



Guía del producto

McAfee Security for Microsoft Exchange 8.6.0

## **COPYRIGHT**

Copyright © 2017 McAfee LLC

## **ATRIBUCIONES DE MARCAS COMERCIALES**

McAfee y el logotipo de McAfee, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, Foundstone, McAfee LiveSafe, McAfee QuickClean, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, TrustedSource y VirusScan son marcas comerciales de McAfee LLC o sus filiales en EE. UU. y otros países. Otros nombres y marcas pueden ser reclamados como propiedad de terceros.

## **INFORMACIÓN DE LICENCIA**

### **Acuerdo de licencia**

AVISO A TODOS LOS USUARIOS: LEA ATENTAMENTE EL ACUERDO LEGAL PERTINENTE CORRESPONDIENTE A LA LICENCIA QUE HAYA ADQUIRIDO, EN EL QUE SE ESTABLECEN LOS TÉRMINOS Y LAS CONDICIONES GENERALES DE APLICACIÓN AL USO DEL SOFTWARE CUYA LICENCIA SE CONCEDE. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS RELATIVOS A LA VENTA, ASÍ COMO OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑEN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (TALES COMO UN FOLLETO, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DISPONIBLE EN EL SITIO WEB DESDE EL QUE HAYA DESCARGADO EL PAQUETE DE SOFTWARE). SI NO ACEPTA TODOS LOS TÉRMINOS ESTABLECIDOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDE, PUEDE DEVOLVER EL PRODUCTO A MCAFEE O AL PUNTO DE VENTA PARA OBTENER EL REEMBOLSO ÍNTEGRO DE SU IMPORTE.

# Contenido

<b>1</b>	<b>Introducción</b>	<b>7</b>
	Funciones del producto . . . . .	7
	Por qué necesita MSME . . . . .	10
	Amenazas para su organización . . . . .	10
	Cómo MSME protege su Exchange Server . . . . .	11
	Análisis de correos electrónicos . . . . .	13
	Análisis de correo electrónico entrante . . . . .	13
	Análisis de correos electrónicos salientes . . . . .	14
	Análisis de correos electrónicos internos . . . . .	15
<b>2</b>	<b>Panel</b>	<b>17</b>
	Información estadística de los elementos detectados . . . . .	17
	Detecciones . . . . .	18
	Programación de una actualización de software . . . . .	22
	Análisis bajo demanda y sus vistas . . . . .	23
	Vista de tareas de análisis bajo demanda . . . . .	24
	Creación de una tarea de análisis bajo demanda . . . . .	25
	Informes de estado . . . . .	27
	Vista de tareas de informe de estado . . . . .	27
	Programación de un nuevo informe de estado . . . . .	28
	Notificaciones por correo electrónico de informes de estado . . . . .	30
	Informes de configuración . . . . .	31
	Vista de tareas del informe de configuración . . . . .	31
	Programación de un nuevo informe de configuración . . . . .	32
	Notificaciones por correo electrónico del informe de configuración . . . . .	33
	Informes gráficos . . . . .	34
	Vista de informes gráficos mediante filtros de búsqueda simple . . . . .	34
	Utilización de filtros de búsqueda avanzados . . . . .	35
<b>3</b>	<b>Elementos detectados</b>	<b>39</b>
	Administración de datos en cuarentena . . . . .	39
	Tipos de detección . . . . .	40
	Filtros de búsqueda principales disponibles . . . . .	42
	Cuadro comparativo sobre filtros de búsqueda . . . . .	45
	Opciones adicionales de búsqueda . . . . .	46
	Búsqueda de elementos detectados . . . . .	47
	Acciones que puede realizar con los elementos en cuarentena . . . . .	48
<b>4</b>	<b>Administrador de directivas</b>	<b>51</b>
	Categorías de directivas para gestionar amenazas . . . . .	52
	Vistas del Administrador de directivas . . . . .	52
	Directiva principal y secundaria . . . . .	53
	Creación de directivas secundarias . . . . .	54
	Analizadores y filtros principales . . . . .	55
	Cuadro comparativo sobre analizadores y filtros . . . . .	57

Lista de todos los analizadores y filtros de una directiva seleccionada . . . . .	59
Adición de un analizador o un filtro . . . . .	60
Creación de nuevas reglas para usuarios específicos . . . . .	60
Acciones que puede realizar en las detecciones . . . . .	61
Recurso compartido . . . . .	63
Configurar opciones de análisis . . . . .	63
Configuración de opciones de alerta . . . . .	64
Crear una alerta . . . . .	65
Configuración de reglas de conformidad y DLP . . . . .	67
Configuración de reglas de filtrado de archivos . . . . .	70
Configuración de intervalos de tiempo . . . . .	71
Administración de opciones del analizador principal para una directiva . . . . .	72
Configuración del analizador antivirus . . . . .	73
Configuración del analizador de conformidad y DLP . . . . .	76
Configuración de opciones de filtrado de archivos . . . . .	78
Configuración de parámetros de reputación de URL de correo . . . . .	79
Comprobación de reputación de TIE para datos adjuntos de correo electrónico . . . . .	82
Configuración de TIE para analizar los datos adjuntos de correo electrónico . . . . .	84
Configuración de antispam . . . . .	85
Configuración de antiphishing . . . . .	90
Administración de configuraciones de filtros para una directiva . . . . .	91
Configuración de contenido dañado . . . . .	92
Configuración de contenido protegido . . . . .	92
Configuración de contenido cifrado . . . . .	93
Configuración de contenido firmado . . . . .	93
Configuración de archivos protegidos con contraseña . . . . .	94
Configuración del filtrado según tamaño del correo . . . . .	94
Configuración de las opciones de control del analizador . . . . .	96
Bloqueo manual de direcciones IP . . . . .	97
Configuración de correo MIME . . . . .	97
Configuración de archivos HTML . . . . .	99
Administración de configuraciones varias para una directiva . . . . .	100
Configuración de mensajes de alerta . . . . .	101
Configuración del texto de renuncia . . . . .	102

**5 Configuración y diagnósticos 105**

Configuración en tiempo real . . . . .	107
Configuración de API de análisis de virus (VSAPI) de Microsoft . . . . .	109
Configuración de análisis en segundo plano . . . . .	110
Configuración de análisis de transporte . . . . .	111
Configuración bajo demanda . . . . .	111
Configuración de exclusión de buzones de correo . . . . .	113
Ejemplos del uso de caracteres comodín para exclusiones de buzón de correo . . . . .	114
Configuración de notificaciones . . . . .	115
Configuración de las notificaciones . . . . .	115
Edición de la plantilla de notificación . . . . .	116
Campos de notificación que puede usar . . . . .	117
Activación de alertas de estado de funcionamiento del producto . . . . .	118
Configuración de antispam . . . . .	120
Configuración de elementos detectados . . . . .	121
Cómo poner elementos en cuarentena mediante McAfee Quarantine Manager . . . . .	122
Poner elementos en cuarentena mediante la base de datos local . . . . .	123
Configuración de preferencias de interfaz de usuario . . . . .	125
Configuración de las opciones del panel . . . . .	125
Configuración de gráficos y cuadros . . . . .	126
Configuración de diagnósticos . . . . .	126

Configuración de registro de depuración . . . . .	126
Configuración del registro de eventos . . . . .	128
Configuración de las opciones del registro del producto . . . . .	129
Configuración del servicio de informe de errores . . . . .	131
Ver registros del producto . . . . .	131
Configuración de DAT . . . . .	132
Importación y exportación de opciones de configuración . . . . .	133
Exportación de la configuración existente de MSME . . . . .	134
Importación de configuración desde otro servidor de MSME . . . . .	134
Importación de Sitelist . . . . .	135
Configuración de proxy antispam . . . . .	135
<b>6 Mantenimiento del programa</b>	<b>137</b>
Modificación de la instalación . . . . .	137
Restauración de configuraciones predeterminadas . . . . .	138
Purga y optimización . . . . .	138
<b>7 Solución de problemas</b>	<b>139</b>
Configuración predeterminada en comparación con la configuración mejorada . . . . .	139
Claves de registro importantes . . . . .	140
<b>8 Preguntas frecuentes</b>	<b>143</b>
General . . . . .	143
Administrador de directivas . . . . .	144
Configuración y diagnósticos . . . . .	145
Complemento McAfee Anti-Spam . . . . .	146
Expresiones regulares (regex) . . . . .	146
<b>Índice</b>	<b>149</b>



# 1

## Introducción

McAfee® Security for Microsoft Exchange (MSME) protege Microsoft Exchange Server contra diversas amenazas que podrían afectar a equipos, redes o empleados.

MSME usa heurística avanzada contra virus, contenido no deseado, programas potencialmente no deseados y tipos de archivos o mensajes prohibidos. También analiza:

- La línea de asunto y el cuerpo de correos electrónicos
- Datos adjuntos de correos electrónicos (en base al tipo, el nombre y el tipo de archivo)
- Texto en los datos adjuntos de correos electrónicos
- URL en el cuerpo del mensaje de correo electrónico

El software también incluye el complemento McAfee Anti-Spam que protege Exchange Server contra correo electrónico de spam y phishing.

### Contenido

- ▶ *Funciones del producto*
- ▶ *Por qué necesita MSME*
- ▶ *Cómo MSME protege su Exchange Server*
- ▶ *Análisis de correos electrónicos*

---

## Funciones del producto

Las funciones principales de MSME se describen en esta sección.

- **Integración de McAfee® Threat Intelligence Exchange (TIE) para la comprobación de reputación de archivos:** admite la comprobación de reputación de archivos de TIE para los datos adjuntos de correo electrónico. Analiza con rapidez los archivos y toma decisiones informadas mediante la validación de la reputación de archivos en función de la información recibida de diversos orígenes conectados al servidor de TIE en su entorno. Cuando el correo electrónico incluye un archivo comprimido, los archivos que contiene se extraen y los tipos de archivos admitidos se envían para la comprobación de reputación de TIE. Para ver la lista de los archivos comprimidos admitidos, véase [KB89577](#).
- **Comprobación de reputación de archivos de McAfee® Advanced Threat Defense:** MSME ahora admite Advanced Threat Defense, un appliance local que facilita la detección y la prevención de malware a través de TIE. Advanced Threat Defense permite proteger sus sistemas frente a malware conocido, de tipo near-zero day y de tipo zero-day sin poner en riesgo la calidad del servicio para los usuarios de la red.
- **Protección frente a la suplantación de correo electrónico:** protege sus sistemas contra los mensajes de correo electrónico de suplantación.
- **Exclusión de correo electrónico de gran tamaño de los análisis:** ahora es posible excluir los mensajes de correo electrónico de los análisis en tiempo real en función del tamaño.

- **Bloqueo de correo electrónico de direcciones IP específicas:** ahora puede incluir en la lista negra una dirección IP concreta o un intervalo de direcciones IP de forma que no puedan enviar correo electrónico a su organización, independientemente de la calificación de reputación de la dirección IP.
- **Compatibilidad con Microsoft Exchange 2016:** existe compatibilidad con la actualización acumulativa (CU) 3 de Microsoft Exchange 2016 y posteriores.
- **Compatibilidad con Microsoft Windows Server 2016:** existe compatibilidad con el sistema operativo de servidor Microsoft Windows 2016 de 64 bits.
- **Mejoras relacionadas con el navegador:** Microsoft Internet Explorer 11.1066, Mozilla Firefox 54.0.1 y Google Chrome 59.0.3071.115.



Asegúrese de desactivar el bloqueo de ventanas emergentes en la configuración del navegador para acceder a la interfaz web del producto.

## Otras funciones

- **Protección antivirus:** analiza todos los mensajes de correo electrónico en busca de virus y protege a Exchange Server interceptando, limpiando y eliminando los virus detectados. MSME usa métodos heurísticos avanzados e identifica virus desconocidos o elementos sospechosos de ser virus y los bloquea.
- **Protección antispam:** le ayuda a ganar el ancho de banda y el espacio de almacenamiento necesarios para Exchange Server asignando una calificación de spam a cada correo electrónico mientras lo analiza, y realizando acciones preconfiguradas en dichos correos.
- **Protección antiphishing:** detecta correos electrónicos de phishing que intentan obtener información personal de manera fraudulenta.
- **Protección frente a URL maliciosas:** protege el sistema frente a URL maliciosas. Cuando se ha activado, MSME analiza cada URL en el cuerpo del correo electrónico, obtiene la calificación de reputación del vínculo, compara dicha calificación con el umbral definido, y realiza la acción pertinente según la configuración.
- **Capacidad para detectar compresores y programas potencialmente no deseados:** detecta compresores que comprimen y cifran el código original de un archivo ejecutable. También detecta programas potencialmente no deseados (PUP), se trata de programas informáticos escritos por compañías legítimas para alterar el estado de seguridad o privacidad de un equipo.
- **Filtrado de contenido:** analiza el contenido y el texto de la línea de asunto o del cuerpo de un correo electrónico y los datos adjuntos del correo. MSME admite el filtrado de contenido mediante expresiones regulares (regex).
- **Filtrado de archivos:** analiza los datos adjuntos de un correo electrónico dependiendo del nombre, el tipo y el tamaño del archivo de los datos adjuntos. MSME también puede filtrar archivos con contenido cifrado, dañado, protegido con contraseña y con firma digital.
- **Conformidad y DLP:** capacidad para garantizar que el contenido del correo electrónico cumple las directivas de confidencialidad y conformidad de la organización. Entre los diccionarios de conformidad predefinidos se cuentan los siguientes.
  - Adición de 60 nuevos diccionarios de conformidad y DLP
  - Compatibilidad con diccionarios de conformidad específicos del sector, como HIPAA, PCI, código fuente (Java, C++, etc.)
  - Mejoras en detecciones basadas en expresiones existentes.
  - Menor cantidad de falsos positivos debido a mejores capacidades para detectar contenido no conforme, según la calificación de umbral y en combinación con el recuento máximo de términos (ocurrencia).

Personalización de directivas para seguridad de contenido y Data Loss Prevention (DLP).



- **Reputación de IP:** un método para detectar una amenaza en mensajes de correo electrónico según la dirección IP del servidor de envío. La calificación de reputación de IP refleja la posibilidad de que una conexión de red sea una amenaza. La reputación de IP aprovecha McAfee Global Threat Intelligence (GTI) para evitar daños y robo de datos mediante el bloqueo de mensajes de correo electrónico en la gateway según la dirección IP del último servidor de correo electrónico. MSME procesa el mensaje antes de que entre a la organización. Para ello rechaza o desecha la conexión según la calificación de reputación de IP.
- **Análisis bajo demanda avanzado:** capacidad para realizar análisis bajo demanda a nivel granular en Exchange Server 2010 y 2013, lo que genera análisis bajo demanda más rápidos. Puede planificar análisis bajo demanda según estos filtros: Asunto, Datos adjuntos, Remitente/Destinario/CC, Tamaño del correo, ID de mensaje, Elementos no leídos, y Duración.
- **Análisis en segundo plano:** facilita el análisis de todos los archivos del almacén de información. Puede planificar un análisis en segundo plano para analizar periódicamente un conjunto seleccionado de mensajes con las últimas actualizaciones y configuraciones de análisis del motor. En MSME, puede excluir buzones de correo que no desee analizar.
- **Alertas de estado de funcionamiento del producto:** se trata de notificaciones sobre el estado de funcionamiento del producto. Puede configurar y planificar estas alertas.
- **Integración con McAfee ePolicy Orchestrator 5.1.x, 5.3.x y 5.9.x:** la integración con ePolicy Orchestrator 5.1.x, 5.3.x y 5.9.x proporciona un método centralizado para administrar y actualizar MSME en todos los servidores Exchange. Esto reduce la complejidad y el tiempo necesario para administrar y actualizar los diferentes sistemas.
- **Interfaz de usuario basada en la Web:** proporciona una interfaz basada en la Web fácil de usar, basada en DHTML.
- **Administración de directivas:** la opción de menú **Administrador de directivas** en la interfaz de usuario del producto muestra las diferentes directivas que puede configurar y gestionar en MSME.
- **Configuración de analizador centralizado, reglas de filtrado y alertas mejoradas:** mediante analizadores, puede configurar opciones que una directiva aplicará al analizar elementos. Mediante reglas de filtrado de archivos, puede configurar reglas que se aplicarán a un nombre, un tipo y un tamaño de archivo.
- **Análisis y acciones bajo demanda o basadas en el tiempo:** analiza correos electrónicos a horas convenientes o a intervalos regulares.
- **Análisis de Extensiones multipropósito de correo de Internet (MIME, Multipurpose Internet Mail Extensions):** estándar de comunicaciones que le permite transferir formatos no ASCII a protocolos (como SMTP) que admiten solamente caracteres ASCII de 7 bits.
- **Administración de cuarentena:** puede especificar la base de datos local que se utilizará como repositorio para los correos electrónicos infectados en cuarentena. Puede decidir almacenar mensajes en cuarentena en su propio servidor ejecutando McAfee Quarantine Manager, lo cual recibe el nombre de *cuarentena remota*.
- **Actualización automática de definiciones de virus, archivos DAT adicionales, motores antivirus y antisпам:** proporciona regularmente archivos DAT, motores de análisis antivirus y antisпам actualizados, y detecta y limpia las últimas amenazas.
- **Retención y purgado de archivos DAT antiguos:** retenga archivos DAT antiguos durante periodos que defina o púrguelos según sea necesario.
- **Compatibilidad con el Editor de Sitelist:** especifica una ubicación desde la que se descargan las actualizaciones automáticas para MSME.
- **Compatibilidad con Small Business Server:** MSME es compatible con Small Business Server.

- **Informes de detección:** genera informes de estado e informes gráficos que le permiten ver información sobre elementos detectados.
- **Informes de configuración:** resume la configuración del producto, como la información sobre el servidor, la versión, el estado y el tipo de licencia, el producto, el registro de depuración, la configuración en tiempo real, las directivas en tiempo real y las directivas de gateway. Puede especificar cuándo el servidor debe enviar el informe de configuración al administrador.
- **Detección de ataques de denegación de servicio:** detecta solicitudes adicionales o ataques que inundan e interrumpen el tráfico normal en una red. Un ataque de denegación de servicio sobrecarga su objetivo con solicitudes de conexión falsas, de modo que el objetivo ignora las solicitudes legítimas. MSME considera estos tres escenarios como ataques de denegación de servicio:
  - El tiempo de análisis excede el límite definido
  - El nivel anidado excede el nivel definido
  - El límite de tamaño de archivo ampliable excede el tamaño definido
- **Notificaciones avanzadas:** permite reenviar los correos electrónicos en cuarentena para la auditoría de cumplimiento a varios usuarios, según la categoría de detección.
- Compatibilidad con VMware Workstation 7.0 o posterior, así como VMware ESX 5.5.

## Por qué necesita MSME

Su organización es vulnerable a muchas amenazas que pueden comprometer su reputación, empleados, equipos y redes.

- La reputación de una organización puede verse comprometida por pérdida de información confidencial o por un abuso contra el que se puedan tomar medidas legales.
- Las distracciones electrónicas y el uso sin restricciones del correo electrónico e Internet pueden comprometer la productividad de los empleados.
- Los virus y otros softwares potencialmente no deseados pueden dañar los equipos, volviéndolos inservibles.
- El uso incontrolado de diferentes tipos de archivos en redes puede causar problemas en el funcionamiento de toda la organización.

## Amenazas para su organización

Conozca las diferentes amenazas que pueden afectar a una organización.

Tipo de amenaza	Descripción
Reputación de una compañía	Un comentario imprudente o no contrastada de un empleado podría causar problemas legales, a menos que se haga pública una renuncia de responsabilidad legal.
Spam (correo electrónico no solicitado)	Los correos electrónicos comerciales no solicitados son el equivalente electrónico al spam o correo basura. Contienen a menudo anuncios no deseados por los destinatarios. Aunque se trate más de una molestia que de una amenaza, el spam puede afectar al rendimiento de la red.
Mensajes de correo electrónico grandes	Los mensajes de correo electrónico grandes o los mensajes que contienen numerosos datos adjuntos pueden ralentizar el rendimiento de los servidores de correo electrónico.
Virus de envío masivo de correo	Aunque se puedan limpiar como cualquier otro virus, pueden propagarse rápidamente, afectando de inmediato al rendimiento de la red.
Correos electrónicos de origen no deseado	Antiguos empleados descontentos e individuos sin escrúpulos conocedores de las direcciones de correo electrónico de los empleados pueden consternar y distraerlos mediante el envío de correos electrónicos no deseados.

Tipo de amenaza	Descripción
Uso no empresarial del correo electrónico	Si la mayoría de los empleados usan direcciones de correo electrónico de destinatario fuera de la organización, dichos correos electrónicos probablemente sean de uso personal o de uso no empresarial.
Pérdida de información confidencial de la compañía	Los empleados podrían divulgar información confidencial relacionada con productos no lanzados, clientes o socios.
Lenguaje ofensivo	Palabras o expresiones ofensivas pueden aparecer en correos electrónicos y datos adjuntos. Además de ofender, también pueden desencadenar acciones legales.
Transferencia de archivos de entretenimiento	Archivos de vídeo o audio grandes con fines de entretenimiento podrían reducir el rendimiento de la red.
Tipos de archivos ineficaces	Algunos archivos usan una gran cantidad de memoria y pueden ser lentos de transferir, pero a menudo hay alternativas disponibles. Por ejemplo, los archivos GIF y JPEG son mucho más pequeños que los archivos BMP equivalentes.
Transferencia de archivos grandes	La transferencia de archivos grandes puede reducir el rendimiento de la red.
Ataque de denegación de servicio	Una oleada deliberada de archivos grandes puede afectar seriamente al rendimiento de la red, y volverla inservible para sus usuarios legítimos. Al analizar archivos comprimidos de gran tamaño, MSME considera tres parámetros para el ataque de denegación de servicio: <ul style="list-style-type: none"> <li>• El tiempo de análisis para los archivos comprimidos excede el umbral.</li> <li>• Se identifican los niveles anidados de archivos comprimidos. Por ejemplo, un archivo .zip contiene otros archivos comprimidos y continúa ampliándose con más archivos comprimidos.</li> <li>• El límite de tamaño ampliable de los archivos comprimidos excede el umbral.</li> </ul>
Texto pornográfico	No debe usarse lenguaje o términos vulgares en correos electrónicos.
Virus y otros softwares potencialmente no deseados	Los virus y otros softwares potencialmente no deseados pueden volver rápidamente inservibles equipos y datos.
Contenido dañado o cifrado	Este tipo de contenido no puede ser analizado. Hay que especificar las directivas apropiadas para solucionarlo.

## Cómo MSME protege su Exchange Server

Conozca cómo MSME protege su Exchange Server mediante el acceso a mensajes de correo electrónico que llegan a Exchange Server y los correos electrónicos que se leen en el buzón de correo y se escriben allí.

### Protección de Microsoft Exchange Server

MSME utiliza la interfaz de análisis de virus de Exchange Server para obtener acceso total a todos los mensajes de correo electrónico que se leen desde el buzón de correo de Exchange Server y se escriben allí.

- El motor de análisis antivirus compara el correo electrónico con todas las firmas de virus conocidas almacenadas en los archivos DAT.
- El motor de administración de contenido analiza el mensaje de correo electrónico en busca de contenido prohibido según se especifica en las directivas de administración de contenido en MSME.

Si se encuentran virus o contenido prohibido en el mensaje de correo electrónico mediante estas comprobaciones, MSME realiza la acción especificada. Si no se detectan elementos, MSME devuelve la información a la interfaz de análisis de virus para completar la solicitud de mensaje original en Microsoft Exchange.

## Detección en tiempo real

MSME se integra con Exchange Server y funciona en tiempo real para detectar y eliminar virus u otro tipo de código dañino o no deseado. También ayuda a mantener el entorno libre de virus mediante el análisis de las bases de datos de Exchange Server. Cada vez que un correo electrónico se envía a o se recibe desde un punto de origen, MSME analiza dicho correo para compararlo con una lista de virus conocidos y comportamientos sospechosos de ser virus, interceptando y limpiando el archivo infectado antes de que se propague. Además, analiza el contenido del mensaje de correo electrónico (y los datos adjuntos) por medio de reglas y directivas definidas en el software.

