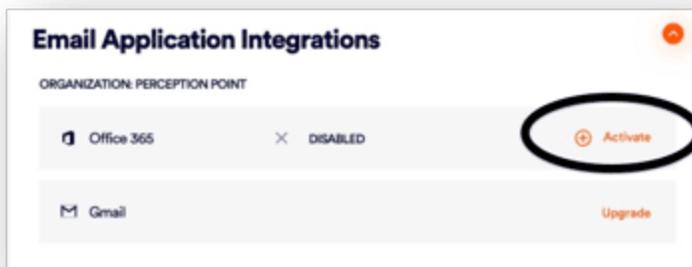
Se enviará el spam a la carpeta de correo no deseado del usuario.

Active la aplicación de remedio de Microsoft 365

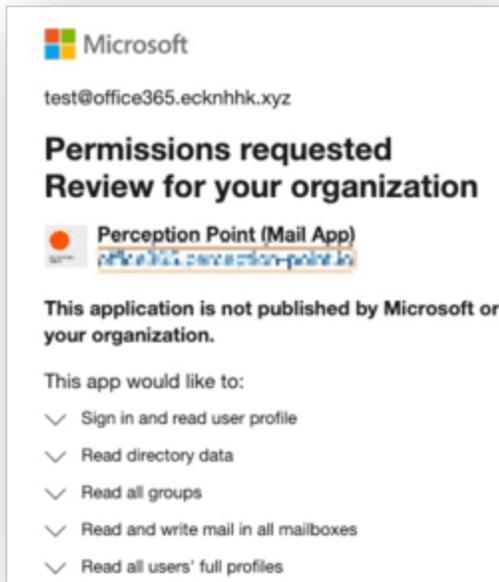
1. Inicie sesión en su cuenta de Perception Point X-Ray xray.perception-point.io.
2. En la parte superior derecha, vaya a su nombre de usuario y seleccione **Configuración > Colaboración**.



3. En **Integraciones de aplicación de correo electrónico > Office 365** haga clic en **Activar**.



Se abrirá una nueva pestaña en el navegador solicitando que inicie sesión en Office 365.



4. Use las credenciales de un administrador global para iniciar sesión, revisar los permisos solicitados y aprobar.

Última fecha de revisión del tema: martes, 28 de septiembre de 2021

Ayuda web para Acronis Cyber Cloud. © Acronis International GmbH, 2003-2021