## Análisis de correos electrónicos

- Los motores antispam, antivirus y de administración de contenido analizan los correos electrónicos y envían el resultado a MSME antes de que el contenido se escriba en el sistema de archivos o sea leído por los usuarios de Microsoft Exchange.
- Los motores de análisis antivirus y antispam comparan el correo electrónico con todas las firmas conocidas almacenadas en los archivos de definición de virus (DAT) actualmente instalados, y reglas antispam. El motor antivirus también analiza el mensaje mediante métodos de detección heurística seleccionados.
- El motor de administración de contenido analiza el mensaje de correo electrónico en busca de contenido prohibido según se especifica en las directivas de administración de contenido que se ejecutan en el software. Si no hay virus ni contenido prohibido o no deseado en el correo electrónico, MSME devuelve la información a Microsoft Exchange. En caso de detección, MSME realiza acciones según lo definido en sus opciones de configuración.

## ¿Cómo funciona un análisis?

- Los elementos más importantes en MSME son el motor de análisis y los archivos DAT. El motor es un analizador de datos complejos. Los archivos DAT contienen mucha información, incluidos miles de controladores diferentes con instrucciones detalladas sobre cómo identificar un virus o un tipo de virus.
- El motor de análisis trabaja con archivos DAT. Identifica el tipo de elemento analizado y descodifica el contenido del objeto para entender de qué elemento se trata. A continuación, usa la información de los archivos DAT para buscar y localizar virus conocidos. Cada virus tiene una firma distintiva. Hay una secuencia de caracteres únicos a un virus y el motor busca esa firma. El motor usa una técnica llamada análisis heurístico para buscar virus desconocidos. Se trata de analizar el código de programa del objeto y buscar características distintivas típicas de los virus.
- Una vez que el motor ha confirmado la identidad de un virus, limpia el objeto en la medida de lo posible. Por ejemplo, quita una macro infectada en datos adjuntos o elimina el código del virus en un archivo ejecutable.

## ¿Qué y cuándo analizar?

- La amenaza de virus puede venir de muchas direcciones como macros infectadas, archivos de programa compartidos, archivos compartidos a través de una red, correos electrónicos y datos adjuntos, disquetes, archivos descargados de Internet, etc. Los productos de software antivirus McAfee Security tienen como objeto áreas específicas de vulnerabilidad. Se recomienda un enfoque desde distintos niveles para proporcionar una gama completa con las capacidades de detección antivirus, de seguridad y de limpieza que necesita.
- MSME proporciona una gama de opciones que puede configurar según las demandas del sistema. Dichas demandas variarán según cuándo y cómo operen las piezas del sistema, y cómo interactúen entre ellas y con el mundo exterior, especialmente mediante correos electrónicos y acceso a Internet.
- Puede configurar o activar diversas acciones que le permitan determinar la manera en que MSME debe gestionar los diferentes elementos y qué acciones debe realizar en elementos detectados o sospechosos.

## Análisis de correos electrónicos

MSME analiza correos electrónicos de manera diferente según sean entrantes, salientes o internos. Cada vez que se envía o se recibe un mensaje de correo electrónico desde un origen, MSME lo analiza y lo compara con una lista de virus conocidos y de elementos sospechosos de ser virus. MSME también analiza el contenido del mensaje del correo electrónico según las reglas y las directivas definidas en el software.

Cuando MSME recibe un correo electrónico, lo analiza en este orden:

- 1 Reputación de dirección IP
- 2 Antispam o phishing
- 3 Antisuplantación
- 4 Contenido dañado o cifrado
- 5 Filtro de archivos
- 6 Análisis de contenido (conformidad y DLP)
- 7 Antivirus
- 8 Reputación de URL de correo

Aunque el análisis de los correos electrónicos se realiza en este orden, si el analizador de filtrado de archivos primero detecta un elemento, este será analizado con el antivirus antes de ponerlo en cuarentena.



Es posible detectar un correo electrónico según la dirección IP de origen cuando se activa la función de reputación de IP en MSME. Esta función está disponible si se instala el complemento McAfee Anti-Spam.

### Análisis de correo electrónico entrante

Información paso por paso de lo que le sucede a un correo electrónico que llega a su organización y cómo MSME lo analiza para determinar si está limpio o infectado.

En el proceso descrito a continuación, se da por hecho que en su organización se ha instalado MSME con todas estas funciones.

Microsoft Exchange Server 2010:

- Transporte perimetral
- Transporte de concentradores
- Buzón de correo

Microsoft Exchange Server 2013 y 2016:

- Transporte perimetral
- MBX

Si no dispone de un servidor de Exchange con las funciones de transporte perimetral y transporte de concentradores, MSME ignora los pasos relacionados con dichas funciones.

#### Procedimiento

- 1 La pila de SMTP alojada en `EdgeTransport.exe` en la función perimetral recibe el correo electrónico.
- 2 El agente de IP de MSME (McTxIPAgent) comprueba la reputación de la dirección IP de origen. La comprobación del agente de IP se ejecuta antes que las operaciones del agente de transporte.
- 3 El agente de transporte de MSME (McAfeeTxAgent) analiza el correo electrónico en busca de spam, phishing o un tamaño excesivo.
- 4 Si se detecta algo, se desecha; si no, se devuelve a la pila de SMTP.
- 5 Si el correo electrónico está limpio, lo procesa McAfeeTxRoutingAgent.
- 6 MSME recibe el mismo flujo y lleva a cabo un análisis de filtrado de archivos, análisis de contenido, análisis antivirus y filtrado de URL.

- 7 Si se detecta algo, se realiza alguna acción según la configuración del producto.
- 8 MSME asigna un sello de antivirus según las especificaciones de Microsoft.
- 9 El correo electrónico se envía a la función de concentradores de Exchange Server.
- 10 La pila de SMTP alojada en `EdgeTransport.exe` en la función de servidor de concentradores recibe el correo electrónico.
- 11 El agente de transporte MSME (McAfeeTxAgent) analiza el correo electrónico en busca de spam o phishing, y analiza su tamaño. Solo en caso de EdgeSync (servidor perimetral y de concentradores), se autentica la sesión cuando se omite el análisis antispam. En ese caso, la verificación del creador se usa para la autenticación de la sesión.
- 12 Si se detecta algo, se desecha el correo; si no, se devuelve a la pila de SMTP.
- 13 Si el correo electrónico está limpio, McAfeeTxRoutingAgent lo procesa y verifica si tiene sello de antivirus (si hay alguno).
- 14 Si tiene sello de antivirus, lo verifica y lo compara con las formas del sello de MSME con el motor/DAT en la función de servidor de concentrador.
- 15 Si el sello es diferente, MSME recibe el mismo flujo y lo analiza para el filtrado de archivos, análisis de contenido y análisis antivirus.
- 16 En transporte, MSME busca el sello de antivirus mientras que en VSAPI, el almacén de Exchange realiza esta tarea y MSME no recibe un pedido de análisis si el sello de antivirus coincide.
- 17 Si se detecta algo, se realiza alguna acción según la configuración del producto.
- 18 MSME asigna un sello de antivirus según las especificaciones de Microsoft.
- 19 El correo electrónico se envía a la función de buzón de Exchange Server.
- 20 El almacén de Exchange recibe el correo electrónico y, antes de guardarlo en su base de datos, verifica el sello de antivirus.
- 21 Si este coincide, guarda el elemento sin analizarlo.
- 22 Si el sello de antivirus no coincide, el almacén de Exchange llama a VSAPI (API de análisis de virus) y analiza el correo electrónico.
- 23 Si se produce una detección, el correo electrónico se sustituye o elimina según la configuración del producto.



La comprobación de VSAPI solo es aplicable a Microsoft Exchange Server 2010.



En el caso de Microsoft Exchange Server 2013 y 2016, las funciones de transporte de concentradores y de buzón de correo no son aplicables.

## Análisis de correos electrónicos salientes

Información paso por paso de lo que le sucede a un correo electrónico que se envía afuera de la organización y cómo MSME lo analiza, para determinar si está limpio o infectado.

### Procedimiento

- 1 El usuario final envía un correo electrónico a un usuario externo mediante el cliente de correo electrónico.
- 2 El almacén de Exchange recibe el correo electrónico y lo analiza en la carpeta Bandeja de salida.

- 3 Si hay detección, se reemplaza o se elimina según la configuración del producto y, si se reemplaza, se envía a la cola de transporte.
- 4 La pila SMTP alojada por `EdgeTransport.exe` en las funciones de concentrador y buzón de correo recibe el correo electrónico.
- 5 El agente de transporte de MSME (McAfeeTxRoutingAgent) realiza un análisis del correo electrónico de filtrado de archivos, análisis de contenido, análisis antivirus, reputación de URL y también de adición de renuncia.
- 6 Si hay detección, se desecha o se reemplaza y se devuelve correspondientemente a la pila de SMTP.
- 7 Si el correo electrónico está limpio, se devuelve a la pila de SMTP para continuar con el enrutamiento.
- 8 Si el correo electrónico se enruta hacia la función de servidor perimetral desde este servidor de concentradores:
  - a La pila de SMTP alojada por `EdgeTransport.exe` en la función de servidor perimetral recibe el correo electrónico.
  - b El agente de transporte MSME (McAfeeTxRoutingAgent) comprueba si hay algún sello de antivirus.
  - c Si está presente el sello de antivirus, se comprueba y compara con el sello que MSME forma con motor/DAT en la función de servidor perimetral.
  - d Si el sello es distinto, MSME recibe el mismo flujo y realiza un análisis de filtrado de archivos, análisis de contenido, análisis antivirus y comprobación de reputación de URL.
  - e Si se detecta algo, se realiza alguna acción según la configuración del producto.
  - f MSME marca el correo electrónico con un sello de antivirus, según las especificaciones de Microsoft sobre la función de servidor perimetral.
- 9 El correo electrónico se devuelve a la pila de SMTP alojado por `EdgeTransport.exe` en la función de servidor perimetral para continuar con el enrutamiento.

## Análisis de correos electrónicos internos

Información paso por paso de lo que le sucede a un correo electrónico que se envía dentro de la organización y cómo MSME lo analiza, para determinar si está limpio o infectado.

### Procedimiento

- 1 El usuario final envía un correo electrónico a un usuario interno mediante el cliente de correo electrónico.
- 2 En el caso de Exchange Server 2010, Exchange recibe el correo electrónico y lo analiza en la carpeta Bandeja de salida. En el caso de Exchange Server 2013 y 2016, el correo electrónico se dirige a la cola de transporte desde la carpeta Bandeja de salida.
- 3 Si hay detección, se reemplaza o se elimina según la configuración del producto y, si se reemplaza, se envía a la cola de transporte.
- 4 La pila de SMTP alojada por `EdgeTransport.exe` en la función de servidor de concentrador recibe el correo electrónico.
- 5 El agente de transporte MSME (McAfeeTxRoutingAgent) analiza el correo electrónico en busca de filtrado de archivos, análisis de contenido y, luego, análisis antivirus.
- 6 Si hay detección, se desecha o se reemplaza y se devuelve correspondientemente a la pila de SMTP.
- 7 MSME marca el correo electrónico con un sello de antivirus, según las especificaciones de Microsoft sobre la función de servidor de concentrador.

- 8 Si el correo electrónico está limpio, se devuelve a la pila de SMTP para continuar con el enrutamiento.
- 9 El servidor de buzón de correo de Exchange recibe el correo electrónico.
- 10 Exchange almacena las comprobaciones de sello de antivirus y, si el sello coincide, el correo electrónico no se envía al análisis de MSME mediante VSAPI; de lo contrario, el correo electrónico se somete a un análisis antivirus, de reputación de URL, de filtrado de archivos y de contenido mediante VSAPI.



# 2

## Panel

El panel organiza y presenta la información de manera tal que es fácil de leer e interpretar.

El panel de MSME proporciona información crucial sobre cómo el servidor está siendo protegido contra spam, phishing, virus, programas potencialmente no deseados, URL maliciosas y contenido no deseado. También ofrece información sobre las estadísticas de detección, componentes adicionales instalados en el producto, información de la versión de los componentes tales como el motor y los archivos DAT, información de la licencia del producto y los elementos analizados recientemente.

### Contenido

- ▶ *Información estadística de los elementos detectados*
- ▶ *Programación de una actualización de software*
- ▶ *Análisis bajo demanda y sus vistas*
- ▶ *Informes de estado*
- ▶ *Informes de configuración*
- ▶ *Informes gráficos*

---

## Información estadística de los elementos detectados

Proporciona información detallada sobre el total de correos electrónicos analizados por MSME, sobre cuántos correos electrónicos activaron la detección y se ponen en cuarentena según la categoría de detección. El panel también proporciona información estadística en forma de gráfico, para ofrecer una interpretación más sencilla, y controla la tasa de detección.

La ficha **Estadísticas** se clasifica en las siguientes secciones:

- **Detecciones**
- **Análisis**
- **Gráfico**



Si hace clic en **Restablecer**, se borra la información estadística de todos los contadores de la sección **Detecciones** y se restablece el valor a cero. El restablecimiento de las estadísticas no elimina elementos en cuarentena de **Elementos detectados**. Los contadores dependen de la ruta de acceso de la base de datos, por lo que si se cambia dicha ruta en **Configuraciones y diagnósticos** | **Elementos detectados** | **Base de datos local**, los contadores se restablecen a cero.

Para modificar la configuración del panel, por ejemplo, el intervalo de actualización, la cantidad máxima de elementos que aparecerán en **Elementos recientemente analizados**, la unidad de escala de gráficos, la configuración de gráficos y cuadros, como los gráficos circulares en 3D, los gráficos circulares segmentados, las transparencias, vaya a **Configuraciones y diagnósticos** | **Preferencias de interfaz de usuario**.

## Detecciones

Muestra toda la información estadística sobre cuántos mensajes de correo electrónico analizados por MSME están limpios y cuántos han activado una detección. En función de la categoría de detección, aumenta el contador respectivo.

Los números en los informes indican el número de correos electrónicos y documentos que activan métodos de detección. Por ejemplo, si un correo electrónico contiene dos datos adjuntos con virus, las estadísticas de **Virus** aumentan en uno y no en dos. Los informes de estadísticas se basan en correos electrónicos en vez de archivos o detecciones individuales, y son más intuitivos en un entorno de servidor de correo.



Si el servidor de MSME se gestiona mediante ePolicy Orchestrator y se reinicia el servicio o se hace clic en el botón **Restablecer**, estas estadísticas variarán en los informes de McAfee ePO debido a los datos históricos almacenados en McAfee ePO. Para obtener más información acerca de los informes de McAfee ePO, consulte *Integración de MSME con ePolicy Orchestrator*.

**Tabla 2-1 Iconos usados. Sección Detecciones**

Icono	Descripción
	Proporciona información adicional en la categoría de detección al situar el puntero sobre el icono.
	Indica que las estadísticas de la categoría de detección respectiva están disponibles en el gráfico.
	Indica que las estadísticas de la categoría de detección respectiva no están disponibles en el gráfico.



Los iconos gráficos y aparecen solo cuando la opción <Seleccionar detecciones> está seleccionada en la lista desplegable **Gráfico**.

La tabla siguiente ofrece más información sobre cada categoría de detección.

**Tabla 2-2 Definiciones de detecciones**

Categoría	Información adicional	Descripción
<b>Limpiar</b>	<p>Si el flujo de correos electrónicos presenta más correos limpios que detecciones, al activar este icono  para correos electrónicos limpios se podría suprimir el gráfico de otras categorías. En esos casos, desactive el icono  junto a la categoría <b>Limpiar</b>.</p>	Mensajes de correo electrónico legítimos que no significan una amenaza para el usuario y no activan ninguno de los analizadores de MSME.
<b>Spam</b>	Este contador está disponible solamente si ha instalado el complemento McAfee Antispam.	Un correo electrónico no solicitado generalmente enviado de forma masiva a varios destinatarios que no lo solicitaron ni se registraron para recibirlo.
	<b>Analizados en busca de spam</b>	Todos los correos electrónicos analizados por MSME en busca de spam.
	<b>Detectados como spam</b>	Correos electrónicos identificados como spam, pero no puestos en cuarentena debido a la configuración de directiva.
	<b>Bloqueados como spam</b>	Correos electrónicos identificados como spam y puestos en cuarentena debido a la configuración de directiva.

**Tabla 2-2 Definiciones de detecciones** (continuación)

Categoría	Información adicional	Descripción
<b>Phishing</b>	Este contador está disponible solamente si ha instalado el complemento McAfee Anti-Spam.	El phishing es un método empleado por personas para obtener información personal por medios engañosos o fraudulentos. Esta información personal puede incluir datos de tarjetas de crédito, contraseñas y datos de inicio de sesión en cuentas bancarias. Estos correos electrónicos imitan fuentes de confianza, como bancos y empresas legítimas. Normalmente, estos correos electrónicos le solicitan que haga clic en un vínculo para comprobar o actualizar ciertos datos personales. Al igual que el spam, los correos electrónicos de phishing se envían de forma masiva.
	<b>Phishing detectado</b>	Correos electrónicos identificados como phishing, pero no puestos en cuarentena debido a la configuración de directiva.
	<b>Phishing bloqueado</b>	Correos electrónicos identificados como phishing y puestos en cuarentena debido a la configuración de directiva.
<b>Correos de suplantación</b>	Este contador está disponible solamente si ha instalado el complemento McAfee Anti-Spam.	
	<b>Error grave de SPF detectado</b>	Correos electrónicos identificados como mensajes de suplantación de tipo error grave.
	<b>Error leve de SPF detectado</b>	Correos electrónicos identificados como mensajes de suplantación de tipo error leve.
<b>Reputación de IP</b>	Este contador está disponible solamente si ha instalado el complemento McAfee Anti-Spam.	Un método para detectar una amenaza en mensajes de correo electrónico sobre la base de la dirección IP del servidor de envío. La calificación de reputación de IP refleja la posibilidad de que una conexión de red sea una amenaza.  La reputación de IP aprovecha McAfee Global Threat Intelligence (GTI) para evitar daños y robo de datos mediante el bloqueo de mensajes de correo electrónico en la gateway según la dirección IP del último servidor de correo electrónico.  MSME procesa el mensaje antes de que entre a la organización. Para ello rechaza o desecha la conexión según la calificación de reputación de IP.
	<b>IP encontrada</b>	Todos los correos electrónicos que llegan al servidor de MSME.
	<b>IP eliminada</b>	Correos electrónicos puestos en cuarentena por MSME debido a la función de reputación de IP. En este caso, no se notifica al remitente acerca del estado de entrega del correo electrónico.
	<b>IP rechazada</b>	Correos electrónicos puestos en cuarentena por MSME debido a la función de reputación de IP. En este caso, sí se notifica al remitente acerca del estado de entrega del correo electrónico.
<b>Virus</b>		Un archivo de programa informático que puede adjuntarse a discos u otros archivos y se replica a sí mismo repetidamente, en general sin conocimiento o permiso del usuario. Algunos virus se adjuntan a archivos, de forma que cuando se ejecuta el archivo, el virus también se ejecuta. Otros virus residen en la memoria del equipo e infectan archivos cuando el equipo abre, modifica o crea archivos. Algunos virus presentan síntomas, otros dañan archivos y sistemas informáticos, pero en cualquier caso, aunque un virus no sea perjudicial sigue siendo un virus.

**Tabla 2-2 Definiciones de detecciones** (continuación)

Categoría	Información adicional	Descripción
	<b>Virus detectados</b>	Virus detectado en un correo electrónico entrante y realización de una acción adecuada según la configuración de directiva.
	<b>Virus limpiados</b>	Virus eliminados de un correo electrónico entrante y para los cuales se lleva a cabo una acción adecuada según la configuración de directiva.
<b>Detecciones de TIE y ATD</b>	<b>Reputaciones de archivos</b>	Datos adjuntos de tipos de archivos admitidos enviados al servidor de TIE para la comprobación de reputación de archivos.
	<b>Reputaciones de certificados</b>	Datos adjuntos de tipos de archivos admitidos y firmados enviados al servidor de TIE para la comprobación de reputación de archivos.
	<b>Envíos de ATD</b>	Datos adjuntos de tipos de archivos admitidos enviados al servidor de ATD para la comprobación de reputación en función del tamaño de archivo y la categoría de aceptación.
	<b>Total de detecciones de TIE</b>	Reputación de datos adjuntos de tipos de archivos admitidos verificada por TIE.
<b>Programas potencialmente no deseados</b>		Los programas potencialmente no deseados (PUP) son programas diseñados por empresas legítimas que podrían alterar las directivas de privacidad o seguridad del equipo en el que se hayan instalado sin el conocimiento del usuario. Estos programas podrían haberse descargado junto con una aplicación legítima que desee usar.
	<b>PUP detectado</b>	PUP detectado en un correo electrónico entrante y para el cual se lleva a cabo una acción adecuada según la configuración de directiva.
	<b>PUP bloqueado</b>	PUP eliminado de un correo electrónico entrante y para el cual se lleva a cabo una acción adecuada según la configuración de directiva.
<b>Tipos de archivo/mensajes prohibidos</b>		Algunos tipos de archivos adjuntos son propensos a los virus. La capacidad de bloquear datos adjuntos por extensión de archivo es otra capa de seguridad para el sistema de correo electrónico. Los correos electrónicos internos y externos se comprueban para saber si contienen mensajes o tipos de archivos prohibidos.
	<b>Tipos de archivos prohibidos</b>	Algunos tipos de archivos adjuntos son propensos a los virus. La capacidad de bloquear datos adjuntos por extensión de archivo es otra capa de seguridad para el sistema de correo electrónico.
	<b>Mensajes prohibidos</b>	Algunos mensajes de correo electrónico cuyo envío mediante el sistema de correo desea prohibir. Se busca contenido prohibido en el correo interno y externo.
<b>Conformidad y DLP</b>	 Para ver los diccionarios disponibles, haga clic en la lista desplegable <b>Categoría</b> en <b>Administrador de directivas</b>   <b>Recurso compartido</b>   <b>Diccionarios de conformidad y DLP.</b>	<p>Detenga la pérdida de información confidencial mediante correo electrónico. MSME brinda análisis de contenido de correo electrónico líder del sector para proporcionar el control más estrecho del contenido de carácter confidencial en cualquier forma con el objetivo de ayudar a cumplir con varias regulaciones estatales, nacionales e internacionales.</p> <p>Evite la pérdida de datos con el sistema de prevención de pérdida de datos (Data Loss Prevention, DLP) de correo electrónico más amplio del sector que realiza coincidencia con patrones a fin de detectar datos y gestión de mensajes basada en directivas que evita la fuga de datos salientes.</p>

**Tabla 2-2 Definiciones de detecciones** (continuación)

Categoría	Información adicional	Descripción
<b>Contenido no deseado</b>		El contenido no deseado es cualquier contenido que el usuario no desea recibir por correo electrónico. Las reglas se pueden definir mediante algunas palabras o frases que activan la directiva correspondiente y bloquean el correo electrónico.
	<b>Empaquetadores</b>	Un archivo ejecutable comprimido que se descomprime o descifra a sí mismo en la memoria durante su ejecución, de modo que el archivo en el disco no sea nunca similar a su imagen en la memoria. Las herramientas de compresión están específicamente diseñadas para omitir el software de seguridad e impedir la ingeniería inversa.
	<b>Contenido cifrado/dañado</b>	Mensajes de correo electrónico que no se pueden clasificar como poseedores de contenido dañado o cifrado.
	<b>Contenido cifrado</b>	Algunos mensajes de correo electrónico pueden estar cifrados, lo que significa que su contenido no se puede analizar.  Las directivas de contenido cifrado especifican la manera de tratar los correos electrónicos cifrados cuando se detectan.
	<b>Contenido firmado</b>	Siempre que se envía información electrónicamente, puede ser alterada de manera accidental o voluntaria. Para evitarlo, algunas herramientas de software de correo electrónico usan una firma digital (la forma electrónica de una firma manuscrita).  Una firma digital es una información adicional añadida al mensaje de un remitente que identifica y autentica al remitente y la información en el mensaje. Está cifrada y actúa como un resumen de datos único. Normalmente, una cadena de letras y números larga aparece al final del correo electrónico recibido. El software de correo electrónico vuelve a analizar la información en el mensaje del remitente y crea una firma digital. Si esa firma es idéntica a la original significa que los datos no se han alterado.  Si el correo electrónico tiene contenido con virus, contenido dañino o es demasiado grande, el software puede limpiar o eliminar algunas partes del mensaje. El correo electrónico todavía sería válido y podría leerse, pero la firma digital original estaría "rota". El destinatario no podría confiar en el contenido del correo electrónico porque dicho contenido también podría haberse alterado de otras maneras.
	<b>Contenido dañado</b>	El contenido de algunos mensajes de correo electrónico puede resultar dañado, lo que significa que no se puede analizar.  Las directivas sobre contenido dañado especifican la manera de tratar los correos electrónicos con contenido dañado cuando se detectan.
	<b>Denegación de servicio</b>	Forma de atacar un equipo, un servidor o una red. El ataque es un producto derivado deliberado o accidental de código de instrucción que se ejecuta desde una red independiente, un sistema conectado a Internet o directamente desde el host. El ataque está diseñado para desactivar o apagar el sistema objetivo e interrumpe la capacidad del sistema para responder a solicitudes de conexión legítimas. Un ataque de denegación de servicio inunda su objetivo con solicitudes de conexión falsas, de modo que el objetivo ignora solicitudes legítimas.

Tabla 2-2 Definiciones de detecciones (continuación)

Categoría	Información adicional	Descripción
	<b>Contenido protegido</b>	El contenido de algunos mensajes de correo electrónico está protegido, lo que significa que no se puede analizar. Las directivas de contenido protegido especifican la manera en que se gestionan los mensajes de correo electrónico con contenido protegido cuando se detectan.
	<b>Archivos protegidos con contraseña</b>	Es posible proteger mediante contraseña un archivo enviado por correo electrónico. Los archivos protegidos con contraseña no se pueden analizar. Las directivas para estos archivos especifican la manera en que se gestionan los mensajes de correo electrónico que contienen uno de ellos.
	<b>Mensajes MIME incompletos</b>	Extensiones multipropósito de correo Internet (MIME) es un estándar de comunicaciones que permite la transferencia de formatos distintos de ASCII mediante protocolos (como SMTP) compatibles solo con caracteres ASCII de 7 bits. MIME define diversas formas de codificar los formatos que no son ASCII para que puedan representarse utilizando caracteres del conjunto de caracteres ASCII de 7 bits. Si el contenido del cuerpo de un mensaje MIME es demasiado grande para enviarse mediante el sistema de transferencia de correo, el cuerpo puede pasar como un número de mensajes MIME más pequeños. Estos mensajes se conocen como "mensajes MIME parciales o incompletos", ya que cada mensaje MIME contiene solo un fragmento del mensaje total que necesita ser transmitido.
<b>Reputación de URL de correo</b>	<b>URL detectadas</b>	Direcciones URL sospechosas detectadas en el correo electrónico mediante la reputación de URL.

## Programación de una actualización de software

Mantenga el software actualizado con el DAT antivirus, el motor antivirus, los controladores adicionales y el motor antispam más recientes mediante la programación de actualizaciones automáticas.



De manera predeterminada, la actualización del producto se lleva a cabo en función de la configuración del repositorio especificada en **Editor de Sitelist**. Para cambiar la configuración del repositorio, use **Editor de Sitelist** desde **Inicio | Todos los programas | McAfee | Security for Microsoft Exchange**. Sin embargo, si el equipo está administrado por un servidor de ePolicy Orchestrator, la actualización del producto se producirá en función de la configuración proporcionada en ePolicy Orchestrator.

### Procedimiento

- 1 Haga clic en **Panel | Estadísticas e información**.
- 2 En la sección **Versiones y actualizaciones**, haga clic en la ficha **Actualizar información**.
- 3 En **Editar programación** (Frecuencia de actualización), haga clic en **Editar programación**.

Aparece la página **Edit Schedule** (Editar programación).

- 4 En **Seleccione una hora**, seleccione una opción en función de la frecuencia de actualización de software requerida.



Como práctica recomendada, programe una actualización diaria mediante **Días** y especifique 1 en el cuadro de texto **Cada día(s)**. Realice actualizaciones de software durante las horas no laborales o cuando el tráfico de red sea bajo.

- 5 Haga clic en **Guardar** y después en **Aplicar**.

Ha programado correctamente una actualización de software.

## Análisis bajo demanda y sus vistas

Un analizador bajo demanda es un analizador de seguridad que se inicia manualmente a horas convenientes o a intervalos regulares. Le permite establecer varias configuraciones y analizar correos o buzones de correo específicos.

MSME le permite crear análisis bajo demanda planificados. Puede crear varias planificaciones, cada una se puede ejecutar automáticamente a intervalos o a horas predeterminados.

Puede planificar análisis regulares cuando la actividad del servidor sea comparativamente baja y no interfiera con su trabajo.



Esta función está disponible solo en un Exchange Server que tiene función de buzón de correo. No puede planificar un análisis bajo demanda en un Exchange Server que tiene solo función de transporte perimetral o de transporte de concentradores.

### Cuándo debe realizar un análisis bajo demanda

Se recomienda realizar un análisis bajo demanda si se produce una interrupción en la organización debido a la presencia de actividad maliciosa. Esto garantiza que las bases de datos de Microsoft Exchange estén limpias y no se infecten durante la interrupción.

McAfee recomienda que realice una tarea de análisis bajo demanda durante las horas no comerciales. Cuando se planifica una tarea de análisis bajo demanda durante una hora no comercial y esta continúa durante las horas de más trabajo, se deben volver a tener en cuenta las bases de datos que se analizan y crear planificaciones alternativas mediante la alteración de los datos que se analizan.

Puede planificar un análisis bajo demanda durante los fines de semana para asegurarse de que las bases de datos de Exchange estén limpias y los correos electrónicos anteriores también sean analizados por las firmas antivirus más recientes. Los administradores deben planificar un análisis bajo demanda y, al mismo tiempo, tener en cuenta la cantidad de servidores Exchange Server, bases de datos y flujo de correo. La meta debe ser completar esta tarea antes del horario comercial.

### ¿Por qué efectuar un análisis bajo demanda?

Se recomienda que realice un análisis bajo demanda por varias razones: Por ejemplo:

- Para comprobar archivos específicos descargados o publicados.
- Para comprobar que los mensajes en Microsoft Exchange Server no contienen virus, posiblemente después de la actualización de DAT, ya que podrá detectar nuevos virus.
- Si ha detectado y limpiado un virus y quiere comprobar que su equipo está totalmente limpio.

## Vista de tareas de análisis bajo demanda

Puede ver una lista de tareas de análisis bajo demanda configuradas para MSME.

### Procedimiento

- Haga clic en **Panel | Análisis bajo demanda**. Aparecerá la página **Análisis bajo demanda** con la lista de tareas de análisis bajo demanda configuradas.



De forma predeterminada, se crea una tarea de análisis bajo demanda planificada llamada **Análisis predeterminado** cuando se instala MSME.

En la página **Análisis bajo demanda**, puede usar las opciones siguientes:

**Tabla 2-3 Definiciones de las opciones**

Opción	Definición
<b>Nombre</b>	Indica el nombre de la tarea de análisis bajo demanda.
<b>Estado</b>	Indica el estado actual de la tarea de análisis bajo demanda en cuanto a si el estado de la tarea es <b>Inactivo</b> , <b>Running</b> (En ejecución), <b>Detenido</b> o <b>Terminado</b> .
<b>Última ejecución</b>	Indica la fecha y la hora en las que se ejecutó por última vez la tarea de análisis bajo demanda.
<b>Próxima ejecución</b>	Indica la fecha y la hora para las cuales se programó que se ejecute la siguiente tarea de análisis bajo demanda.
<b>Acción</b>	Muestra estas opciones para todas las tareas de análisis bajo demanda disponibles: <ul style="list-style-type: none"> <li>• <b>Modificar</b></li> <li>• <b>Eliminar</b></li> <li>• <b>Ejecutar ahora</b></li> <li>• <b>Mostrar estado</b></li> </ul> <p>La opción <b>Detener</b> aparece solamente si se está ejecutando una tarea de análisis bajo demanda.</p>
<b>Modificar</b>	Permite editar la tarea de análisis bajo demanda.
<b>Eliminar</b>	Elimina la tarea de análisis bajo demanda seleccionada.
<b>Ejecutar ahora</b>	Inicia la tarea de análisis bajo demanda seleccionada de manera inmediata. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Ejecutar ahora solo se puede utilizar después de crear y aplicar una tarea de análisis bajo demanda sin planificar. </div>
<b>Mostrar estado</b>	Muestra el estado actual de una tarea de análisis bajo demanda. La página <b>Estado de la tarea</b> aparece con las siguientes fichas: <ul style="list-style-type: none"> <li>• <b>General:</b> proporciona más información acerca de la tarea de análisis bajo demanda, como el tiempo total de ejecución, el progreso, la versión del motor y de los DAT que se usan para el análisis, los resultados del análisis, el total de elementos analizados, las reglas infringidas y las carpetas analizadas.</li> <li>• <b>Configuración:</b> proporciona más información de la base de datos analizada y la directiva utilizada.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  La opción <b>Mostrar estado</b> está disponible solamente después de iniciar una tarea de análisis bajo demanda. </div>
<b>Detener</b>	Detiene una tarea de análisis bajo demanda en ejecución.



**Tabla 2-3 Definiciones de las opciones** (continuación)

Opción	Definición
Actualizar	Actualiza la página con la información más reciente de la tarea de análisis bajo demanda.
Nueva exploración	Permite programar una nueva tarea de análisis bajo demanda.

Ha visto satisfactoriamente todas las tareas de análisis bajo demanda disponibles configuradas para MSME.

## Creación de una tarea de análisis bajo demanda

Programe una tarea de análisis bajo demanda para buscar y eliminar virus y contenido prohibido en los buzones de correo electrónico en intervalos de tiempo convenientes.

### Antes de empezar

Asegúrese de no eliminar **MSMEODuser** del Active Directory creado durante la instalación del producto. Este usuario es necesario para realizar análisis bajo demanda de los buzones de correo.

### Procedimiento

- 1 Haga clic en **Panel | Análisis bajo demanda**. Aparecerá la página **Análisis bajo demanda**.
- 2 Haga clic en **Nueva exploración**. Aparecerá la página **Seleccionar cuándo se va a realizar el análisis**.
- 3 En la ficha **Seleccione una hora**, especifique cuándo desea que se ejecute el análisis. Las opciones disponibles son las siguientes.
  - **Sin programar**: seleccione esta opción si no ha decidido cuándo realizar el análisis bajo demanda o para desactivar la programación de un análisis bajo demanda existente.
  - **Una vez**: especifique una fecha y hora para programar un solo análisis bajo demanda.
  - **Horas**: seleccione esta opción para planificar la tarea en función de las horas si tiene que ejecutar la tarea de análisis bajo demanda más de una vez al día. Por ejemplo, supongamos que actualmente son las 14:00 horas y desea crear una tarea de análisis bajo demanda que cumpla las condiciones siguientes:
    - El análisis bajo demanda debe comenzar exactamente a las 14:30.
    - El análisis bajo demanda debe realizarse dos veces al día.Para efectuarlo, escriba **12** para las horas y **30** para los minutos.
  - **Días**: seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el análisis en una semana. Por ejemplo, si desea que el análisis bajo demanda se realice cada tres días, especifique **3** en **días** y seleccione la hora de inicio de la tarea.
  - **Semanas**: seleccione esta opción para programar la tarea según la frecuencia con que se tenga que ejecutar el análisis en un mes. Por ejemplo, si desea que el análisis bajo demanda se ejecute cada dos semanas, especifique **2** en **semanas** y seleccione los días y la hora de inicio de la tarea.
  - **Meses**: seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el análisis en un año. Por ejemplo, si desea que el análisis bajo demanda se ejecute cada segundo sábado de mes, seleccione **segundo** en la lista desplegable **El**, **Sábado** en la lista desplegable **de** y, a continuación, seleccione todos los meses y la hora de inicio de la tarea.



Active **Detener tarea tras haberse ejecutado durante** <n> horas <n> minutos para detener una tarea de análisis bajo demanda si supera el tiempo especificado.

- 4 Haga clic en **Siguiente**. Aparecerá la página **Seleccionar lo que se analizará**. Las opciones disponibles son las siguientes.
- **Analizar todas las carpetas:** seleccione esta opción para analizar los buzones de correo de Exchange Server.
  - **Analizar carpetas seleccionadas:** seleccione esta opción para analizar solo buzones de correo específicos de Exchange Server.
  - **Analizar todo excepto las carpetas seleccionadas:** seleccione esta opción para analizar todo excepto los buzones de correo específicos que se añaden a la lista **Carpetas para analizar**.



En Microsoft Exchange 2013 y 2016, la carpeta pública aparece como parte del análisis del buzón de correo, y el análisis bajo demanda siempre es recursivo para las carpetas públicas. En Microsoft Exchange 2010, puede seleccionar carpetas públicas en el nivel de carpeta o subcarpeta para realizar un análisis bajo demanda recursivo.

- 5 Haga clic en **Siguiente**. Aparecerá la página **Configurar opciones de análisis**.
- 6 En la lista desplegable **Directiva de uso**, seleccione una opción de directiva en función de sus necesidades de análisis.

Directiva	Descripción
<b>Predeterminado</b>	La configuración predeterminada de todos los analizadores y filtros, a excepción de los siguientes analizadores: <ul style="list-style-type: none"> <li>• <b>Analizador de conformidad y DLP</b></li> <li>• <b>Filtrado de archivos</b></li> </ul>
<b>Buscar virus</b>	Filtros y configuración de antivirus. Estas directivas proporcionan una manera fácil de comprobar el contenido viral en bases de datos.
<b>Eliminar virus</b>	Filtros y configuración de antivirus. Estas directivas proporcionan una manera fácil de eliminar el contenido viral en bases de datos.
<b>Búsqueda de contenido no conforme</b>	Configuración de análisis de contenido. Estas directivas son útiles si quiere ver el efecto de las reglas de análisis de contenido creadas o asignadas recientemente.
<b>Eliminación de contenido no conforme</b>	Configuración de análisis de contenido. Estas directivas son útiles si quiere ver el efecto de las reglas de análisis de contenido creadas o asignadas recientemente y eliminar el contenido no conforme.
<b>Análisis completo</b>	Configuración para todos los analizadores y filtros. Estas directivas se usan normalmente para analizar a intervalos regulares.

Las configuraciones y las acciones para realizar se especifican en las directivas bajo demanda de **Administrador de directivas**.

- 7 Seleccione las opciones **Análisis reanudable** y **Reiniciar a partir del último elemento** para ejecutar la tarea de análisis bajo demanda en varias sesiones en la base de datos del buzón de correo.



A veces se recomienda ejecutar una tarea de análisis bajo demanda en todos los buzones de correo. El análisis de todos los buzones de correo en una sesión podría tardar más y afectar a la productividad del sistema. En vez de analizar todos los buzones de correo en una sesión, puede programar el análisis para varias sesiones.

- 8 En Exchange Server, ahora existe la posibilidad de llevar a cabo tareas de análisis bajo demanda pormenorizadas. Puede restringir el análisis usando los campos siguientes:
- Asunto
  - De
  - Para

- ID de mensaje
- Destinatarios
- Rango de fechas
- Tamaño del correo
- Datos adjuntos
- Elementos no leídos

Los análisis bajo demanda pormenorizados permiten ahorrar tiempo y obtener resultados de análisis específicos.

- 9 Haga clic en **Siguiente**. Aparece la página **Introduzca un nombre para el análisis**.
- 10 Especifique un nombre descriptivo para la tarea de análisis bajo demanda basado en la directiva seleccionada en la página anterior. Por ejemplo, si está creando una tarea de análisis bajo demanda para realizar un análisis completo el fin de semana, especifique el nombre `Análisis completo de fin de semana`.
- 11 Haga clic en **Finalizar** y después en **Aplicar**.

Al realizar estos pasos, se crea satisfactoriamente una tarea de análisis bajo demanda.

---

## Informes de estado

Un informe de estado es un informe planificado enviado a un administrador en un momento determinado. El informe contiene estadísticas de detección dentro de ese espacio de tiempo determinado.

Con **Informes de estado**, es posible automatizar la tarea de consulta periódica de estadísticas. Puede programar una tarea periódica para reunir los datos estadísticos simples, como el número de detecciones en una fecha determinada, y enviar un correo electrónico al administrador de Exchange o a una lista de distribución.

Estos informes ayudan a conocer qué servidores Exchange Server reciben más amenazas; de esta manera, es posible pensar mecanismos para reducir el panorama de amenazas.

Puede elegir un espacio de tiempo, una dirección de correo electrónico de destinatario o una lista de distribución a la cual enviar el informe y un asunto para el correo electrónico. Los informes de estado se envían al destinatario en formato HTML o CSV.

Según la configuración, el informe de estado que se envía por correo electrónico contiene información estadística sobre los elementos detectados, como virus, spam, phishing, reputación de IP, programas potencialmente no deseados, tipos de archivo prohibidos, contenido no deseado, conformidad y DLP, correos electrónicos limpios y total de correos electrónicos analizados. Para obtener más información sobre cómo programar el envío de un informe de estado, consulte *Programación de un nuevo informe de estado*.



Después de instalar MSME, el informe de estado se toma al menos 24 horas para revelar las estadísticas en la notificación por correo electrónico.

## Vista de tareas de informe de estado


Puede ver una lista de tareas de informe de estado configuradas para MSME.

### Procedimiento

- Haga clic en **Panel | Informes de estado**. Aparece la página **Informes de estado**, que muestra las tareas de informe de estado configuradas.

En la página **Informes de estado**, puede usar las opciones siguientes:

**Tabla 2-4 Definiciones de las opciones**

Opción	Definición
<b>Nombre</b>	Indica el nombre de la tarea de informes.
<b>Estado</b>	Indica el estado actual de la tarea de informe, por ejemplo, <b>Inactivo</b> , <b>En ejecución</b> , <b>Detenido</b> o <b>Finalizado</b> .
<b>Última ejecución</b>	Indica la fecha y la hora en las que se ejecutó por última vez la tarea de informe.
<b>Próxima ejecución</b>	Indica la fecha y la hora para las cuales se programó la ejecución de la siguiente tarea de informe.
<b>Acción</b>	Muestra las opciones para las tareas de informe disponibles: <ul style="list-style-type: none"> <li>• <b>Modificar</b></li> <li>• <b>Eliminar</b></li> <li>• <b>Ejecutar ahora</b></li> <li>• <b>Mostrar estado</b></li> </ul> Aparece la opción <b>Detener</b> solamente si hay una tarea de informe en ejecución.
<b>Modificar</b>	Haga clic en <b>Modificar</b> para editar la configuración de la tarea de análisis bajo demanda.
<b>Eliminar</b>	Elimina la tarea de informe seleccionada.
<b>Ejecutar ahora</b>	Inicia la tarea de informe seleccionada inmediatamente.
<b>Mostrar estado</b>	Muestra el estado actual de la tarea de informe. La página <b>Estado de la tarea</b> tiene la ficha siguiente: <ul style="list-style-type: none"> <li>• <b>General</b>: proporciona más información sobre la tarea de informe, como el horario de inicio y finalización, el tiempo de ejecución, la acción actual y el progreso.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  La opción <b>Mostrar estado</b> está disponible solamente una vez iniciada la tarea de informe. </div>
<b>Actualizar</b>	Actualiza la página con la información de informe más actualizada.
<b>Nuevo informe</b>	Programa una nueva tarea de informe de estado.

Ha visto satisfactoriamente todas las tareas de informe de estado configuradas para MSME.

## Programación de un nuevo informe de estado

Programa una nueva tarea de informe de estado para enviar las estadísticas de detección a una dirección de correo electrónico o una lista de distribución específicas en intervalos convenientes.

### Procedimiento

- 1 Haga clic en **Panel | Informes sobre el estado**. Aparece la página **Informes sobre el estado**.
- 2 Haga clic en **Nuevo informe**. Aparece la página **Informe**.
- 3 En la ficha **Cuándo informar**, especifique cuándo desea ejecutar la tarea de informe de estado. Las opciones disponibles son las siguientes:
  - **Sin programar**: seleccione esta opción si no ha decidido cuándo realizar la tarea de informe de estado o para desactivar la programación de una tarea de informe de estado existente.
  - **Una vez**: especifique una fecha y hora para programar una tarea de informe de estado.

- **Horas:** seleccione esta opción para programar la tarea sobre la base de horas si debe ejecutar la tarea de informe de estado más de una vez en el día. Por ejemplo, consideremos que la hora actual es 14:00 y tiene que crear una tarea de informe que especifique las siguientes condiciones:
  - La tarea de informe de estado debe comenzar exactamente a las 14:30.
  - La tarea de informe de estado debe realizarse dos veces al día.

Para lograr esto, especifique 12 para las horas y 30 para los minutos.
- **Días:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de estado en una semana. Por ejemplo, si desea que la tarea de informe de estado se realice cada tres días, especifique 3 en **día(s)** y seleccione el horario de inicio de la tarea.
- **Semanas:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de estado en un mes. Por ejemplo, si desea que la tarea de informe de estado se realice cada dos semanas, especifique 2 en **semana(s)** y seleccione el día y la hora de inicio de la tarea.
- **Meses:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de estado en un año. Por ejemplo, si desea que la tarea de informe de estado se realice el segundo sábado de cada mes, seleccione **segundo** en la lista desplegable **El**, **Sábado** en la lista desplegable **de**. Luego seleccione todos los meses y el horario en el que la tarea debe iniciarse.



Active **Detener tarea tras haberse ejecutado durante** <n> hora(s) <n> minuto(s) para detener una tarea de informe de estado si excede el horario especificado.

- 4 Haga clic en **Siguiente**. Aparece la página **Configuración de informes**. Las opciones disponibles son las siguientes:

**Tabla 2-5 Definiciones de las opciones**

Opción	Definición
<b>Correo electrónico del destinatario</b>	<p>Especifica la dirección de correo electrónico del destinatario o la dirección SMTP de la lista de distribución. En la mayoría de los casos, esta debería ser la dirección de correo electrónico del administrador de Exchange.</p> <p> De manera predeterminada, la dirección de correo electrónico de <b>Configuración y diagnósticos   Notificaciones   Configuración   General   Correo electrónico del administrador</b> se usa como la dirección de correo electrónico del destinatario.</p>
<b>Línea del asunto para el informe</b>	<p>Especifica un asunto descriptivo para el correo electrónico. Por ejemplo, si desea tener un informe de estado diario en formato HTML, especifique <code>Informe de estado diario de MSME (HTML)</code>.</p>
<b>Número de filas</b>	<p>Especifica la cantidad de filas (n) que se mostrarán en el correo electrónico del informe de estado. Cada fila del informe de estado muestra el número total de detecciones en un día determinado. El informe contiene el recuento de detecciones de los últimos días (n), exceptuando el día en el que se activó el informe de estado. Por ejemplo: si especifica 1, el informe de estado contendrá una fila que muestra las detecciones del día anterior.</p> <p> Puede especificar un máximo de 365.</p>
<b>Tipo de informe</b>	<p>Especifica el formato del informe de estado que se envía al destinatario. Las opciones disponibles son las siguientes:</p> <ul style="list-style-type: none"> <li>• <b>CSV:</b> seleccione esta opción si desea que el informe se envíe al destinatario en formato de valores delimitados por comas como archivo adjunto <code>.csv</code>.</li> <li>• <b>HTML:</b> seleccione esta opción si desea que el informe de estado se envíe al destinatario en formato HTML como archivo adjunto <code>.html</code> o que aparezca en el cuerpo del mensaje del correo electrónico.</li> </ul>

- 5 Haga clic en **Siguiente**. Aparecerá la página **Introduzca un nombre de tarea**.
- 6 Especifique un nombre descriptivo de tarea de informe de estado basado en la programación y el formato seleccionado en las páginas anteriores. Por ejemplo, si crea una tarea de informe de estado semanal que proporcione las estadísticas de detección de los días de la semana en formato HTML, el nombre de la tarea debe ser `Informe de estado semanal (HTML)`.
- 7 Haga clic en **Finalizar** y, luego, en **Aplicar**.


Al realizar estos pasos, se crea satisfactoriamente una tarea de información de estado.

## Notificaciones por correo electrónico de informes de estado

Según el informe de estado programado, el destinatario recibe un correo electrónico con las estadísticas de todos los correos electrónicos que MSME analiza y detecta durante el plazo especificado.

Según la configuración del informe de estado, el correo electrónico sobre dicho informe contiene información estadística de los elementos detectados, el total de correos electrónicos limpios y el total de los correos electrónicos analizados ese día.

**Tabla 2-6 Definiciones de las opciones**

Opción	Definición
<b>De</b>	Muestra la dirección de correo electrónico que se especificó en <b>Configuración y diagnósticos   Notificaciones   Configuración   General   Correo electrónico del remitente</b> .
<b>Para</b>	Muestra la dirección de correo electrónico del destinatario deseado que se especificó en <b>Configuración y diagnósticos   Notificaciones   Configuración   General   Correo electrónico del administrador</b> .
<b>Asunto</b>	Muestra el asunto de la notificación por correo electrónico del informe de estado que se especificó en <b>Panel   Informes sobre el estado   Configuración de informes   Línea del asunto para el informe</b> .
<b>Estadísticas de análisis para el servidor</b>	Muestra el <b>Nombre de equipo</b> donde se ha instalado MSME.
<b>Fecha</b>	Muestra la fecha en formato MM/DD/AAAA.
<b>Detecciones</b>	Muestra las estadísticas de detección de <b>Virus, Spam, Phishing, Reputación de IP, Programa potencialmente no deseado, Tipo de archivos prohibidos, Contenido no deseado, y Conformidad y DLP</b> en el cuerpo del mensaje.  <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Las estadísticas sobre <b>Spam, Phishing y Reputación de IP</b> están disponibles solo si se ha instalado el complemento McAfee Anti-Spam.         </div>
<b>Limpiar</b>	Muestra la cantidad total de correos electrónicos limpios que MSME detectó como limpios y que no representaban una amenaza. Por ejemplo, incluso un correo electrónico sobre un informe de estado enviado al administrador se contará como correo electrónico limpio en las estadísticas.
<b>Total analizados</b>	Muestra la cantidad total de correos electrónicos que MSME analizó en un día.



Los correos electrónicos de informe de estado se bloquean si se configura el valor **Umbral de reputación de IP** como **IP de confianza (menor a 0)** o **IP neutra (igual o superior a 0)** en **Configuración y diagnósticos | Antispam | Reputación de IP de McAfee GTI**.

## Informes de configuración

Un informe de configuración es un informe planificado enviado a un administrador en un momento determinado. El informe contiene la información del sistema, configuración de directiva e información del producto MSME.

Con los **Informes de configuración**, es posible automatizar la tarea de visualización periódica del resumen de la configuración del producto.

Esta función es útil cuando existen varios administradores en la organización y se desea realizar un seguimiento de las opciones de configuración de MSME. También resulta útil cuando hay varias instalaciones de MSME administradas por ePolicy Orchestrator y se desea realizar un seguimiento de la configuración del producto.

Puede elegir un espacio de tiempo, una dirección de correo electrónico de destinatario o una lista de distribución a la cual enviar el informe y un asunto para el correo electrónico.

Según la configuración, el informe contendrá información sobre el sistema y el producto, por ejemplo, información sobre el servidor y la versión del producto, el estado y el tipo de licencia, HotFix, el registro de depuración, la configuración de análisis en tiempo real y las directivas en tiempo real, y las directivas de gateway. Para obtener más información sobre cómo programar el envío de un informe de configuración, consulte *Programación de un nuevo informe de configuración*.

## Vista de tareas del informe de configuración

Puede ver una lista de tareas del informe de configuración de MSME.

### Procedimiento


- Haga clic en **Panel | Informes de configuración**. Aparece la página **Informes de configuración**, que muestra las tareas de informe de configuración.

En la página **Informes de configuración** puede usar estas opciones:

**Tabla 2-7 Definiciones de las opciones**

Opción	Definición
<b>Nombre</b>	Indica el nombre de la tarea de informes.
<b>Estado</b>	Indica el estado actual de la tarea de informe, por ejemplo, <b>Inactivo</b> , <b>En ejecución</b> , <b>Detenido</b> o <b>Finalizado</b> .
<b>Última ejecución</b>	Indica la fecha y la hora en las que se ejecutó por última vez la tarea de informe.
<b>Próxima ejecución</b>	Indica la fecha y la hora para las cuales se programó la ejecución de la siguiente tarea de informe.
<b>Acción</b>	Muestra las opciones para las tareas de informe disponibles: <ul style="list-style-type: none"> <li>• <b>Modificar</b></li> <li>• <b>Eliminar</b></li> <li>• <b>Ejecutar ahora</b></li> <li>• <b>Mostrar estado</b></li> </ul> La opción <b>Detener</b> solamente aparece si hay una tarea de informe en ejecución.
<b>Modificar</b>	Haga clic en <b>Modificar</b> para editar la configuración de la tarea de análisis bajo demanda.
<b>Eliminar</b>	Elimina la tarea de informe seleccionada.
<b>Ejecutar ahora</b>	Inicia la tarea de informe seleccionada inmediatamente.

**Tabla 2-7 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Mostrar estado</b>	<p>Muestra el estado actual de la tarea de informe. La página <b>Estado de la tarea</b> tiene la ficha siguiente:</p> <ul style="list-style-type: none"> <li>• <b>General:</b> proporciona más información sobre la tarea de informe, como el horario de inicio y finalización, el tiempo de ejecución, la acción actual y el progreso.</li> </ul> <p> La opción <b>Mostrar estado</b> está disponible solamente una vez iniciada la tarea de informe.</p>
<b>Actualizar</b>	Actualiza la página con la información de informe más actualizada.
<b>Nuevo informe</b>	Permite programar una nueva tarea de informe de configuración.

Ha visto satisfactoriamente todas las tareas de informe de configuración disponibles para MSME.

## Programación de un nuevo informe de configuración

Programa una nueva tarea de informe de configuración para enviar la configuración del producto y la información del sistema a una dirección de correo electrónico o una lista de distribución específicas en intervalos convenientes.

### Procedimiento

- 1 Haga clic en **Panel | Informes de configuración**. Aparecerá la página **Informes de configuración**.
- 2 Haga clic en **Nuevo informe**. Aparece la página **Informe**.
- 3 En la ficha **Cuándo informar**, especifique cuándo desea ejecutar la tarea de informe de configuración. Las opciones disponibles son las siguientes:
  - **Sin programar:** seleccione esta opción si no ha decidido cuándo realizar la tarea de informe de configuración o para desactivar la programación de una tarea de informe de configuración existente.
  - **Una vez:** especifique una fecha y hora para programar una tarea de informe de configuración.
  - **Horas:** seleccione esta opción para programar la tarea sobre la base de horas si debe ejecutar la tarea de informe de configuración más de una vez en el día. Por ejemplo, consideremos que la hora actual es 14:00 y tiene que crear una tarea de informe que especifique las siguientes condiciones:
    - La tarea de informe de configuración debe comenzar exactamente a las 14:30.
    - La tarea de informe de configuración debe realizarse dos veces al día.

Para lograr esto, especifique 12 para las horas y 30 para los minutos.
  - **Días:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de configuración en una semana. Por ejemplo, si desea que la tarea de informe de configuración se realice cada tres días, especifique 3 en **día(s)** y seleccione el horario de inicio de la tarea.
  - **Semanas:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de configuración en un mes. Por ejemplo, si desea que la tarea de informe de configuración se realice cada dos semanas, especifique 2 en **semana(s)** y seleccione el día y la hora de inicio de la tarea.
  - **Meses:** seleccione esta opción para programar la tarea según la frecuencia con que se tiene que ejecutar el informe de configuración en un año. Por ejemplo, si desea que la tarea de informe de configuración se realice el segundo sábado de cada mes, seleccione **segundo** en la lista desplegable **El, Sábado** en la lista desplegable **de**. Luego seleccione todos los meses y el horario en el que la tarea debe iniciarse.




Active **Detener tarea tras haberse ejecutado durante** <n> **hora(s)** <n> **minuto(s)** para detener una tarea de informe de configuración si excede el horario especificado.



- 4 Haga clic en **Siguiente**. Aparece la página **Configuración de informes**. Las opciones disponibles son las siguientes:

**Tabla 2-8 Definiciones de las opciones**

Opción	Definición
<b>Correo electrónico del destinatario</b>	<p>Especifica la dirección de correo electrónico del destinatario o la dirección SMTP de la lista de distribución. En la mayoría de los casos, esta debería ser la dirección de correo electrónico del administrador de Exchange.</p> <p> De manera predeterminada, la dirección de correo electrónico de <b>Configuración y diagnósticos   Notificaciones   Configuración   General   Correo electrónico del administrador</b> se usa como la dirección de correo electrónico del destinatario.</p>
<b>Línea del asunto para el informe</b>	Especifica un asunto descriptivo para el correo electrónico. Por ejemplo, si desea un informe de configuración semanal, especifique <i>Informe de configuración semanal de MSME</i> .

- 5 Haga clic en **Siguiente**. Aparece la página **Introduzca un nombre de tarea**.
- 6 Especifique un nombre descriptivo de tarea de informe de configuración basado en la programación y el formato seleccionado en las páginas anteriores. Por ejemplo, si crea una tarea de informe de configuración mensual que proporciona información del producto y del sistema el primer lunes de cada mes, el nombre de la tarea debe ser *Informe de configuración mensual (primer lunes)*.
- 7 Haga clic en **Finalizar** y, luego, en **Aplicar**.


Al realizar estos pasos, se crea satisfactoriamente una tarea de información de configuración.

## Notificaciones por correo electrónico del informe de configuración

En función del informe de configuración programado, el destinatario recibe un correo electrónico que contiene información de producto de MSME, configuración de directivas e información del sistema durante el tiempo especificado.

**Tabla 2-9 Definiciones de las opciones**

Opción	Definición
<b>Información de servidor</b>	Muestra información del servidor, como el nombre del equipo, la dirección IP y la versión de Exchange.
<b>Información sobre versión</b>	Muestra información de MSME, como versión del producto, fecha y versión de DAT, versión del motor, reglas antispam e información del motor (si corresponde).
<b>Estado de la licencia</b>	Muestra información de licencias del producto, como el tipo de licencia de MSME y del complemento antispam.
<b>Información del producto</b>	Muestra información adicional del producto respecto de si hay Service Pack o HotFix instalados.
<b>Registro de depuración</b>	Muestra información del <b>Registro de depuración</b> , como el nivel, el tamaño máximo del archivo de registro y la ubicación del archivo.
<b>Configuración en tiempo real</b>	Muestra la configuración actual de <b>Configuración en tiempo real</b> que especifica la configuración que está activada o desactivada.
<b>Directivas en tiempo real</b>	Muestra los analizadores y los filtros principales activados para la <b>Directiva principal en tiempo real</b> .
<b>Directivas de puerta de enlace</b>	Muestra el estado actual del analizador antispam y antiphishing para la <b>Directiva principal   de gateway</b> .

 Esto sucede solo si está instalado el complemento McAfee Anti-Spam.

## Informes gráficos

Permite generar informes gráficos para comprender el nivel de amenaza durante un espacio de tiempo específico. Proporciona una vista explícita de los elementos detectados en la forma de **Gráfico de barras** o **Gráfico circular**.

Estos informes, junto con el informe de estado, le servirán al usuario y a la organización para identificar servidores que reciban amenazas importantes y serán de ayuda para proponer soluciones a los problemas.

Los informes gráficos se utilizarán cuando se desee ver el nivel de amenaza actual sin llevar a cabo ninguna acción sobre los elementos detectados. Los **Informes gráficos** le permiten realizar consultas según ciertos filtros; será posible ver **Top 10 reports** (10 informes principales) para diferentes detecciones.

Los **Informes gráficos** se clasifican en:

- **Simple:** utiliza solamente algunos filtros de búsqueda para mostrar los 10 informes principales del día o de la semana.
- **Avanzado:** utiliza más opciones de búsqueda mediante filtros, intervalo de tiempo y opciones de gráficos.

### Vista de informes gráficos mediante filtros de búsqueda simple

Genere un informe gráfico sobre detecciones mediante filtros de búsqueda simple por día o por semana.

#### Procedimiento

- 1 Haga clic en **Panel | Informes gráficos**. Aparece la página **Informes gráficos**.
- 2 Haga clic en la ficha **Simple**.
- 3 En la lista desplegable **Periodo de tiempo**, seleccione **Hoy** o **Esta semana** para ver las detecciones puestas en cuarentena para el día o para la semana.
- 4 En la lista desplegable **Filtrar**, seleccione el informe que desee ver. Las opciones disponibles son las siguientes.
  - **Los 10 virus principales:** enumera los nombres de los diez virus principales clasificados según el recuento de detecciones.
  - **Las 10 principales detecciones de spam:** enumera las diez principales detecciones de correos electrónicos con spam clasificadas según el recuento de mensajes con spam.
  - **Los 10 principales destinatarios de spam:** enumera los diez principales destinatarios de spam clasificados según el recuento total de mensajes con spam recibidos.
  - **Las 10 principales detecciones de phishing:** enumera las diez principales detecciones de correos electrónicos con phishing clasificadas según el recuento de mensajes con phishing.
  - **Diez principales direcciones IP bloqueadas:** enumera las diez principales direcciones IP clasificadas según el recuento bloqueado de correos electrónicos devueltos.
  - **Diez principales programas no deseados:** enumera los diez principales programas potencialmente no deseados que pueden ser amenazas.
  - **10 principales detecciones de TIE:** muestra las diez amenazas potenciales principales detectadas por TIE.
  - **10 principales detecciones de suplantación:** muestra los diez principales correos electrónicos de suplantación detectados.
  - **Diez principales detecciones de conformidad y DLP:** enumera las diez principales infracciones de conformidad y prevención de fuga de datos clasificadas según la cantidad de detecciones que activó esa regla.

- **Los 10 principales archivos infectados:** enumera los diez principales nombres de archivo clasificados por recuento de detecciones.
  - **10 URL bloqueadas principales:** enumera las diez principales URL bloqueadas que podrían constituir amenazas.
  - **10 detecciones principales :** enumera las diez detecciones principales, clasificadas según el recuento de detecciones. Este gráfico contiene todas las categorías, como virus, detecciones de spam, destinatarios de spam, detecciones de phishing, direcciones IP bloqueadas, programas no deseados, DLP y conformidad, URL maliciosas y los archivos infectados enumerados anteriormente.
- 5 Haga clic en **Buscar**. Los resultados de la búsqueda se muestran en el panel **Ver resultados**.  
En **Aumentar gráfico**, seleccione el porcentaje de aumento para ampliar o reducir la vista del gráfico en el panel **Ver resultados**.

## Utilización de filtros de búsqueda avanzados

Genere informes gráficos de detecciones mediante filtros de búsqueda avanzada.

### Procedimiento

- 1 Haga clic en **Panel | Informes gráficos**. Aparecerá la página **Informes gráficos**.
- 2 Haga clic en la ficha **Avanzadas**.

- 3 Seleccione como mínimo un filtro y como máximo tres filtros en la lista:

**Tabla 2-10 Filtros primarios**

Filtro	Descripción
<b>Asunto</b>	Busca usando el asunto del correo electrónico.
<b>Destinatarios</b>	Busca usando el correo electrónico del destinatario.
<b>Motivo</b>	Busca utilizando el activador de detección o el motivo por el que el elemento se puso en cuarentena. Al seleccionar el filtro <b>Motivo</b> , se activan los filtros secundarios para restringir aun más la búsqueda. Por ejemplo, podría interesarle buscar todos los elementos puestos en cuarentena debido a que se ha activado la regla <b>Tamaño del correo</b> como motivo.
<b>Número de ticket</b>	Para buscar mediante el número de ficha. Un número de ficha es una entrada de 16 dígitos de caracteres alfanuméricos que el software genera automáticamente por cada detección.
<b>Nombre de detección</b>	Para buscar por el nombre de elemento detectado.
<b>Calificación spam</b>	Permite buscar por la calificación de spam. Por ejemplo, podría interesarle buscar todos los elementos puestos en cuarentena con una <b>Calificación spam</b> igual a 3.

**Calificación spam** es un número que indica la cantidad de spam potencial contenido en un mensaje de correo electrónico. El motor aplica reglas antispam a los mensajes de correo electrónico que analiza. Todas las reglas están asociadas a una calificación. Para evaluar el riesgo de que un mensaje de correo electrónico contenga spam, estas calificaciones se suman a fin de ofrecer una calificación de spam general para ese mensaje de correo electrónico. Cuanto más alta sea la calificación de spam general, más alto será el riesgo de que los mensajes de correo electrónico contengan spam. La calificación de spam puede variar entre 0 y 100. Los mensajes entrantes empiezan con una calificación de spam de cero. Cada vez que un mensaje infringe un filtro, aumenta la calificación de spam.



Los filtros secundarios están disponibles solamente para el filtro **Motivo**. Si no desea especificar un filtro secundario, asegúrese de que el campo esté en blanco para que se ejecuten consultas relativas a todas las detecciones.

**Tabla 2-11 Filtros secundarios**

Filtro	Descripción
<b>Anti-Virus</b>	Busca elementos puestos en cuarentena al encontrarse un posible virus en un mensaje.
<b>Conformidad y DLP</b>	Busca elementos puestos en cuarentena al encontrarse contenido prohibido en el mensaje. Por ejemplo: palabras inadecuadas.
<b>Filtro de archivos</b>	Busca elementos puestos en cuarentena al encontrarse un archivo prohibido en el mensaje.
<b>Antispam</b>	Busca elementos puestos en cuarentena cuando se encuentra spam. Por ejemplo: mensajes de correo electrónico en cadena.
<b>Reputación de IP</b>	Busca elementos puestos en cuarentena cuando la reputación de IP supera el umbral definido.
<b>Cifrado o dañado</b>	Busca elementos puestos en cuarentena al encontrarse contenido cifrado o dañado en el correo electrónico.
<b>Programa potencialmente no deseado</b>	Busca elementos puestos en cuarentena al encontrarse un programa potencialmente no deseado en el correo electrónico.
<b>Phishing</b>	Busca elementos puestos en cuarentena al encontrarse contenido de phishing en el correo electrónico.

**Tabla 2-11 Filtros secundarios** (continuación)

Filtro	Descripción
<b>Herramienta de compresión</b>	Busca elementos puestos en cuarentena al encontrarse herramientas de compresión (programas pequeños, archivos ejecutables comprimidos, código cifrado) en el correo electrónico.
<b>Tamaño del correo</b>	Busca elementos puestos en cuarentena cuando el tamaño del correo supera el límite máximo establecido.
<b>Cifrado</b>	Busca elementos puestos en cuarentena al encontrarse contenido cifrado en el correo electrónico.
<b>Firmado</b>	Busca elementos puestos en cuarentena al encontrarse contenido firmado en el correo electrónico.
<b>Dañado</b>	Busca elementos puestos en cuarentena al encontrarse contenido dañado en el correo electrónico.
<b>Denegación de servicio</b>	Busca elementos puestos en cuarentena al producirse una amenaza de denegación de servicio. Por ejemplo: si desea recuperar todos los correos electrónicos puestos en cuarentena durante el evento.
<b>Contenido protegido</b>	Busca elementos puestos en cuarentena al encontrarse contenido protegido al que es posible que no se pueda acceder para su escrutinio.
<b>Protegido con contraseña</b>	Busca elementos puestos en cuarentena al encontrarse contenido protegido mediante contraseña al que es posible que no se pueda acceder para su escrutinio.
<b>MIME bloqueado</b>	Busca elementos puestos en cuarentena al encontrarse MIME (extensión multipropósito del correo de Internet) bloqueado en el correo electrónico.
<b>Reputación de URL</b>	Busca elementos puestos en cuarentena cuando la reputación de URL supera el umbral definido.
<b>Reputación de TIE</b>	Busca elementos puestos en cuarentena cuando la reputación de TIE supera el umbral definido.
<b>Error leve de SPF</b>	Busca elementos puestos en cuarentena al encontrarse contenido de suplantación en el correo electrónico.
<b>Error grave de SPF</b>	Busca elementos puestos en cuarentena al encontrarse contenido de suplantación en el correo electrónico.



Para obtener más información acerca de los filtros de búsqueda, consulte *Filtros de búsqueda*.

- 4 Seleccione **Todas las fechas** o un **Rango de fechas** de las listas desplegadas.

Si selecciona **Todas las fechas**, la consulta devuelve resultados de búsqueda de la base de datos de cuarentena desde el día en que comenzó a poner en cuarentena los elementos detectados. Si selecciona **Rango de fechas**, seleccione la **Fecha**, el **Mes**, el **Año**, la **Hora** y los **Minutos** de los campos **Desde** y **Hasta** a fin de que la consulta busque dentro de un rango de fechas.

- 5 Seleccione **Gráfico de barras** o **Gráfico circular** según sea necesario.
- 6 Si selecciona **Gráfico circular**, seleccione un filtro de la lista desplegable para restringir la búsqueda:

**Tabla 2-12 Consulta el**

Filtro	Descripción
Destinatarios	Busca usando la dirección de correo electrónico del destinatario.
Remitente	Busca usando la dirección de correo electrónico del remitente.
Nombre de archivo	Busca usando el nombre del archivo en cuarentena.
Nombre de detección	Realiza búsquedas usando el nombre de un elemento detectado.

**Tabla 2-12 Consulta el** *(continuación)*

<b>Filtro</b>	<b>Descripción</b>
Asunto	Realiza búsquedas usando el asunto del correo electrónico.
Motivo	Realiza búsquedas usando el activador de detección o el motivo por el cual el elemento se puso en cuarentena.
Nombre de regla	Realiza búsquedas usando el nombre de la regla que activó la detección.
Nombre de directiva	Realiza búsquedas usando el nombre de directiva que efectuó la detección.

- a En **Máximo número de resultados**, especifique la cantidad de resultados que desea ver. Puede ver hasta 99 resultados de búsqueda. Este campo está disponible solamente si selecciona el gráfico circular.
- 7 Haga clic en **Buscar**. Los resultados de la búsqueda se muestran en el panel **Ver resultados**. En **Aumentar gráfico**, seleccione el porcentaje de acercamiento para aumentar o reducir el tamaño en que se muestra el gráfico en el panel Ver resultados. Los resultados de la búsqueda se muestran en el panel **Ver resultados**.

# 3

## Elementos detectados

Consultar información sobre todos los mensajes de correo electrónico que contengan potenciales amenazas detectadas y puestas en cuarentena mediante MSME. Puede utilizar varios filtros de búsqueda para restringir la búsqueda y encontrar elementos en cuarentena que le sean de interés, ver los resultados y realizar las acciones necesarias en los elementos en cuarentena.

En la interfaz de usuario del producto, haga clic en **Elementos detectados** para ver los elementos en cuarentena según la categoría de detección. Las categorías de detección son:

- **Spam**
- **Reputación de IP**
- **Phishing**
- **Virus**
- **Detecciones de TIE y ATD**
- **Correos de suplantación**
- **Programas potencialmente no deseados**
- **Contenido no deseado**
- **Tipos de archivo/mensajes prohibidos**
- **Conformidad y DLP**
- **Reputación de URL de correo**
- **Todos los elementos**



Las opciones **Spam**, **Phishing**, **Filtro de SPF** y **Reputación de IP** solo están disponibles si se ha instalado el complemento McAfee Anti-Spam.

### Contenido

- ▶ *Administración de datos en cuarentena*
- ▶ *Tipos de detección*
- ▶ *Filtros de búsqueda principales disponibles*
- ▶ *Cuadro comparativo sobre filtros de búsqueda*
- ▶ *Opciones adicionales de búsqueda*
- ▶ *Búsqueda de elementos detectados*
- ▶ *Acciones que puede realizar con los elementos en cuarentena*

---

## Administración de datos en cuarentena

En función de sus requisitos, decida si usará la base de datos local o un servidor de administración de cuarentena dedicado, conocido como McAfee Quarantine Manager, para poner en cuarentena los elementos detectados.

De manera predeterminada, los elementos detectados se ponen en cuarentena en una base de datos PostgreSQL local, instalada por MSME.

## Configuración de la ubicación de cuarentena

En función de las opciones de configuración de **Elementos detectados**, puede elegir poner en cuarentena los elementos detectados en la base de datos local o puede usar el software de administración de cuarentena de McAfee, ampliamente conocido como McAfee Quarantine Manager, para poner en cuarentena los elementos detectados en un servidor separado.



En los sistemas gestionados, si selecciona el servidor de MQM para poner en cuarentena los elementos detectados, asegúrese de que la configuración se implemente solo en los sistemas previstos. De lo contrario, la configuración se aplicará a todos los servidores de MSME en el **Árbol de sistemas**.

En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Elementos detectados** y seleccione:

- **McAfee Quarantine Manager:** para poner en cuarentena los elementos detectados en el servidor de MQM.
- **Base de datos local:** para poner en cuarentena los elementos detectados en el servidor local de MSME, en la ruta de acceso especificada.

## Base de datos local en comparación con McAfee Quarantine Manager: casos de uso

Esta tabla ayuda a comprender cuándo conviene usar la base de datos local o McAfee Quarantine Manager para la administración de cuarentena:

Use la base de datos local	Use McAfee Quarantine Manager
Para administrar los elementos en cuarentena de una instalación de MSME.	Para administrar los elementos en cuarentena desde varias instalaciones de MSME o alguno de estos productos de MSME configurados en la organización: <ul style="list-style-type: none"> <li>• McAfee Security for Microsoft Exchange</li> <li>• McAfee Email and WebSecurity Appliance</li> <li>• McAfee Security for Lotus Domino (Windows)</li> </ul> <div data-bbox="695 1186 737 1228" style="float: left; margin-right: 5px;"></div> Puede descargar e instalar McAfee Quarantine Manager de manera gratuita si ha adquirido alguno de los productos anteriormente mencionados.
Si desea usar la base de datos PostgreSQL para poner elementos en cuarentena.	Si desea usar la base de datos de MySQL o Microsoft SQL Server para poner elementos en cuarentena.




Para obtener más información sobre el software McAfee Quarantine Manager y sus funciones, consulte la documentación del producto.

## Tipos de detección

Los elementos detectados son mensajes de correo electrónico identificados por MSME como posibles amenazas, por ejemplo, virus, spam, phishing, contenido no conforme, una URL o tipos de archivo prohibidos.

Los tipos de detección en MSMEMSME son:



Tipos de detección	Descripción
Spam	Un mensaje de correo electrónico no deseado, comúnmente correo electrónico masivo no solicitado. Por lo general, el spam se envía a varios destinatarios que no han pedido recibirlo. El spam se envía mediante correo electrónico, mensajes instantáneos, grupos de noticias Usenet, motores de búsqueda web, blogs y mensajería de texto. Puede incluir anuncios legítimos, anuncios engañosos y mensajes de phishing diseñados para engañar a los destinatarios y hacerlos revelar información personal y financiera. Los mensajes de correo electrónico no son considerados spam si un usuario ha dado su visto bueno para recibirlos.
Reputación de IP	Se trata de un método de detección de mensajes mediante la dirección IP del servidor que los envía. McAfee reúne información sobre miles de millones de direcciones IP y puertos de red, y proporciona cientos de billones de vistas únicas. De esta manera, calcula una calificación de reputación según el tráfico de la red, teniendo en cuenta el puerto, el destino, el protocolo y las solicitudes de conexión entrantes y salientes. <b>Calificación de reputación de IP</b> y refleja la probabilidad de que una conexión de red represente una amenaza. MSME utiliza esta calificación para determinar una acción según una directiva local.
Phishing	Se trata de un método para obtener información personal de manera fraudulenta, como contraseñas, números de la Seguridad Social y detalles de tarjetas de crédito, mediante el envío de mensajes de correo electrónico falsificados que parecen ser enviados por fuentes de confianza, como bancos o empresas legítimas. Normalmente, los correos electrónicos de phishing les piden a los destinatarios que hagan clic en un vínculo del correo electrónico para comprobar o actualizar detalles de contacto o información de la tarjeta de crédito. Al igual que el spam, los correos electrónicos de phishing se envían a una gran cantidad de direcciones, con la expectativa de que algún usuario proceda según lo solicitado en el correo electrónico y revele información personal.
Virus	<p>Un archivo de programa informático que puede adjuntarse a discos u otros archivos y se replica a sí mismo repetidamente, en general sin conocimiento o permiso del usuario. Algunos virus se adjuntan a archivos, de forma que cuando se ejecuta el archivo, el virus también se ejecuta. Otros virus residen en la memoria del equipo e infectan archivos cuando el equipo abre, modifica o crea archivos. Algunos virus presentan síntomas, otros dañan archivos y sistemas informáticos, pero en cualquier caso, aunque un virus no sea perjudicial sigue siendo un virus.</p> <div data-bbox="526 1205 570 1255" style="float: left; margin-right: 10px;"></div> <div data-bbox="597 1205 1511 1262" style="background-color: #f0f0f0; padding: 5px;">No puede <b>Descargar</b>, <b>Liberar</b>, <b>Reenviar</b>, o <b>Ver</b> elementos en cuarentena desde la categoría de detección <b>Virus</b>.</div>
Detecciones de TIE y ATD	Además de los DAT y de McAfee GTI, puede utilizar las capacidades de detección mejoradas de McAfee Global Threat Intelligence y McAfee Advanced Threat Defense.
Correos de suplantación	La suplantación de correo electrónico es una estratagema utilizada con frecuencia para engañar a los usuarios mediante el envío de correo electrónico con una dirección de remitente distinta. Los usuarios podrían abrir estos mensajes de correo electrónico y responder a ellos sin saber que no proceden realmente de un origen legítimo.
Programas potencialmente no deseados	Con frecuencia, son programas de software legítimos (no malware) que pueden alterar el estado de seguridad o el nivel de privacidad del equipo en el que se instalan. Este software puede incluir, aunque no necesariamente, spyware, adware, registradores de pulsaciones de teclado, crackers de contraseñas, herramientas de hackers y marcadores, y podría descargarse junto con un programa que el usuario sí desea. Los usuarios preocupados por la seguridad conocen estos programas y, en ocasiones, los eliminan.
Contenido no deseado	<p>Cualquier contenido que activa una regla de análisis de contenido. Puede incluir palabras ofensivas, abusivas, desagradables o incluso información confidencial de una empresa. El <b>Contenido no deseado</b> se puede categorizar en:</p> <ul style="list-style-type: none"> <li>• <b>Empaquetadores</b></li> <li>• <b>Contenido cifrado</b></li> <li>• <b>Contenido firmado</b></li> <li>• <b>Contenido dañado</b></li> <li>• <b>Denegación de servicio</b></li> <li>• <b>Contenido protegido</b></li> <li>• <b>Archivos protegidos con contraseña</b></li> <li>• <b>Mensajes MIME incompletos</b></li> </ul>

Tipos de detección	Descripción
<b>Tipos de archivo/mensajes prohibidos</b>	Algunos tipos de archivos adjuntos son propensos a los virus. La capacidad de bloquear datos adjuntos por extensión de archivo es otra capa de seguridad para el sistema de correo electrónico. Los correos electrónicos internos y externos se comprueban para saber si contienen mensajes o tipos de archivos prohibidos.
<b>Conformidad y DLP</b>	<p>Detenga la pérdida de información confidencial mediante correo electrónico. MSME brinda análisis de contenido de correo electrónico líder del sector para proporcionar el control más estrecho del contenido de carácter confidencial en cualquier forma con el objetivo de ayudar a cumplir con varias regulaciones estatales, nacionales e internacionales.</p> <p>Evite la pérdida de datos con el sistema de prevención de pérdida de datos (Data Loss Prevention, DLP) de correo electrónico más amplio del sector que ejecuta coincidencia con patrones a fin de detectar datos y gestión de mensajes basada en directivas que evita la fuga de datos salientes.</p>
<b>Reputación de URL de correo</b>	Impide la entrega de correo electrónico con URL no deseadas que podrían contener vínculos no deseados, vínculos de phishing o malware.



Las opciones **Spam**, **Phishing**, **Filtro de SPF** y **Reputación de IP** solo están disponibles si se ha instalado el complemento McAfee Anti-Spam.

### Véase también

[Cuadro comparativo sobre filtros de búsqueda en la página 45](#)

[Opciones adicionales de búsqueda en la página 46](#)

## Filtros de búsqueda principales disponibles

Los filtros de búsqueda le permiten definir criterios de búsqueda y realizar búsquedas más eficientes y efectivas desde la base de datos de cuarentena.

La opción de filtro de búsqueda principal disponible varía según la categoría de elemento detectado seleccionada. Estos filtros de búsqueda aparecen en la sección **Ver resultados** de la categoría de elementos detectados.






Use **Columnas para mostrar** en la sección **Ver resultados** para seleccionar los filtros de búsqueda que desee ver.



**Tabla 3-1 Elementos detectados. Filtros de búsqueda principales**

Filtro de búsqueda	Definición
<b>Acción realizada</b>	<p>Busca un elemento por la acción que se realizó en él. Las acciones que realiza MSME son las siguientes:</p> <ul style="list-style-type: none"> <li>• <b>Limpiar</b></li> <li>• <b>Limpiado</b></li> <li>• <b>Eliminados</b></li> <li>• <b>Mensaje eliminado</b></li> <li>• <b>Acceso denegado</b></li> <li>• <b>Inició la sesión</b></li> <li>• <b>Sustituidos</b></li> <li>• <b>Rechazado</b></li> </ul>
<b>Motor antispam</b>	<p>Busca un elemento mediante el motor antispam, que analiza los mensajes de correo electrónico en busca de ataques de phishing y spam.</p> <p>Para ver el <b>Motor antispam</b> actual utilizado, vaya a <b>Panel   Versiones y actualizaciones   Actualizar información   Motor antispam   Versión de reglas</b>. Por ejemplo, la versión de <b>Motor antispam</b> aparece con el formato: 9286</p>

**Tabla 3-1 Elementos detectados. Filtros de búsqueda principales** (continuación)

Filtro de búsqueda	Definición
<b>Regla antispam</b>	Busca un elemento según las reglas antispam, que se actualizan cada pocos minutos para capturar las últimas campañas de spam enviadas por remitentes de spam. Para ver la <b>Regla antispam</b> actual utilizada, vaya a <b>Panel   Versiones y actualizaciones   Actualizar información   Motor antispam   Versión de reglas</b> . Por ejemplo, la versión de regla aparece con el formato: core:4373:streams:840082:uri:1245250
<b>DAT antivirus</b>	Busca un elemento según la versión del archivo DAT antivirus con una firma distintiva. Para ver el <b>DAT antivirus</b> actual utilizado, vaya a <b>Panel   Versiones y actualizaciones   Actualizar información   Motor antivirus   Versión de DAT   Controladores adicionales</b> . Por ejemplo, la versión de DAT aparece con el formato: 6860.0000
<b>Motor antivirus</b>	Busca mediante el motor antivirus un elemento con una secuencia de caracteres exclusiva de un virus o contenido no deseado. Para ver el <b>Motor antivirus</b> actual utilizado, vaya a <b>Panel   Versiones y actualizaciones   Actualizar información   Motor antivirus   Versión de DAT   Controladores adicionales</b> . Por ejemplo, la versión de <b>Motor antivirus</b> aparece con el formato: 5400.1158
<b>Expresiones prohibidas</b>	Busca según el contenido de frases prohibidas definidas en <b>Reglas de conformidad y DLP en Administrador de directivas   Recurso compartido   Diccionarios de conformidad y DLP</b> .
<b>Nombre de detección</b>	Busca un elemento detectado según su nombre.
<b>Nombre de archivo</b>	Busca por el nombre de archivo detectado en el elemento en cuarentena. Para ver el <b>Nombre de archivo</b> utilizado, vaya a <b>Administrador de directivas   Recurso compartido   Diccionarios de conformidad y DLP   Reglas de filtrado de archivos</b> .
<b>Carpeta</b>	Busca por carpeta, donde se almacenan elementos en cuarentena, como el buzón de correo del usuario.   La carpeta no está disponible si el correo electrónico está en cuarentena en el nivel de transporte en tiempo real.
<b>Calificación de reputación de IP</b>	Busca un elemento según la <b>Calificación de reputación de IP</b> del remitente. Los elementos en cuarentena se basan en el <b>Umbral de reputación de IP</b> especificado en <b>Configuración y diagnósticos   Antispam   Reputación de IP de McAfee GTI</b> .   Este filtro está disponible solamente si ha instalado el complemento McAfee Anti-Spam.
<b>Nombre de directiva</b>	Busque un elemento según el nombre de la directiva, por ejemplo, la <b>Directiva principal</b> o la directiva secundaria que detectó el elemento.
<b>Motivo</b>	Busca un elemento según el motivo por el que se detectó. Se puede basar en los analizadores y los filtros, como <b>Antivirus, Antispam, Antiphishing, Conformidad y DLP</b> , etcétera.
<b>Motivos</b>	Busca según reglas activadas por un correo electrónico determinado. Utilice esta opción si un elemento activó varios analizadores o filtros. Por ejemplo, si un correo electrónico de spam contiene un virus, los <b>Motivos</b> son <b>Antispam</b> y <b>Antivirus</b> .
<b>Destinatarios</b>	Busca un elemento mediante la dirección de correo electrónico del destinatario.
<b>Calificación de reputación</b>	Busca por nivel de autenticidad de la fuente del correo electrónico según la información actualizada disponible. Los elementos en cuarentena se basan en el <b>Umbral de reputación de IP</b> especificado en <b>Configuración y diagnósticos   Antispam   Reputación de mensajes de McAfee GTI</b> .   Este filtro está disponible solamente si ha instalado el complemento McAfee Anti-Spam.

**Tabla 3-1 Elementos detectados. Filtros de búsqueda principales** (continuación)

Filtro de búsqueda	Definición
Nombre de regla	Busca un elemento según la regla que activó uno o más analizadores o filtros. La regla que activó el analizador o el filtro se basa en las <b>Acciones</b> configuradas para cada directiva.
Analizado por	Busca un elemento por el nombre de analizador que lo detectó.
Remitente	Busca un elemento por la dirección de correo electrónico del remitente.
IP del remitente	Busca un elemento por dirección IP del sistema del remitente. Los elementos en cuarentena se basan en el <b>Umbral de reputación de IP</b> especificado en <b>Configuración y diagnósticos</b>   <b>Antispam</b>   <b>Reputación de IP de McAfee GTI</b> .   Este filtro está disponible solamente si ha instalado el complemento McAfee Anti-Spam.
Servidor	Busca un elemento según el nombre del equipo.
Calificación spam	Busca un elemento según la calificación de spam, un número que indica la cantidad de spam potencial en el mensaje de correo electrónico. El motor aplica reglas antispam a los mensajes de correo electrónico que analiza. Cada regla se asocia con una calificación.  Para evaluar el riesgo de que un mensaje de correo electrónico contenga spam, estas calificaciones se suman para dar una calificación de spam general para ese mensaje de correo electrónico. Cuanto más alta es la calificación de spam general, más alto es el riesgo de que los correos electrónicos contengan spam.   Este filtro está disponible solamente si ha instalado el complemento McAfee Anti-Spam.
Estado	Busca un elemento según su estado actual. Los estados de elemento disponibles son los siguientes: <ul style="list-style-type: none"> <li>• <b>Sin preparar:</b> elementos a los cuales no se les realizó ninguna acción, como purga, liberación, reenvío o eliminación. El estado inicial de todos los elementos es <b>Sin preparar</b>.</li> <li>• <b>Liberado:</b> elementos liberados de la base de datos de cuarentena.</li> <li>• <b>En cola del gestor de cuarentena:</b> elementos que están en la cola de la base de datos de McAfee Quarantine Manager.</li> <li>• <b>Reenviado:</b> elementos reenviados a los destinatarios deseados.</li> </ul>
Asunto	Busca un elemento según la línea de asunto de un correo electrónico.
Tarea	Busca un elemento según el nombre de la tarea de análisis, que puede ser de análisis de transporte o VSAPI en tiempo real, o de análisis bajo demanda. La tarea de análisis en tiempo real que aparece en la sección <b>Ver resultados</b> se basa en la configuración activada en <b>Configuración y diagnósticos</b>   <b>Configuración en tiempo real</b> . Para conocer el elemento detectado debido a una tarea de análisis bajo demanda, vaya a <b>Panel</b>   <b>Análisis bajo demanda</b> .
Número de ficha	Busca un elemento según el número de ficha, que es un identificador alfanumérico único asignado a una detección específica y se envía como notificación por medio de correo electrónico. Ayuda a identificar la detección asociada.
Calificación de TIE	Busca elementos según la calificación de reputación de TIE.



Los filtros de búsqueda principales aplicables a las categorías de detección **Spam**, **Phishing** y **Reputación de IP** están disponibles solamente si se ha instalado el complemento McAfee Anti-Spam.

#### Véase también

*Opciones adicionales de búsqueda en la página 46*

## Cuadro comparativo sobre filtros de búsqueda

Proporciona información sobre qué filtro de búsqueda está disponible para una determinada categoría de elementos detectados.

Los filtros de búsqueda disponibles en MSME varían según la categoría del elemento detectado que haya seleccionado. Este es un material de referencia para consultar cuando no esté seguro de qué filtro de búsqueda está disponible para una categoría específica de elementos detectados.

Consultar este cuadro comparativo ayuda a conocer los filtros de búsqueda disponibles para un tipo específico de detección.

**Tabla 3-2 Cuadro comparativo. Filtros de búsqueda de tipos de detección**

Filtrar	Spam	Reputación de IP	Phishing	Virus	Programas potencialmente no deseados	Contenido no deseado	Tipos de arch./mens. prohibidos	Conform. y DLP	Rep. de URL de correo
<b>Acción realizada</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Motor antispam</b>	✓		✓						
<b>Regla antispam</b>	✓		✓						
<b>DAT antivirus</b>				✓	✓				
<b>Motor antivirus</b>				✓	✓				
<b>Expresiones prohibidas</b>						✓		✓	✓
<b>Nombre de detección</b>				✓	✓				
<b>Nombre de archivo</b>				✓	✓	✓	✓	✓	✓
<b>Carpeta</b>				✓	✓	✓	✓	✓	✓
<b>Calificación de reputación de IP</b>		✓							
<b>Nombre de directiva</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>Destinatarios</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>Calificación de reputación</b>	✓		✓						
<b>Nombre de regla</b>	✓		✓		✓	✓	✓	✓	✓
<b>Analizado por</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>Remitente</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>IP del remitente</b>	✓	✓	✓						
<b>Servidor</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>Calificación spam</b>	✓		✓						
<b>Asunto</b>	✓		✓	✓	✓	✓	✓	✓	✓
<b>Número de ticket</b>	✓		✓	✓	✓	✓	✓	✓	✓



Los filtros de búsqueda **Motivo**, **Motivos**, **Estado** y **Tarea** no están disponibles en este gráfico comparativo, ya que solo lo están para la categoría **Elementos detectados** | **Todos los elementos**.



**Véase también**

*Tipos de detección en la página 40*

## Opciones adicionales de búsqueda

Proporciona información sobre opciones adicionales de búsqueda para restringir aún más los resultados de búsqueda.

**Tabla 3-3 Definiciones de las opciones**

Opción	Definición
<b>Y</b>	Busca elementos sobre la base de condiciones configuradas en la opción de filtrado anterior y siguiente, en las cuales los resultados de búsqueda cumplen ambas condiciones.
<b>O</b>	Busca elementos sobre la base de condiciones configuradas en la opción de filtrado anterior y siguiente, en las cuales los resultados de búsqueda cumplen cualquiera de las condiciones.
<b>Contiene</b>	Busca un elemento que contenga el texto especificado en el filtro principal de búsqueda. Por ejemplo, si desea buscar elementos en cuarentena detectados en la carpeta <b>Elementos enviados</b> , seleccione <b>Carpeta</b> como filtro de búsqueda principal, seleccione <b>Contiene</b> de la lista desplegable y luego escriba <code>enviados</code> en el cuadro de texto y haga clic en <b>Buscar</b> . Puede ver los resultados en la sección <b>Ver resultados</b> .
<b>No contiene</b>	Busca un elemento que excluya el texto especificado en los resultados de búsqueda. Por ejemplo, si no desea que los elementos registrados aparezcan en los resultados de búsqueda, seleccione <b>Acción realizada</b> como filtro de búsqueda principal, seleccione <b>No contiene</b> de la lista desplegable y luego escriba <code>registro</code> y haga clic en <b>Buscar</b> . Puede ver los resultados en la sección <b>Ver resultados</b> .
<b>Coincidencia exacta</b>	Busca un elemento que sea exactamente igual al texto especificado. Por ejemplo, si desea buscar elementos en cuarentena detectados por una versión específica de <b>Motor antivirus</b> número 5400.1158, seleccione <b>Motor antivirus</b> como filtro de búsqueda principal, seleccione <b>Coincidencia exacta</b> de la lista desplegable y luego escriba <code>5400.1158</code> en el cuadro de texto y haga clic en <b>Buscar</b> . Puede ver los resultados en la sección <b>Ver resultados</b> .
<b>Coincidencia con expresión regular</b>	Busca un elemento que coincida con un patrón particular, usando expresiones regulares. Por ejemplo, si desea realizar una búsqueda sobre la base de una dirección de correo electrónico válida en cualquier parte de la detección, seleccione <b>Nombre de detección</b> como filtro de búsqueda principal, seleccione <b>Coincidencia con expresión regular</b> de la lista desplegable, luego escriba <code>\b[A-Z0-9._%+-]+@[?:[A-Z0-9-]+\.)+[A-Z]{2,4}\b</code> y haga clic en <b>Buscar</b> . Puede ver los resultados en la sección <b>Ver resultados</b> .
<b>Igual a</b>	Busque un elemento que contenga <b>Calificación de spam</b> , <b>Calificación de reputación</b> o <b>Calificación de reputación de IP</b> que equivalga al valor especificado.
<b>Inferior a</b>	Busque un elemento que contenga <b>Calificación de spam</b> , <b>Calificación de reputación</b> o <b>Calificación de reputación de IP</b> que sea menor que el valor especificado.
<b>Superior a</b>	Busque un elemento que contenga <b>Calificación de spam</b> , <b>Calificación de reputación</b> o <b>Calificación de reputación de IP</b> que sea mayor que el valor especificado.
<b>Distinción mayúsculas/minúsculas</b>	Permite seleccionar si su criterio de búsqueda distingue mayúsculas de minúsculas.
<b>Todas las fechas</b>	Permite seleccionar si desea buscar elementos en todas las fechas. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Los resultados de búsqueda aparecen según la fecha de almacenamiento en la base de datos de elementos en cuarentena. </div>
<b>Rango de fechas</b>	Busca un elemento dentro de un rango de fechas definido según sus requisitos. Aquí puede especificar el día, el mes, el año y la hora con los parámetros <b>Desde</b> y <b>Hasta</b> . También puede usar el icono del calendario para especificar el rango de fechas. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  El rango de fechas se basa en el horario local del sistema. </div>
<b>Buscar</b>	Haga clic aquí para obtener una lista de elementos en cuarentena coincidentes con los criterios de búsqueda que aparecen en la sección <b>Ver resultados</b> .
<b>Borrar filtro</b>	Haga clic aquí para volver a la configuración de búsqueda predeterminada.

**Véase también**

*Filtros de búsqueda principales disponibles en la página 42*

## Búsqueda de elementos detectados

Use los filtros de búsqueda para buscar elementos específicos en cuarentena que le interesen y para realizar la acción correspondiente.

Puede usar una combinación de filtros de búsqueda, como operadores lógicos booleanos, expresiones regulares, texto que distingue entre mayúsculas y minúsculas o intervalos de fechas.

**Procedimiento**

- 1 En la interfaz de usuario del producto, haga clic en **Elementos detectados**.
- 2 En el panel izquierdo, haga clic en la categoría de detección deseada, como **Spam**, **Phishing** o **Todos los elementos**.
- 3 En el panel **Buscar**, seleccione los filtros de búsqueda deseados desde las listas desplegables (si es necesario). Las opciones de búsqueda disponibles son las siguientes:

**Tabla 3-4 Opciones de búsqueda**




Función de búsqueda	Descripción
Filtro de búsqueda principal	<p>Seleccione si desea refinar los criterios de búsqueda en función de un filtro específico, como <b>Nombre de directiva</b>, <b>Acción realizada</b>, <b>Remitente</b>, etc.</p> <p> Para obtener más información acerca de los filtros de búsqueda principales, consulte la sección <i>Opciones de búsqueda principales disponibles</i>.</p>
Operador lógico booleano	<p>Seleccione esta opción si desea refinar la búsqueda mediante estos operadores lógicos:</p> <ul style="list-style-type: none"> <li>• <b>Y</b></li> <li>• <b>O</b></li> </ul> <p> Para obtener más información sobre estas opciones de filtros, consulte la sección <i>Opciones adicionales de búsqueda</i>.</p>
Filtro de búsqueda secundario	<p>Seleccione esta opción si desea refinar la búsqueda mediante estos filtros secundarios:</p> <ul style="list-style-type: none"> <li>• <b>Contiene</b></li> <li>• <b>No contiene</b></li> <li>• <b>Coincidencia exacta</b></li> <li>• <b>Coincidencia con expresión regular</b></li> <li>• <b>Igual a</b></li> <li>• <b>Inferior a</b></li> <li>• <b>Superior a</b></li> </ul> <p> Para obtener más información sobre estas opciones de filtros, consulte la sección <i>Opciones adicionales de búsqueda</i>.</p>

Tabla 3-4 Opciones de búsqueda (continuación)

Función de búsqueda	Descripción
<b>Distinción mayúsculas/ minúsculas</b>	Permite seleccionar si su criterio de búsqueda distingue mayúsculas de minúsculas.
<b>Rango de fechas</b>	<p>Seleccione esta opción si desea refinar la búsqueda a todas las fechas o a un periodo de tiempo específico.</p> <ul style="list-style-type: none"> <li>• <b>Todas las fechas</b></li> <li>• <b>Rango de fechas</b></li> </ul>

4 Haga clic en **Buscar**.

Al realizar esta tarea, ha buscado correctamente los elementos eliminados que coinciden con los criterios de búsqueda, que ahora aparecen en la sección **Ver resultados**.

## Acciones que puede realizar con los elementos en cuarentena

Observe los resultados de búsqueda según los parámetros definidos y lleve a cabo las acciones necesarias en los elementos en cuarentena.




Ahora puede ejecutar varias acciones en dichos elementos en cuarentena.

Tabla 3-5 Tipos de acciones

Acción	Definición
<b>Liberar</b>	<p>Permite liberar un elemento en cuarentena. Seleccione un registro aplicable en el panel <b>Ver resultados</b> y haga clic en <b>Liberar</b>. El mensaje de correo electrónico original se libera de la base de datos para entregarlo al destinatario.</p> <ul style="list-style-type: none"> <li>• Cuando se descarga, libera o reenvía el elemento, se analiza en busca de virus y aparece en la sección <b>Panel   Elementos recientemente analizados</b>.</li> <li>• Una vez efectuada la liberación satisfactoriamente, el elemento aparece con el estado <b>Liberado</b> en la categoría <b>Elementos detectados   Todos los elementos</b>.</li> </ul>
<b>Descarga</b>	<p>Para descargar un elemento en cuarentena para su búsqueda o análisis. Seleccione un registro aplicable en el panel <b>Ver resultados</b> y haga clic en <b>Descargar</b>.</p> <ul style="list-style-type: none"> <li>• No puede <b>Descargar</b>, <b>Reenviar</b>, <b>Ver</b> ni <b>Liberar</b> varios registros a la vez desde la categoría <b>Elementos detectados   Todos los elementos</b>. Sin embargo, puede <b>Liberar</b> varios registros desde una categoría específica.</li> </ul>





Tabla 3-5 Tipos de acciones (continuación)

Acción	Definición
<b>Exportar a archivo CSV</b>	<p>Permite exportar y guardar información sobre todos los elementos en cuarentena devueltos por la búsqueda en formato <code>.csv</code>. Si existen miles de elementos en cuarentena en la base de datos, en lugar de desplazarse por varias páginas, puede utilizar esta opción para descargar estos registros a un archivo en formato CSV y generar, más adelante, informes personalizados en Microsoft Excel.</p> <p>En el panel <b>Ver resultados</b>, haga clic en <b>Exportar a archivo CSV</b> para <b>Abrir</b> o <b>Guardar</b> los resultados de búsqueda en la carpeta o ubicación deseada.</p> <p>Para especificar un límite respecto a cuántos elementos en cuarentena deben aparecer en <b>Ver resultados</b>, modifique el valor <b>Tamaño máximo de consulta (registros)</b> de <b>Configuración y diagnósticos   Elementos detectados   Base de datos local</b>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <ul style="list-style-type: none"> <li>Si no encuentra un campo específico en los resultados de búsqueda del archivo CSV, asegúrese de activar el campo necesario en la opción <b>Columnas para mostrar</b>.</li> <li>Use la opción <b>Importar datos</b> de Microsoft Excel para abrir el archivo CSV en una ubicación distinta.</li> </ul> </div>
<b>Reenviar</b>	<p>Permite reenviar los elementos en cuarentena al destinatario deseado. Use punto y coma como delimitador para reenviar los elementos en cuarentena a varios destinatarios. Esta acción envía los elementos en cuarentena en un nuevo correo electrónico como adjunto (formato <code>.eml</code>).</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Para reenviar el elemento en cuarentena a una lista de distribución (LD) dentro de la organización, especifique la dirección SMTP de la lista.</p> </div>
<b>Ver</b>	Permite ver el elemento en cuarentena en una ventana independiente.
<b>Agregar a remitentes bloqueados</b>	Permite añadir la dirección de correo electrónico de un remitente a la lista de direcciones bloqueadas para correos electrónicos, que también se conoce como lista negra.
<b>Agregar a remitentes permitidos</b>	Permite añadir la dirección de correo electrónico de un remitente a la lista de direcciones permitidas para correos electrónicos, que también se conoce como lista blanca.
<b>Columnas para mostrar</b>	Permite seleccionar más encabezados de columna para agregarlos al panel <b>Ver resultados</b> . Esta opción ofrece una lista de filtros disponibles en el panel <b>Búsqueda</b> y algunas funciones más.
<b>Seleccionar todo</b>	Permite seleccionar todos los elementos en cuarentena que aparecen en la página de la sección <b>Ver resultados</b> . Por ejemplo, si tiene 100 elementos en cuarentena y configura los elementos para ver 10 <b>por página</b> , solo se seleccionarán 10 elementos que aparecen en la sección <b>Ver resultados</b> .
<b>No seleccionar nada</b>	Permite anular la selección de todos los elementos en cuarentena que aparecen en la sección <b>Ver resultados</b> .
<b>Eliminar</b>	<p>Permite eliminar los elementos en cuarentena que seleccionó en esa página de la sección <b>Ver resultados</b> de la categoría seleccionada.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Mantenga presionada la tecla <b>Ctrl</b> para seleccionar varios elementos.</p> </div>

**Tabla 3-5 Tipos de acciones** (continuación)

Acción	Definición
<b>Eliminar todo</b>	Para eliminar todos los elementos en cuarentena de la base de datos para la categoría seleccionada.
<b>Vistas por página</b>	Para especificar el número máximo de elementos en cuarentena que desea ver por página. Las opciones son: <ul style="list-style-type: none"> <li>• 10</li> <li>• 20</li> <li>• 50</li> <li>• 100</li> </ul>

Cada elemento del panel **Ver resultados** muestra una imagen, que indica:

Icono	Descripción
	Un elemento que está en cuarentena y se puede descargar, reenviar, liberar o ver.
	Un elemento que está solamente registrado y no se puede descargar, reenviar, liberar ni ver.

# 4

## Administrador de directivas

Le permite configurar o administrar diferentes directivas y las acciones correspondientes en el producto. Determina cómo se tratan los diferentes tipos de amenazas cuando se detectan.

Una directiva se define como un principio o una regla para guiar las decisiones y lograr resultados racionales. Las directivas se adoptan dentro de una organización para ayudar a la toma de decisiones objetiva.

En MSME, una directiva determina la configuración que se usa y las acciones que se deben realizar cuando se activa una detección en el entorno de Exchange. Puede crear varias directivas y definir opciones y acciones específicas en directivas particulares. Por ejemplo, puede crear varias directivas secundarias para la opción **En tiempo real** y tener una configuración y una acción diferentes establecidas para cada directiva.

En resumen, directiva de MSME = configuración del analizador + acciones para realizar.



Use la opción **Recurso compartido** del menú en **Administrador de directivas** para modificar o crear reglas para la configuración de los analizadores, los filtros y las alertas desde una ubicación común. Use **Recurso compartido** para ahorrar tiempo al crear y aplicar las directivas de MSME.

### Pasos para crear una directiva

Como administrador, para crear una directiva, debe:

- 1 Activar el analizador o el filtro.
- 2 Editar la configuración de los analizadores y filtros desde la directiva o **Recurso compartido**.
- 3 Especifique la acción por realizar cuando se activa una detección.
- 4 Especifique los usuarios a los que se aplica la directiva.
- 5 Aplique la configuración para la categoría de directiva apropiada.

### Contenido

- ▶ *Categorías de directivas para gestionar amenazas*
- ▶ *Vistas del Administrador de directivas*
- ▶ *Directiva principal y secundaria*
- ▶ *Analizadores y filtros principales*
- ▶ *Cuadro comparativo sobre analizadores y filtros*
- ▶ *Lista de todos los analizadores y filtros de una directiva seleccionada*
- ▶ *Adición de un analizador o un filtro*
- ▶ *Creación de nuevas reglas para usuarios específicos*
- ▶ *Acciones que puede realizar en las detecciones*
- ▶ *Recurso compartido*
- ▶ *Administración de opciones del analizador principal para una directiva*
- ▶ *Administración de configuraciones de filtros para una directiva*
- ▶ *Administración de configuraciones varias para una directiva*

---

## Categorías de directivas para gestionar amenazas

Mire las categorías de directivas disponibles y aplique una directiva predeterminada existente (conocida como *Directiva principal*) para toda la organización.

MSME le ayuda a prevenir amenazas electrónicas mediante conjuntos especiales de reglas y configuraciones (conocidas como directivas) que puede crear a medida según las necesidades de la organización de Exchange.

Cuando instala MSME por primera vez en Exchange Server, habrá una **Directiva principal** predeterminada para las siguientes opciones de menú:

- **En tiempo real**
- **Bajo demanda (predeterminado)**
- **Bajo demanda (buscar virus)**
- **Bajo demanda (eliminación de virus)**
- **Bajo demanda (búsqueda de contenido prohibido)**
- **Bajo demanda (eliminación de contenido prohibido)**
- **Bajo demanda (análisis completo)**
- **Gateway**

Puede personalizar directivas en cada categoría para gestionar de manera precisa amenazas que puedan afectar la organización de Exchange.

---

## Vistas del Administrador de directivas

Observe y ordene las directivas secundarias según su herencia y prioridad.

Los tipos de vistas de **Administrador de directivas** son:

- **Vista de herencia**
- **Vista avanzada**

### Vista de herencia

Muestra la prioridad y el estado de la directiva principal y todas las directivas secundarias. MSME actúa sobre un correo electrónico según las opciones configuradas en la directiva secundaria con la prioridad más alta. Cuando no se cumplen las reglas de una directiva secundaria, MSME sigue con la directiva secundaria con el nivel de prioridad siguiente. Cuando no se cumplen las reglas en ninguna de las directivas secundarias, se aplican las opciones configuradas en la directiva principal.

Cuando selecciona **Vista de herencia**, las directivas secundarias aparecen según la herencia de la directiva.

En esta vista, puede hacer lo siguiente:

- Visualizar la directiva y su prioridad
- Visualizar las directivas secundarias heredadas y sus directivas padre
- Activar o desactivar directivas secundarias
- Eliminar directivas secundarias

## Vista avanzada

Muestra todas las directivas en orden ascendente según la prioridad y proporciona una opción para cambiar la prioridad de una directiva secundaria.

En esta vista, puede hacer lo siguiente:

- Visualizar las directivas ordenadas por prioridad
- Modificar la prioridad de una directiva



Use estos iconos para modificar la prioridad de una directiva:

- : aumenta la prioridad de una directiva.
- : reduce la prioridad de una directiva.

- Activar o desactivar directivas secundarias
- Eliminar directivas secundarias
- Editar el nombre de la directiva, la descripción y la directiva padre haciendo clic en **Detalles**

## Directiva principal y secundaria

Una configuración de directiva dentro de una estructura jerárquica comúnmente se pasa de una directiva de primer nivel a una de segundo nivel, de una de segundo nivel a una de tercer nivel y así sucesivamente. Este concepto se denomina herencia. En MSME, la directiva de primer nivel predeterminada se llama **Directiva principal** y la de segundo nivel se llama **Directiva secundaria**.

### Directiva principal

Son directivas de primer nivel, disponibles para todas las categorías de directiva, que definen la manera en la que se analizan elementos en busca de virus, en la que se filtran archivos y otras configuraciones. Estas directivas se aplican a todos los usuarios de una organización.



No puede eliminar la **Directiva principal**, ya que actúa como base para crear las directivas secundarias.

### Directivas secundarias

Son directivas que heredan sus opciones y acciones de otra directiva. Puede crear más directivas secundarias con opciones y acciones distintas, según sea necesario, para aplicarlas a usuarios específicos.

Las directivas secundarias son necesarias en caso de que necesite excepciones a la **Directiva principal** para adaptarla a áreas geográficas, funciones, buzones de correo, dominios o departamentos de su organización. En MSME, el término general para dichas directivas es "grupo de directivas".

Acción que se realiza en un correo electrónico según las opciones configuradas en la directiva secundaria con la prioridad más alta. Cuando no se cumplen las reglas de la directiva secundaria con la prioridad más alta, MSME pasa a la directiva secundaria con el nivel de prioridad siguiente. Solamente cuando no se cumplen las reglas en ninguna de las directivas secundarias, se aplican las opciones configuradas en la directiva principal.

Si selecciona **Inherit settings from parent policy** (Heredar configuración de directiva principal) en la página de configuración del analizador o del filtro, la directiva heredada (directiva secundaria) usa la misma configuración que la directiva principal. Sin embargo, si se produce una detección, puede realizar una acción diferente. Cualquier cambio a la configuración de la **Directiva principal** se refleja en esta directiva secundaria.

Por ejemplo: Se crea una directiva secundaria para actuar en todos los mensajes de correo electrónico identificados por MSME como una amenaza para:

- Poner en cuarentena: para todos los usuarios
- Registrar, poner en cuarentena y notificar al administrador: para administradores

Este ejemplo simple le proporciona más detalles sobre cuándo podría necesitar una directiva secundaria.

**Tabla 4-1 Ejemplo de cuándo se necesita una directiva secundaria**

Tipo de directiva	Analizador	Nivel de protección	Usuarios	Acciones para realizar
Directiva principal	Antivirus	Protección media	Todos los usuarios	<b>Cuarentena</b>
Directivas secundarias	Antivirus	Protección alta	Administradores	<b>Registro, Cuarentena y Notificar al administrador</b>



Al restaurar MSME a su configuración predeterminada se quitan las directivas secundarias existentes. Asegúrese de hacer una copia de seguridad de las directivas y las configuraciones usando **Exportar** en la ficha **Configuración y diagnósticos** | **Importar y exportar configuración** | **Configuración**, antes de restaurar MSME a su configuración de fábrica.

## Creación de directivas secundarias

Cree directivas sobre la base de una **Directiva principal** o una secundaria para satisfacer necesidades especiales de cualquier parte de la organización. Cree directivas secundarias para cualquier situación excepcional no cubierta por la **Directiva principal**.

Resultan útiles cuando no desea aplicar reglas de la **Directiva principal** a usuarios o grupos determinados de la organización. Puede crear excepciones y hacer que MSME lleve a cabo un análisis específico.

Estos son algunos ejemplos de cuándo conviene crear una directiva secundaria:

- Permitir correos electrónicos entrantes para usuarios de nivel ejecutivo de la organización después del análisis, pero ponerlos en cuarentena si se trata de otros usuarios.
- Permitir ciertos formatos de archivo para grupos de usuarios específicos, por ejemplo, puede bloquearles los archivos .wav a todos los usuarios, a excepción de un departamento específico de la organización.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú para el que quiere crear una directiva secundaria.
- 2 Haga clic en **Create Subpolicy** (Crear directiva secundaria).  
Aparecerá la página **Crear una directiva secundaria**.
- 3 En **Configuración inicial** | **Identificación** | **Nombre de la directiva secundaria**, especifique un nombre que identifique a la directiva y lo que hace.
- 4 Introduzca una **Descripción** para la directiva (opcional).
- 5 Seleccione la **Directiva padre** para la directiva secundaria desde la cual hereda la configuración.
- 6 Haga clic en **Siguiente**.
- 7 En **Activar reglas** | **Reglas**, haga clic en **Nueva regla**.

8 En **Especificar una regla de directiva**, puede seleccionar:

- **<select a rule template>** (<seleccionar una plantilla de regla>): para especificar la regla de directiva según el remitente o el destinatario. Puede crear reglas nuevas según las siguientes opciones:
  - **La dirección SMTP del remitente es la dirección de correo electrónico**
  - **La dirección SMTP del remitente no es la dirección de correo electrónico**
  - **La dirección de SMTP de los destinatarios es la dirección de correo electrónico**
  - **La dirección de SMTP de los destinatarios no es la dirección de correo electrónico**
  - **El remitente está en el grupo de Active Directory**
  - **El remitente no está en el grupo de Active Directory**
  - **Los destinatarios están en el grupo de Active Directory**
  - **Los destinatarios no están en el grupo de Active Directory**



Asegúrese de no crear reglas con conflictos en las direcciones de correo electrónico o en los nombres de usuario. No se admiten expresiones regulares (regex) para usuarios especificados; solo se admiten comodines.

- **Copiar reglas de otra directiva:** para copiar reglas de otra directiva.

9 Haga clic en **Agregar**.

10 Especifique las condiciones en las que la directiva debe activarse para el usuario. Puede seleccionar:

- **Se aplica cualquier regla**
- **Se aplican todas las reglas**
- **No se aplica ninguna regla**

11 Haga clic en **Siguiente**.

12 En **Analizadores y filtros**, puede seleccionar:

- **Heredar todas las configuraciones de la directiva padre:** para heredar todas las propiedades de la directiva padre.
- **Inicializar la configuración seleccionada con valores copiados de otra directiva:** para seleccionar analizadores y filtros específicos de las directivas disponibles.

13 Haga clic en **Finalizar**.

---

## Analizadores y filtros principales

Determine los tipos de analizadores y de filtros que se pueden aplicar al crear directivas.

### Analizadores principales

Observe y configure las opciones de estos analizadores en **Administrador de directivas** | **Recurso compartido**.

Analizador	Definición
<b>Analizador antivirus</b>	Defina la configuración para detectar amenazas como virus, troyanos, gusanos, herramientas de compresión, spyware y adware, entre otros.
<b>Analizador de conformidad y DLP</b>	Cree o configure <b>Reglas de conformidad y DLP</b> para las directivas de confidencialidad y conformidad de su organización de Exchange con 60 <b>Diccionarios de conformidad y DLP</b> nuevos.
<b>Filtrado de archivos</b>	Cree nuevas reglas de filtrado de archivos para cumplir con las necesidades de la organización de Exchange. Configure estas opciones según el nombre, la categoría o el tamaño de archivo.
<b>Reputación de URL de correo</b>	Configure parámetros para detectar URL que contengan vínculos no deseados, vínculos de phishing y malware.
<b>Antispam</b>	Configure las opciones para detectar mensajes de correo electrónico que estén categorizados como spam, según la calificación de spam, el tamaño, las reglas y las listas de correo.
<b>Antiphishing</b>	Configure las opciones de informes para detectar mensajes de correo electrónico que estén categorizados como phishing.



Las opciones de **Antispam** y **Antiphishing** están disponibles solamente si ha instalado el complemento McAfee Anti-Spam.

## Filtros

Active o desactive estos filtros, y especifique las acciones por realizar cuando se produzca una detección según las necesidades de la organización de Exchange.



Puede activar o desactivar algunos filtros, pero no puede configurar las opciones personalizadas. Esos filtros no aparecen en la lista desplegable **Recurso compartido** | **Analizadores y alertas** | **Analizadores** | **Categoría**.

Filtro	Definición
<b>Contenido dañado</b>	Configura las opciones para actuar en mensajes de correo electrónico que sean detectados como contenido dañado.
<b>Contenido protegido</b>	Configura las opciones para actuar en mensajes de correo electrónico que sean detectados como contenido protegido.
<b>Contenido cifrado</b>	Configura las opciones para actuar en mensajes de correo electrónico que sean detectados como contenido cifrado.
<b>Contenido firmado</b>	Configura las opciones para actuar en mensajes de correo electrónico que sean detectados como contenido firmado.
<b>Archivos protegidos con contraseña</b>	Configura las opciones para actuar en mensajes de correo electrónico que contengan archivos protegidos con contraseña.  Puede omitir la directiva sobre el filtrado de archivos para permitir la entrada de correo electrónico con datos adjuntos de archivos protegidos con contraseña según sea preciso.  Para obtener más información, consulte <i>Configuración de archivos protegidos con contraseña</i> .
<b>Filtrado según tamaño del correo</b>	Crea o configura las opciones para actuar en mensajes de correo electrónico que excedan las opciones de filtrado de tamaño de correo. Configura las opciones para poner en cuarentena los mensajes de correo electrónico según el tamaño general del correo, el tamaño de los adjuntos y la cantidad de adjuntos.
<b>Control del analizador</b>	Crea o configura las opciones del analizador principal para actuar en mensajes de correo electrónico según el nivel de anidación, el tamaño de archivo expandido y el tiempo de análisis.



Filtro	Definición
<b>Configuración del correo MIME</b>	Crea o configura las opciones para detectar amenazas categorizadas como mensaje MIME.
<b>Archivos HTML</b>	Crea o configura las opciones para actuar en mensajes de correo electrónico que contengan elementos HTML, como comentarios, URL, metadatos y secuencias de comandos.

### Varios

Configura varias opciones, como alertas y renuncias, que se envían a usuarios finales si se produce una detección.

Varios	Definición
<b>Configuración de alerta</b>	Crea o configura las opciones para una alerta de correo electrónico si se produce una detección. Configura las opciones, como el formato (HTML o texto), la codificación, el nombre de archivo, el encabezado y el pie de página del correo electrónico de alerta.
<b>Texto de renuncia</b>	Crea o configura el texto de renuncia que debe aparecer en el correo electrónico que se envía al usuario final si se produce una detección.

## Cuadro comparativo sobre analizadores y filtros

Proporciona información sobre qué analizador o filtro está disponible de manera predeterminada para cada categoría de directiva.

El analizador o filtro disponible en MSME varía según la categoría de directiva que haya seleccionado.

Este es un material de referencia para consultar cuando no esté seguro de qué analizador o filtro está disponible para una categoría específica de directivas. Consultar este cuadro comparativo ayuda a conocer los analizadores y filtros disponibles para cada categoría de directiva; los acrónimos son:

- TR: **En tiempo real**
- BD (P): **Bajo demanda (predeterminado)**
- BD (BV): **Bajo demanda (búsqueda de virus)**
- BD (EV): **Bajo demanda (eliminación de virus)**
- BD (BCNC): **Bajo demanda (búsqueda de contenido no conforme)**
- BD (ECNC): **Bajo demanda (eliminación de contenido no conforme)**
- BD (AC): **Bajo demanda (análisis completo)**
- GW: **Gateway**

### Analizadores principales

Analizadores principales	TR	BD (P)	BD (BV)	BD (EV)	BD (BCNC)	BD (ECNC)	BD (AC)	GW
<b>Analizador antivirus</b>	✓	✓	✓	✓			✓	
<b>Analizador de conformidad y DLP</b>	✓	✓			✓	✓	✓	

Analizadores principales	TR	BD (P)	BD (BV)	BD (EV)	BD (BCNC)	BD (ECNC)	BD (AC)	GW
Filtrado de archivos	✓	✓					✓	
Reputación de URL de correo	✓	✓					✓	
Antispam								✓
Antiphishing								✓



Aunque el **Analizador de conformidad y DLP** esté disponible para las categorías de directiva **En tiempo real** y **Bajo demanda (predeterminado)**, no está activo o habilitado de manera predeterminada. Deberá crear las reglas necesarias y luego especificar una acción que se llevará a cabo cuando se active una regla y habilite el analizador.

## Filtros

Filtros	TR	BD (P)	BD (BV)	BD (EV)	BD (BCNC)	BD (ECNC)	BD (AC)	GW
Contenido dañado	✓	✓					✓	
Contenido protegido	✓	✓			✓	✓	✓	
Contenido cifrado	✓	✓			✓	✓	✓	
Contenido firmado	✓	✓			✓	✓	✓	
Archivos protegidos con contraseña	✓	✓			✓	✓	✓	
Filtrado según tamaño del correo	✓							✓
Control del analizador	✓	✓	✓	✓	✓	✓	✓	✓
Configuración del correo MIME	✓	✓			✓		✓	✓
Archivos HTML	✓	✓			✓		✓	✓

### Opciones de renuncia y alerta

Configuraciones varias	TR	BD (P)	BD (BV)	BD (EV)	BD (BCNC)	BD (ECNC)	BD (AC)	GW
Configuración de alerta	✓	✓		✓	✓	✓	✓	✓
Texto de renuncia	✓							

## Lista de todos los analizadores y filtros de una directiva seleccionada

Observe el estado de los analizadores y los filtros disponibles para la categoría de directiva seleccionada. El tipo de configuración que está disponible depende de la directiva seleccionada.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas** y en la opción de menú de categoría de directiva.

Aparecerá la página de la directiva para el elemento seleccionado en el menú.

- 2 Haga clic en **Directiva principal** o en la subdirectiva que desee.

Aparecerá la página de directiva correspondiente. Los filtros aplicables están disponibles en las páginas de directiva respectivas.

- 3 En la página de directiva, puede utilizar las fichas siguientes.

- **Enumerar todos los analizadores:** para ver el analizador o el filtro activado para la directiva.
- **Ver configuración:** para ver la configuración del analizador o el filtro, y las acciones especificadas.
- **Especificar usuarios:** para especificar reglas de directivas para aplicarlas a usuarios específicos.



Puede especificar usuarios solamente para directivas secundarias.

- 4 En la ficha **Enumerar todos los analizadores**, puede usar lo siguiente.

**Tabla 4-2 Configuración de directivas**

Opción	Definición
<b>Directiva</b>	Permite seleccionar la directiva que quiere configurar.
<b>Agregar analizador/filtro</b>	Permite configurar la directiva de modo que se aplique solamente en momentos específicos. Por ejemplo, puede crear una configuración antivirus nueva con reglas distintas, aplicable solamente los fines de semana.
<b>Analizadores principales</b>	Permite configurar la directiva para cada uno de estos analizadores: <ul style="list-style-type: none"> <li>• <b>Analizador antivirus</b></li> <li>• <b>Analizador de conformidad y DLP</b></li> <li>• <b>Filtrado de archivos</b></li> <li>• <b>Reputación de URL de correo</b></li> <li>• <b>Antispam</b></li> <li>• <b>Antiphishing</b></li> </ul>

Tabla 4-2 Configuración de directivas (continuación)

Opción	Definición
Filtros	Permite configurar la directiva para cada uno de estos filtros: <ul style="list-style-type: none"> <li>• Contenido dañado</li> <li>• Contenido protegido</li> <li>• Contenido cifrado</li> <li>• Contenido firmado</li> <li>• Archivos protegidos con contraseña</li> <li>• Filtrado según tamaño del correo</li> <li>• Control del analizador</li> <li>• Configuración del correo MIME</li> <li>• Archivos HTML</li> </ul>
Configuraciones varias	Permite configurar las alertas y los mensajes de renuncia de las directivas. <b>Varios</b> incluye: <ul style="list-style-type: none"> <li>• Configuración de alerta</li> <li>• Texto de renuncia</li> </ul>

## Adición de un analizador o un filtro

Agregue un analizador o filtro para crear configuraciones para casos excepcionales en la organización de Exchange.

Añadir un analizador o un filtro es útil cuando desea un analizador o un filtro adicional:

- Con diferentes opciones y reglas
- Activado solamente durante un intervalo de tiempo específico

### Procedimiento

- 1 En **Administrador de directivas**, seleccione una categoría de directiva.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria.
- 3 En la ficha **Enumerar todos los analizadores**, haga clic en **Agregar analizador/filtro**.



La opción **Agregar analizador/filtro** está disponible solamente para la categoría de directiva **En tiempo real y Gateway**.

- 4 En la lista desplegable **Especificar la categoría**, seleccione el analizador o el filtro necesario.
- 5 En la sección **Cuándo utilizar esta instancia**, seleccione un intervalo de tiempo existente o cree uno nuevo.
- 6 Haga clic en **Guardar**.
- 7 Haga clic en **Aplicar**.




Edite las opciones y las reglas según las necesidades de la organización.

## Creación de nuevas reglas para usuarios específicos

Cree nuevas reglas y especifique las condiciones que se deben aplicar a un usuario particular.

Puede crear reglas para usuarios o grupos específicos para tener una excepción en la directiva.

## Procedimiento

- 1 En **Administrador de directivas**, seleccione una categoría de directiva.
  - 2 Haga clic en la subdirectiva que desee configurar para usuarios concretos.
  - 3 Haga clic en la ficha **Especificar usuarios**.
  - 4 Haga clic en **Nueva regla**.
  - 5 En **Especificar una regla de directiva**, puede seleccionar lo siguiente:
    - **<select a rule template>** (<seleccionar una plantilla de regla>): para especificar la regla de directiva según el remitente o el destinatario. Puede crear reglas nuevas según las siguientes opciones:
      - **La dirección SMTP del remitente es la dirección de correo electrónico**
      - **La dirección SMTP del remitente no es la dirección de correo electrónico**
      - **La dirección de SMTP de los destinatarios es la dirección de correo electrónico**
      - **La dirección de SMTP de los destinatarios no es la dirección de correo electrónico**
      - **El remitente está en el grupo de Active Directory**
      - **El remitente no está en el grupo de Active Directory**
      - **Los destinatarios están en el grupo de Active Directory**
      - **Los destinatarios no están en el grupo de Active Directory**
-  Asegúrese de no crear reglas con conflictos en las direcciones de correo electrónico o en los nombres de usuario. No se admiten expresiones regulares (regex) para usuarios especificados; solo se admiten comodines.
- **Copiar reglas de otra directiva:** para copiar reglas de otra directiva.
- 6 Haga clic en **Agregar**.
  - 7 Especifique las condiciones bajo las que la directiva debe activarse para el usuario. Puede seleccionar lo siguiente:
    - **Se aplica cualquier regla**
    - **Se aplican todas las reglas**
    - **No se aplica ninguna regla**
  - 8 Haga clic en **Aplicar** para guardar la regla del usuario específico.

## Acciones que puede realizar en las detecciones

Para cada configuración de analizador y filtro en una directiva, puede especificar una acción principal y una secundaria para realizar en una detección. Puede especificar la acción que debe realizarse con un mensaje de correo electrónico o su adjunto cuando activa una detección.

Al activarse una regla de directiva basada en la configuración del analizador o de los filtros, MSME actúa en la detección según la acción principal y la secundaria configuradas.

Al configurar acciones se debe seleccionar una acción principal como mínimo. También se pueden seleccionar varias acciones secundarias. Por ejemplo, si la acción principal es eliminar el correo electrónico que activa la detección, la acción secundaria puede ser registrar la detección y notificar al administrador.

Las acciones principales disponibles dependen del tipo de categoría de directiva y de su configuración del analizador y de los filtros.



Haga clic en **Restablecer** para restablecer las acciones a su configuración predeterminada para el analizador y la categoría de directiva.

**Tabla 4-3 Acciones principales**

Acción	Definición
<b>Intentar limpiar cualquier virus o troyano detectado</b>	Permite limpiar el correo electrónico que contiene un virus o un troyano detectado por el <b>Analizador antivirus</b> .
<b>Sustituir elemento por una alerta</b>	Permite sustituir un correo electrónico que activó la detección con una alerta.
<b>Eliminar elemento incrustado</b>	Permite eliminar el adjunto que activó la detección en un correo electrónico.
<b>Eliminar mensaje</b>	Permite eliminar el correo electrónico que activó la detección.
<b>Permitir paso</b>	Permite que el correo electrónico continúe hacia la siguiente fase de análisis o que llegue al usuario final.
<b>Score-based action (Acción basada en calificación)</b>	Permite realizar una acción basada en la calificación de spam. Está disponible solamente para el analizador antispam, en el que tiene que seleccionar <b>If the spam score is</b> (Si la calificación de spam es) alta, intermedia o baja.
<b>Enrutar a la carpeta basura de sistema</b>	Permite enrutar el correo electrónico detectado por el analizador <b>Antispam</b> a la dirección de correo electrónico especificada en <b>Configuración y diagnósticos</b>   <b>Antispam</b>   <b>Filtro antispam de gateway</b>   <b>Dirección de la carpeta de correo basura de sistema</b> .
<b>Enrutar a la carpeta de correo basura del usuario</b>	Para enrutar el correo electrónico detectado por el analizador <b>Antispam</b> a la carpeta <b>Junk E-mail</b> (Carpeta de correo basura) del destinatario.
<b>Rechazar el mensaje</b>	Permite rechazar el correo electrónico y enviarle una notificación al usuario.
<b>Sustituir el archivo adjunto por una alerta</b>	Permite reemplazar el adjunto en un mensaje de correo electrónico por una alerta, si el analizador <b>Filtrado de tamaño de correo</b> se activa cuando se excede el tamaño de adjunto.
<b>Sustituir todos los archivos adjuntos por una única alerta</b>	Permite reemplazar el mensaje de correo electrónico que contiene varios adjuntos por una sola alerta, si el analizador <b>Filtrado de tamaño de correo</b> se activa cuando se excede el conteo de adjuntos.
<b>No permitir que los cambios alteren la firma</b>	Permite impedir que MSME altere la firma cuando se detecta un mensaje de correo electrónico que incluya <b>Contenido firmado</b> .
<b>Permitir que los cambios rompan la firma</b>	Permite que MSME rompa la firma cuando se detecta un mensaje de correo electrónico que tenga <b>Contenido firmado</b> .

**Tabla 4-4 Acciones secundarias**

Acción	Definición
<b>Registro</b>	Permite incluir la detección en un registro.
<b>Cuarentena</b>	<p>Permite almacenar, en la base de datos de cuarentena, una copia del correo electrónico que activó la detección. Para visualizar todos los elementos en cuarentena, vaya a <b>Elementos detectados</b>   <b>Todos los elementos</b> o la categoría de detección específica.</p> <p>Seleccione <b>Reenviar correo electrónico en cuarentena</b> para enviar el correo electrónico a un revisor o una lista de distribución específicos, según la categoría de detección. Para configurar las notificaciones según la categoría de detección, vaya a <b>Configuración y diagnósticos</b>   <b>Notificaciones</b>   <b>Configuración</b>   <b>Avanzado</b>.</p>

La opción **Reenviar correo electrónico en cuarentena** no es aplicable para el **Analizador antivirus** o las políticas de **Gateway**.

Tabla 4-4 Acciones secundarias (continuación)

Acción	Definición
Notificar al administrador	Permite enviar una copia del correo electrónico al administrador especificado en <b>Correo electrónico del administrador</b> desde <b>Configuración y diagnósticos   Notificaciones   Configuración   General</b> .
Notificar al remitente interno	Permite enviar un mensaje de alerta al remitente interno, si el mensaje de correo electrónico se origina dentro del dominio autoritativo de Exchange Server.
Notificar a remitente externo	Permite enviar un mensaje de alerta al remitente, si el mensaje de correo electrónico original no se origina dentro del dominio autoritativo de Exchange Server.
Notificar al destinatario interno	Permite enviar un mensaje de alerta al destinatario, si el destinatario está dentro del dominio autoritativo de Exchange Server.
Notificar a destinatario externo	Permite enviar un mensaje de alerta al destinatario, si el destinatario no está dentro del dominio autoritativo de Exchange Server.

## Recurso compartido

Una ubicación común para editar configuraciones de analizadores, filtros, alertas, diccionarios de conformidad y DLP, e intervalos de tiempo. Cuando configure directivas, se recomienda que aplique el mismo recurso (configuración de analizador y filtro) a más de una directiva. En tales escenarios, use **Recurso compartido**.

Por ejemplo, si desea usar una renuncia diferente para los destinatarios internos y los externos, cree renunciaciones diferentes para los destinatarios y aplíquelas en la directiva secundaria necesaria.

En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Recurso compartido**. Puede utilizar las siguientes fichas:

- **Analizadores y alertas:** para editar o crear nuevas configuraciones de analizadores y filtros.
- **Diccionarios de conformidad y DLP:** para editar o crear nuevas **Reglas de conformidad y DLP**, y **Reglas de filtrado de archivos**.
- **Intervalos de tiempo:** para editar o crear nuevos intervalos de tiempo, como días de la semana o del fin de semana.



Cualquier cambio que se haga a estas opciones se aplica automáticamente a todas las directivas que usan estas configuraciones.


## Configurar opciones de análisis

Cree o modifique la configuración del analizador según las necesidades de la organización de Exchange.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Recurso compartido**. Aparecerá la página **Recursos compartidos**.
- 2 Haga clic en la pestaña **Analizadores y alertas**.
- 3 En la lista desplegable **Categoría** de la sección **Analizadores**, seleccione el analizador que desea configurar. El tipo de analizador aparece con el nombre de la configuración, las directivas utilizadas y la acción por configurar. Puede usar:

**Tabla 4-5 Definiciones de las opciones**

Opción	Definición
<b>Categoría</b>	Permite seleccionar el analizador que quiere configurar.
<b>Crear nueva</b>	Permite crear configuraciones nuevas según sus necesidades. Es necesaria en una situación en la que se requieren excepciones para ciertas opciones del analizador y para aplicarlas a una directiva.
<b>Editar</b>	Permite editar la configuración del analizador seleccionado.
<b>Eliminar</b>	Permite eliminar la configuración del analizador.  <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;"> <p> No puede eliminar un analizador si</p> <ul style="list-style-type: none"> <li>• Es un analizador predeterminado.</li> <li>• Lo usa alguna directiva. Para saber cuántas directivas usan esta configuración de analizador, consulte la columna <b>Utilizado por</b>.</li> </ul> </div>

4 Una vez configuradas las opciones del analizador, haga clic en **Guardar** y, a continuación, en **Aplicar**.

Ha configurado satisfactoriamente las opciones para un analizador según las necesidades de la organización de Exchange.

## Configuración de opciones de alerta

Crea o modifica las opciones de alerta del analizador seleccionado para ajustarlas según las necesidades de la organización de Exchange.

### Procedimiento


- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Recurso compartido**.  
Aparecerá la página **Recursos compartidos**.
- 2 Haga clic en la pestaña **Analizadores y alertas**.
- 3 En la lista desplegable **Categoría** de la sección **Alertas**, seleccione la alerta que desea configurar para el analizador. El tipo de analizador aparece con el nombre de la configuración, las directivas utilizadas y la acción por configurar. Puede usar:

**Tabla 4-6 Definiciones de las opciones**

Opción	Definición
<b>Categoría</b>	Permite seleccionar el analizador que quiere configurar.
<b>Crear nueva</b>	Permite crear configuraciones nuevas según sus necesidades. Es necesaria en una situación en la que se requieren excepciones para ciertas opciones del analizador y para aplicarlas a una directiva.
<b>Ver</b>	Permite ver la configuración de alertas predeterminada de un analizador.



**Tabla 4-6 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Editar</b>	Permite editar la configuración del analizador seleccionado. Para obtener más información sobre las variables que puede usar en las alertas, consulte la sección <i>Campos de notificación que puede usar</i> .
<b>Eliminar</b>	Permite eliminar la configuración del analizador.  <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p> No puede eliminar una alerta si</p> <ul style="list-style-type: none"> <li>• es una alerta predeterminada del analizador.</li> <li>• la usa alguna directiva. Para saber cuántas directivas usan esta configuración de alertas, consulte la columna <b>Utilizado por</b>.</li> </ul> </div>

- 4 Una vez configuradas las opciones del analizador, haga clic en **Guardar** y, a continuación, en **Aplicar**.

Ha configurado satisfactoriamente las opciones para una alerta según las necesidades de la organización de Exchange.

## Crear una alerta

Cree un mensaje de alerta para las acciones realizadas por un analizador o filtro.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas** | **Recurso compartido**.  
Aparecerá la página **Recursos compartidos**.
- 2 Haga clic en la pestaña **Analizadores y alertas**.
- 3 En la lista desplegable **Categoría** de la sección **Alertas**, seleccione la alerta que desea configurar para el analizador.
- 4 Haga clic en **Crear nuevo**.  
Aparecerá la página **Editor de alertas**.
- 5 Introduzca un **Nombre de alerta** significativo.
- 6 Seleccione las opciones de **Estilo**, **Fuente**, **Tamaño** y **Tokens** de las listas desplegables correspondientes.



Estas opciones están disponibles solamente si selecciona **Contenido HTML (WYSIWYG)** en el menú desplegable **Mostrar**.

7 Utilice una de estas herramientas para personalizar la alerta:



**Tabla 4-7 Opciones de la barra de herramientas**

Opciones	Descripción
Negrita	Permite poner el texto seleccionado en negrita.
Cursiva	Permite poner el texto seleccionado en cursiva.
Subrayado	Permite subrayar el texto seleccionado.
Alinear a la izquierda	Permite alinear a la izquierda el párrafo seleccionado.
Centrar	Permite centrar el párrafo seleccionado.
Alinear a la derecha	Permite alinear a la derecha el párrafo seleccionado.
Justificar	Permite ajustar el párrafo seleccionado de modo que las líneas dentro del párrafo ocupen una anchura dada, con los bordes izquierdo y derecho rectos.
Lista ordenada	Permite poner el texto seleccionado en una lista numerada.
Lista sin ordenar	Permite poner el texto seleccionado en una lista con viñetas.
Anular sangría	Permite mover el texto seleccionado a una distancia establecida hacia la derecha.
Sangrar	Permite mover el texto seleccionado a una distancia establecida hacia la izquierda.
Color del texto	Permite cambiar el color del texto seleccionado.
Color de fondo	Permite cambiar el color de fondo del texto seleccionado.
Regla horizontal	Permite insertar una línea horizontal.
Insertar vínculo	Permite insertar un hipervínculo donde se encuentra el cursor actualmente. En <b>URL</b> , introduzca la URL. En <b>Texto</b> , introduzca el nombre del hipervínculo como quiere que aparezca en el mensaje de alerta. Si quiere que el vínculo se abra en una nueva ventana, seleccione <b>Abrir vínculo</b> en una nueva ventana, después haga clic en <b>Insertar vínculo</b> .
Insertar imagen	Permite insertar una imagen donde se encuentra el cursor actualmente. En <b>Dirección URL de la imagen</b> , introduzca la ubicación de la imagen. En <b>Texto alternativo</b> , introduzca el texto que quiere usar en lugar de la imagen cuando se suprimen las imágenes o cuando se muestra el mensaje de alerta en un navegador de solo texto. Si quiere dar a la imagen un título, introduzca el nombre del título en <b>Usar este texto como título de la imagen</b> . Haga clic en <b>Insertar imagen</b> .
Insertar tabla	Permite insertar una tabla en la posición actual del cursor. Introduzca valores en <b>Filas</b> , <b>Columnas</b> , <b>Ancho de la tabla</b> , <b>Grosor del borde</b> , <b>Relleno de celdas</b> y <b>Espaciado entre celdas</b> para configurar la tabla, después haga clic en <b>Insertar tabla</b> .

- 8 En el menú desplegable **Mostrar**, especifique la manera en que el mensaje de alerta deberá mostrarse en la interfaz de usuario. Puede seleccionar:
- **Contenido HTML (WYSIWYG)**: permite ocultar el código HTML subyacente y mostrar solamente el contenido del mensaje de alerta.
  - **Contenido HTML (origen)**: permite visualizar el mensaje de alerta con el código HTML como aparece antes de la compilación.
  - **Contenido de texto sin formato**: permite visualizar el contenido como texto sin formato.

Puede usar los siguientes campos de notificación para incluirlos en el mensaje de alerta. Por ejemplo, en su mensaje de alerta, si quiere que aparezcan el nombre del elemento detectado y las acciones realizadas cuando se detectó, use **%vrs%** y **%act%** en la página **Editor de alertas**. Para obtener más información acerca de las opciones de campo de notificación, consulte la sección *Campos de notificación que puede usar*.



McAfee recomienda que se guarden los archivos de registro en formato de texto simple para que el contenido se pueda visualizar mediante un cliente de correo electrónico.

- 9 Haga clic en **Guardar** para volver a la página de la directiva.



Haga clic en **Restablecer** para deshacer todos los cambios realizados desde que guardó por última vez el mensaje de alerta.

## Configuración de reglas de conformidad y DLP

Cree o modifique diccionarios y reglas de conformidad y DLP para satisfacer las necesidades de la organización de Exchange.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Recurso compartido**.

Aparecerá la página **Recursos compartidos**.

- 2 Haga clic en la ficha **Diccionarios de conformidad y DLP**.



- 3 En la lista desplegable **Seleccione un idioma** en la sección **Reglas de conformidad y DLP**, seleccione el idioma.



También puede ver y editar todos los diccionarios de configuraciones regionales admitidas. (Las configuraciones regionales admitidas son Chino simplificado, Francés, Alemán, Japonés y Español.)

- 4 En la lista desplegable **Categoría** de la sección **Reglas de conformidad y DLP**, seleccione la categoría que desea ver o configurar. El grupo de reglas aparecerá con el nombre, las políticas utilizadas y la acción que se debe configurar. Puede usar:

Tabla 4-8 Definiciones de las opciones

Opción	Definición
<b>Categoría</b>	<p>Para seleccionar el analizador necesario que desea configurar. Esta versión cuenta con 60 diccionarios más de conformidad y DLP, lo que garantiza que el contenido de los correos electrónicos cumpla con las directivas de conformidad y confidencialidad de la organización.</p> <p>Los diccionarios de conformidad predefinidos incluyen:</p> <ul style="list-style-type: none"> <li>• Incorporación de 60 nuevos diccionarios de conformidad y DLP</li> <li>• Compatibilidad con diccionarios de conformidad específicos del sector, como HIPAA, PCI, código fuente (Java, C++, etc.)</li> </ul> <p>Los diccionarios se categorizan de la siguiente manera:</p> <ul style="list-style-type: none"> <li>• Basados en calificaciones: se activa una regla cuando el correo electrónico excede el umbral de calificación y el recuento máximo de términos, lo que reduce los falsos positivos.</li> <li>• No basados en calificaciones: se activa una regla cuando se encuentra una palabra o una frase en el mensaje de correo electrónico.</li> </ul>
<b>Nueva categoría</b>	<p>Permite crear un nuevo diccionario de <b>Reglas de conformidad y DLP</b>.</p> <p> Cualquier nueva categoría o condición que cree es no basada en calificación.</p>
<b>Crear nueva</b>	<p>Para crear un nuevo grupo de reglas para la categoría seleccionada en función de sus necesidades. Se precisa en una situación en la que necesita reglas específicas para la activación de una detección y su aplicación en una directiva.</p>
<b>Editar</b>	<p>Permite editar la configuración de una regla de <b>Conformidad y DLP</b> seleccionada.</p>
<b>Eliminar</b>	<p>Permite eliminar la regla de <b>Conformidad y DLP</b>.</p> <p> No puede eliminar una regla de <b>Conformidad y DLP</b> en los casos siguientes</p> <ul style="list-style-type: none"> <li>• Está activada. Anule la selección de la regla, haga clic en <b>Aplicar</b> para la configuración y luego en <b>Eliminar</b>.</li> <li>• La usa alguna directiva. Para saber cuántas directivas usan esta configuración de analizador, consulte la columna <b>Utilizado por</b>.</li> </ul>



Por ejemplo, seleccione **Número de tarjeta de crédito** o cualquier diccionario que satisfaga sus necesidades en la lista desplegable **Categoría** y observe la opción mejorada **Grupo de reglas** disponible.

- Para crear un nuevo grupo de reglas, haga clic en **Crear nueva de Reglas de conformidad y DLP** correspondiente a una categoría seleccionada.
- Aparece la página **Nueva regla de analizador de conformidad y DLP** para la categoría seleccionada.
- Introduzca **Nombre de regla** y **Descripción** para la regla.
  - Seleccione **Agregar esta regla al grupo de reglas de esta categoría** para agregar la nueva regla al grupo de reglas de la categoría seleccionada.
  - En **Palabra o frase**, especifique las palabras o frases que se deben buscar en **La regla se activará cuando se encuentre la siguiente palabra o expresión**. A continuación, seleccione una de las siguientes opciones:
    - **Expresión regular**: si está activada, la regla se activa en para el texto especificado que sea una expresión regular (regex). Regex es un método preciso y conciso para hacer coincidir cadenas de texto, tales como palabras, caracteres o patrones de caracteres.

Por ejemplo, la secuencia de caracteres "árbol" que aparece consecutivamente en cualquier contexto, como arboleda, arboladura o arbolar.



- La función regex está desactivada para algunas frases.
- Consulte <http://www.regular-expressions.info/reference.html> o <http://www.zytrax.com/tech/web/regex.htm> para obtener más detalles.

- **Usar comodín:** si está activada, la regla se activa para la palabra o la frase especificada que contenga los caracteres comodín. (Los caracteres comodín se usan frecuentemente en lugar de uno o más caracteres, cuando no sabe cuál es el carácter real o no quiere introducir el nombre entero).
- **Empieza por:** si está activada, la regla se activa para el texto especificado que forma el principio de la palabra o la frase.
- **Termina por:** si está activada, la regla se activa para el texto especificado que forma el final de la palabra o la frase.
- **Distinción mayúsculas/minúsculas:** si está activada, se activa la regla si las mayúsculas o las minúsculas del texto especificado coinciden con las de la palabra o las de la frase.



Para detectar una palabra o frase con coincidencia exacta, seleccione las opciones **Empieza con** y **Termina con**.

- 9 Seleccione **Especificar otras palabras del contexto o expresiones**, que es una acción secundaria cuando se detecta la palabra o la frase primaria. Especifique cualquier palabra o frase adicional que pueda acompañar a la palabra o la frase primaria que active la detección.
- 10 Seleccione **Activar si TODAS las frases están presentes**, **Activar si hay ALGUNA frase presente** o **Activar si no hay NINGUNA frase presente** en el menú desplegable.
- 11 Seleccione **dentro de un bloque de** para especificar el número de **Caracteres** de un bloque que se analizará.
- 12 Haga clic en **Agregar palabra contextual** para introducir palabras o expresiones adicionales.
- 13 Especifique la palabra o la frase en **Especificar palabras o frases**, seleccione una de las condiciones (las mismas opciones que en el paso 7), después haga clic en **Agregar**.
- 14 En **Formato de archivo**, seleccione **Todo** para activar todas las categorías de archivos y sus subcategorías. Puede seleccionar varias categorías y tipos de archivos en las categorías seleccionadas coincidentes. Al seleccionar **Todo** en el selector de la subcategoría se anulará cualquier otra selección ya hecha.
- 15 Si no ha seleccionado **Todo**, haga clic en **Borrar selecciones** para quitar la selección de cualquier opción del tipo de archivo seleccionado.
- 16 Haga clic en **Guardar** para volver a la página **Recursos compartidos**.
- 17 Haga clic en **Aplicar** para guardar la configuración.

Ha configurado satisfactoriamente diccionarios y reglas de conformidad y DLP para satisfacer las necesidades de la organización de Exchange.

## Configuración de reglas de filtrado de archivos

Cree nuevas reglas para detectar archivos según el nombre, el tipo o el tamaño.

### Antes de empezar

La regla de filtrado de archivos se activa solamente cuando selecciona una condición. Asegúrese de crear una regla individual para cada una de las siguientes categorías:

- Nombre de archivo
- Categoría de archivo
- Tamaño de archivo



Esta tarea proporciona información para configurar las tres categorías. Según los requisitos de la organización de Exchange, seleccione solo una categoría para una regla de filtrado de archivos y cree diferentes reglas para cada categoría. Si una regla contiene varias categorías, como **Filtrado de nombres de archivo**, **Filtrado de categorías de archivo** y **Filtrado de tamaños de archivo**, se deben cumplir todos los criterios para activar la regla.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Recurso compartido**.
- 2 Haga clic en la ficha **Diccionarios de conformidad y DLP**.
- 3 En **Reglas de filtrado de archivos**, haga clic en **Crear nueva**.
- 4 Introduzca un **Nombre de regla** único. Dé a la regla un nombre significativo, de modo que pueda identificarla y conocer su función fácilmente. Por ejemplo, Bloquear MPP o ArchivosMayoresA5MB.
- 5 Active **Evaluar elementos dentro de archivos de almacenamiento**.



Seleccione esta opción si la regla Filtro de archivos es aplicable para analizar los archivos de almacenamiento. Al seleccionar esta regla, las reglas Filtro de archivos subsiguientes se aplican a los archivos de almacenamiento.

- 6 En la página **Regla de filtrado de archivo**, puede usar lo siguiente.


**Tabla 4-9 Definiciones de las opciones: filtrado de nombres de archivo**

Opción	Definición
<b>Activar filtrado de nombres de archivo</b>	Para activar el filtrado de archivos por sus nombres.
<b>Llevar a cabo la acción si el nombre del archivo coincide con</b>	Especifique el nombre de los archivos que activan esta regla. Puede usar caracteres comodín (* o ?) para hacer coincidir varios nombres de archivo. Por ejemplo, si quiere filtrar archivos de Microsoft PowerPoint, introduzca *.ppt.
<b>Agregar</b>	Permite añadir el nombre de archivo especificado en <b>Realizar acción cuando el nombre de archivo coincida con</b> a la lista de filtrado de nombres de archivo.
<b>Editar</b>	Para editar o modificar una regla de filtrado de archivos existente.
<b>Eliminar</b>	Para quitar el nombre de archivo de la lista de filtrado.



No puede eliminar una regla de filtrado de archivos si la utiliza una directiva. La columna **Utilizado por** deberá mostrar **0 directivas** para la regla que desea eliminar. Primero deberá eliminar de la directiva la regla de filtrado de archivos; luego haga clic en **Eliminar**.

**Tabla 4-10 Definiciones de las opciones. Filtrado de categoría de archivo**

Opción	Definición
Activar filtrado de categorías de archivo	Para activar el filtrado de archivos de acuerdo con el tipo de archivo.
Llevar a cabo la acción cuando la categoría de archivo es	<p>Especifique el tipo de archivo que afecta a esta regla.</p> <p> Los tipos de archivos se dividen en categorías y subcategorías.</p>
Categorías de archivos	Seleccione una categoría de tipo de archivo. Un símbolo de asterisco (*) aparecerá junto al tipo de archivo para indicar que se filtrará el tipo de archivo seleccionado.
Subcategorías	<p>Seleccione la subcategoría que desea filtrar.</p> <p>Para seleccionar más de una subcategoría, haga <b>Ctrl+Clic</b> o <b>Mayús+Clic</b>.</p> <p>Para seleccionar todas las subcategorías, haga clic en <b>Todas</b>.</p> <p>Haga clic en <b>Borrar selecciones</b> para deshacer la última selección.</p>
Ampliar esta regla a categorías de archivos no reconocidas	Para aplicar esta regla a cualquier otra categoría o subcategoría de archivos no mencionadas en la lista de categorías y subcategorías.



Para permitir el acceso de archivos .zip protegidos con contraseña que contienen archivos restringidos, asegúrese de que la **Regla para omitir protegida con contraseña** sea la primera regla de la lista.

**Tabla 4-11 Definiciones de las opciones. Filtrado de tamaño de archivo**

Opción	Definición
Activar filtrado de tamaños de archivo	Para filtrar archivos según su tamaño.
Llevar a cabo la acción cuando el tamaño del archivo sea	<p>Especifique un valor en el cuadro de texto adyacente y la lista desplegable y, a continuación, seleccione:</p> <ul style="list-style-type: none"> <li>• <b>Superior a:</b> para especificar que la acción solamente debe ser aplicada si el archivo es mayor que el tamaño especificado.</li> <li>• <b>Inferior a:</b> para especificar que la acción solamente debe ser aplicada si el archivo es menor que el tamaño especificado.</li> </ul>

7 Haga clic en **Guardar** para volver a la página **Recursos compartidos**.

8 Haga clic en **Aplicar** para crear la regla de filtrado de archivos.

Ha creado satisfactoriamente la regla de filtrado de archivos según el requisito de la organización de Exchange.

## Configuración de intervalos de tiempo

Configure intervalos de tiempo diferentes o existentes que se puedan aplicar a las directivas según las necesidades de la organización de Exchange.

La opción **Intervalos de tiempo** le permite especificar el tiempo durante el que se deben activar determinadas reglas. Por ejemplo, puede restringir la carga o descarga de archivos grandes durante el horario de oficina.

Puede suceder que necesite mayores intervalos de tiempo, según los diferentes usuarios, las ubicaciones geográficas o las horas de trabajo. Puede crear más intervalos de tiempo según las horas laborables, las horas no laborables, el mantenimiento semanal, etc.

De manera predeterminada, MSME ofrece los siguientes intervalos de tiempo:

- **Todo el tiempo**
- **Días de la semana**
- **Fines de semana**



No es posible eliminar ni editar el intervalo de tiempo predeterminado **Todo el tiempo**, dado que la utiliza la **Directiva principal**.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas** | **Recurso compartido**.  
Aparecerá la página **Recursos compartidos**.
- 2 Haga clic en la ficha **Intervalos de tiempo**.
- 3 Haga clic en **Crear nuevo**.  
Aparecerá la página **Intervalo de tiempo**.
- 4 Introduzca un **Nombre del intervalo de tiempo** único, como `Horas laborables` o `Mantenimiento del sistema (semanal)`.
- 5 En **Seleccionar día y hora**, seleccione los días para realizar la acción.
- 6 Seleccione **Todo el día** o la opción **Horas seleccionadas**.
- 7 Especifique la hora de **Inicio** y **Fin** de la lista desplegable, si la opción elegida es **Horas seleccionadas**.
- 8 Haga clic en **Guardar** para volver a la página **Recursos compartidos**.
- 9 Haga clic en **Aplicar** para guardar la configuración.

Ha configurado o creado satisfactoriamente el intervalo de tiempo según el requisito de la organización de Exchange.

## Administración de opciones del analizador principal para una directiva

Cree o edite opciones del analizador y especifique llevar a cabo una acción adecuada sobre el elemento detectado cuando se activa una directiva.

Los analizadores principales disponibles son:

- **Analizador antivirus**
- **Analizador de conformidad y DLP**
- **Filtrado de archivos**
- **Antispam**
- **Antiphishing**



## Procedimientos

- *Configuración del analizador antivirus en la página 73*  
Configure el **Analizador antivirus** en una directiva para identificar, frustrar y eliminar virus informáticos y otro malware.
- *Configuración del analizador de conformidad y DLP en la página 76*  
Configure el **Analizador de conformidad y DLP** en una directiva para identificar datos de texto que no cumplen las normativas en un correo electrónico o un adjunto y realizar las acciones necesarias.
- *Configuración de opciones de filtrado de archivos en la página 78*  
Configure las opciones de una directiva para detectar archivos según el nombre, el tipo o el tamaño, y para llevar a cabo las acciones necesarias.
- *Configuración de parámetros de reputación de URL de correo en la página 79*  
Configure los parámetros de **Reputación de URL de correo** para detectar URL maliciosas en el cuerpo del mensaje de correo electrónico.
- *Comprobación de reputación de TIE para datos adjuntos de correo electrónico en la página 82*  
MSME proporciona ahora capacidades de detección de amenazas adicionales; con este fin, emplea la comprobación de reputación de TIE para los datos adjuntos que proceden de mensajes de correo electrónico en los niveles de puerta de enlace, concentrador y buzón.
- *Configuración de TIE para analizar los datos adjuntos de correo electrónico en la página 84*  
Active la comprobación de reputación de TIE para los datos adjuntos de correo electrónico en función de la categoría de reputación de archivos.
- *Configuración de antispam en la página 85*  
Configure las opciones de una directiva para identificar mensajes de correo electrónico con spam y llevar a cabo las acciones necesarias.
- *Configuración de antiphishing en la página 90*  
Configure una directiva para bloquear mensajes de phishing mediante el motor y reglas antispam, y llevar a cabo las acciones necesarias.

## Configuración del analizador antivirus

Configure el **Analizador antivirus** en una directiva para identificar, frustrar y eliminar virus informáticos y otro malware.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento en el menú secundario que tenga el analizador antivirus.  
  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Analizador antivirus**.
- 4 En **Activación**, seleccione **Activar** a fin de activar la configuración del analizador antivirus para el elemento de submenú seleccionado.



- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si añade un nuevo analizador a la directiva, puede especificar un intervalo de tiempo para que el analizador se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

5 En la sección **Opciones**, puede usar lo siguiente.

Opción	Definición
<b>Protección alta</b>	Permite analizar todos los archivos, archivos de almacenamiento, virus desconocidos, virus de macro desconocidos, software de envío masivo de correo y programas potencialmente no deseados en busca de macros.
<b>Protección media</b>	Permite analizar todos los archivos, archivos de almacenamiento, virus desconocidos, virus de macro desconocidos, software de envío masivo de correo y programas potencialmente no deseados.
<b>Baja protección</b>	Permite analizar solamente los tipos de archivos, archivos de almacenamiento, software de envío masivo de correo y programas potencialmente no deseados predeterminados.
<b>&lt;create new set of options&gt;</b>	Para crear la configuración del analizador antivirus personalizada.
<b>Editar</b>	Para editar el nivel de protección existente.

6 Si selecciona editar o modificar la configuración del analizador, en **Nombre de instancia**, escriba un nombre único para la instancia de configuración de analizador antivirus. Este campo es obligatorio.

7 En la ficha **Opciones básicas** correspondiente a **Especificar los archivos para analizar**, seleccione una de las opciones siguientes.

- **Analizar todos los archivos:** para especificar que hay que analizar todos los archivos, sin importar su tipo.
- **Tipos de archivos predeterminados:** para especificar que solamente los tipos de archivos predeterminados deben ser analizados.
- **Tipos de archivos definidos:** para especificar qué tipos de archivos deben ser analizados.

8 Seleccione otras opciones disponibles en **Opciones de analizador**. Puede seleccionar lo siguiente:

- **Analizar archivos de almacenamiento (ZIP, ARJ, RAR...)**
- **Buscar virus de archivo desconocidos**
- **Buscar virus de macro desconocidos**
- **Activar reputación de archivos de McAfee Global Threat Intelligence:** activa la información sobre amenazas recolectada por McAfee Labs para evitar daños y robo de datos incluso antes de que esté disponible una actualización de firma. Seleccione el nivel de confidencialidad entre las opciones disponibles.
- **Analizar todos los archivos de macro**
- **Buscar todas las macros y tratar como infectadas**
- **Quitar todas las macros de los archivos de documento**



Las opciones **Buscar todas las macros y tratar como infectadas** y **Quitar todas las macros de los archivos de documento** tienen una funcionalidad combinada. Cuando se selecciona **Buscar todas las macros y tratar como infectadas**, la opción **Quitar todas las macros de los archivos de documento** se selecciona de forma automática. Cuando se activa esta opción, todas las macros de los datos adjuntos se tratan como si estuvieran infectadas.

9 En la ficha **Avanzadas** correspondiente a **Categorías de malware personalizado**, especifique los elementos que se tratarán como malware. Hay dos maneras de seleccionar los tipos de malware:

- Seleccione los tipos de malware en la lista con casillas de verificación.
- Seleccione **Nombres de detección específicos**, introduzca una categoría de malware, después haga clic en **Agregar**.



Al introducir el nombre de la categoría de malware, puede utilizar caracteres comodín para la coincidencia de modelos.

- 10** Seleccione la opción **No realice la verificación de malware personalizada si el objeto ya se ha limpiado**, si los elementos limpiados no deben someterse a la verificación de malware personalizada.
- 11** En **Opciones de limpieza**, especifique qué sucede con los archivos reducidos a cero bytes después de la limpieza. Seleccione cualquiera de las opciones siguientes.
- **Conservar el archivo de cero bytes:** sirve para guardar los archivos limpiados de cero bytes.
  - **Eliminar archivo de cero bytes:** sirve para quitar cualquier archivo de cero bytes tras haber sido limpiado.
  - **Tratar como un error al limpiar:** para tratar los archivos de cero bytes como si no hubieran sido limpiados y aplicar la acción de error al limpiar.
- 12** En la ficha **Herramientas de compresión**, seleccione lo siguiente.
- **Activar detección:** permite activar o desactivar la detección de compresores.
  - **Excluir nombres especificados:** permite especificar qué compresores pueden ser excluidos del análisis.
  - **Incluir solo nombres especificados:** permite especificar qué compresores quiere que el software detecte.
  - **Agregar:** permite agregar nombres de compresores a una lista. Puede usar caracteres comodín para hacer coincidir varios nombres.
  - **Eliminar:** permite quitar nombres de compresores que haya agregado. Se activa este vínculo al hacer clic en **Agregar**.
- 13** En la ficha **Programas potencialmente no deseados**, seleccione lo siguiente.
- **Activar detección:** para activar o desactivar la detección de programas potencialmente no deseados. Haga clic en el vínculo de renuncia y lea la renuncia antes de configurar la detección de programas potencialmente no deseados.
  - **Seleccionar los tipos de programa que detectar:** para especificar si cada tipo de programa potencialmente no deseado de la lista debe ser detectado o ignorado.
  - **Excluir nombres especificados:** para especificar qué programas potencialmente no deseados pueden ser excluidos del análisis. Por ejemplo, si ha activado la detección de spyware, puede crear una lista de programas de spyware que quiere que el software ignore.
  - **Incluir solo nombres especificados:** para especificar qué programas potencialmente no deseados quiere que detecte el software. Por ejemplo, si activa la detección de spyware y especifica que solamente los programas nombrados de spyware deben detectarse, se ignorarán el resto de programas de spyware.
  - **Agregar:** para añadir nombres de programas potencialmente no deseados a una lista. Puede usar caracteres comodín para hacer coincidir varios nombres.
  - **Eliminar:** para eliminar nombres de programas potencialmente no deseados que haya añadido. Se activa este vínculo al hacer clic en **Agregar**.



El sitio web de [McAfee Threat Intelligence Services](#) incluye una lista de nombres de malware reciente. Use **Search the Threat Library** (Buscar en la biblioteca de amenazas) para consultar información acerca de malware específico.

- 14** Haga clic en **Guardar** para volver a la página de la directiva.

15 En **Acciones para realizar**, haga clic en **Editar**. En las siguientes fichas, especifique las acciones de analizador antivirus que se deben realizar al detectarse un virus (o un comportamiento similar al de un virus).

- **Limpieza:** seleccione **Intentar limpiar cualquier virus o troyano detectado** para activar varias acciones. Seleccione las acciones para realizar en:
  - **Registro**
  - **Poner en cuarentena**
  - **Notificar al administrador**
  - **Notificar al remitente interno**
  - **Notificar a remitente externo**
  - **Notificar al destinatario interno**
  - **Notificar a destinatario externo**
- **Acciones predeterminadas:** en la lista desplegable **Realizar la siguiente acción**, seleccione una acción.
  - **Sustituir elemento por una alerta**
  - **Eliminar elemento incrustado**
  - **Eliminar mensaje**
  - **Permitir paso**



Para obtener más información sobre las acciones principales y secundarias, consulte la sección *Acciones que puede realizar en las detecciones*.

16 Seleccione el documento de alerta correspondiente o haga clic en **Crear** para crear un nuevo documento de alerta. En **Y también**, seleccione otras acciones adicionales que realizar en estas fichas:

- **Software malicioso personalizado**
- **Compresores**
- **Programas potencialmente no deseados**

17 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.

18 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración del analizador de conformidad y DLP

Configure el **Analizador de conformidad y DLP** en una directiva para identificar datos de texto que no cumplen las normativas en un correo electrónico o un adjunto y realizar las acciones necesarias.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento en el menú secundario que tenga el analizador **Conformidad y DLP**.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Analizador de conformidad y DLP**.

- 4 En **Activación**, seleccione **Activar** para activar la configuración del analizador de conformidad y DLP para el elemento del menú secundario seleccionado.



- De forma predeterminada, todas las opciones de configuración del analizador están desactivadas para **Analizador de conformidad y DLP**.
- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si añade un nuevo analizador a la directiva, puede especificar un intervalo de tiempo para que el analizador se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 5 En **Opciones**, puede usar:

- **Incluir formatos de documento y de base de datos:** para analizar formatos de documentos y bases de datos en busca de contenido que no cumple las normativas.
- **Analizar el texto de todos los archivos adjuntos:** sirve para analizar el texto de todos los archivos adjuntos.
- **Crear:** para crear un mensaje de alerta cuando el contenido de un correo electrónico se sustituye debido a la activación de una regla. Consulte *Creación de una alerta* para obtener más instrucciones.
- **Ver/ocultar:** sirve para mostrar u ocultar la vista previa del mensaje de alerta. Si se oculta la vista previa, al hacer clic en este vínculo se mostrará. Si se muestra la vista previa, al hacer clic en este vínculo se ocultará.

- 6 En **Directivas y acciones asociadas de conformidad y DLP**, haga clic en **Agregar regla**.

Aparecerá la página **Reglas de conformidad y DLP**.

- 7 Dentro de **Especificar acciones para la regla**, seleccione el idioma en el menú desplegable **Seleccionar un idioma**.

También puede ver y editar todos los diccionarios de configuraciones regionales admitidas. (Las configuraciones regionales admitidas son Chino simplificado, Francés, Alemán, Japonés y Español.)

Por ejemplo, cuando se ha instalado MSME en la configuración regional Alemán, se pueden ver igualmente los diccionarios de otras configuraciones regionales admitidas. Cualquier categoría que cree estará disponible en todas las configuraciones regionales admitidas.

- 8 En **Especificar acciones para la regla**, seleccione un grupo de reglas del menú desplegable **Seleccionar grupo de reglas** que active una acción si se infringe una o varias reglas. Cada frase puede tener una **Calificación** establecida para una categoría en la **Frase de Analizador de conformidad y DLP**.

Para algunos grupos de reglas, es posible que deba especificar las opciones siguientes:

- **Umbral de calificación:** para especificar el umbral de calificación máxima en el que se activa el analizador.
- **Número máx. de términos:** para especificar la cantidad máxima de veces que este grupo de reglas se puede activar. Cuando se excede esta cantidad, se activa el analizador para realizar la acción especificada.

La ecuación del actual **Umbral de calificación** = **Calificación** x **Número de términos** (instancia). Se activa una regla cuando el valor es mayor o igual que el **Umbral de calificación**.

Para comprender cómo ayudan el **Umbral de calificación** y el **Número máx. de términos** a activar una regla, consideremos un ejemplo del diccionario de lenguaje Pascal. Supongamos que tiene una **Calificación** de la **Frase de Analizador de conformidad y DLP** "PAnsiChar" de 5.

En **Seleccionar grupo de reglas**, si seleccionó el diccionario de **Pascal Language** (Lenguaje Pascal) y estableció el valor de:

- **Umbral de calificación** = 15
- **Número máx. de términos** = 4

Si se encuentra dos veces "PAnsiChar" en el código, el umbral de calificación actual será 10, y NO se activará la regla.

Si "PAnsiChar" se encuentra cinco veces en el código, el umbral de calificación actual se seguirá calculando como **Calificación x Número máx. de términos** que es  $5 * 4 = 20$ . Este valor es mayor que el umbral de calificación definido. Por consiguiente, se activa la regla.

Supongamos que modifica la **Calificación** de "PAnsiChar" a 8. Si la frase "PAnsiChar" se encuentra tres veces en el código, el umbral de calificación actual es 24. Ahora la regla se activa, ya que excedió el **Umbral de calificación** especificado.

Si hay varias reglas, el **Umbral de calificación** es el valor combinado de todas las reglas de un diccionario.



Una regla se activa solamente cuando el valor es mayor o igual que el **Umbral de calificación** y no se activa aunque la instancia de la frase exceda el valor de **Número máx. de términos** de un correo electrónico.

- 9 En **En caso de detección, realizar la siguiente acción:**, seleccione las acciones que debe realizar el analizador de conformidad y DLP en caso de detectar contenido que no cumple las normativas en un correo electrónico.
- 10 En **Y también**, seleccione una o más acciones.
- 11 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.
- 12 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de opciones de filtrado de archivos

Configure las opciones de una directiva para detectar archivos según el nombre, el tipo o el tamaño, y para llevar a cabo las acciones necesarias.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el analizador **Filtrado de archivos**.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Filtrado de archivos**.
- 4 En **Activación**, seleccione **Activar** a fin de activar la configuración del analizador de filtrado de archivos para el elemento de submenú seleccionado.




- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si añade un analizador a la directiva, puede especificar un intervalo de tiempo para que el analizador se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**.


- 5 Seleccione **Analizar archivos incrustados** para analizar los mensajes de correo electrónico incrustados.

- 6 En **Selección de alertas**, haga clic en las opciones siguientes.
  - **Crear**: para crear un mensaje de alerta cuando el adjunto de un correo electrónico se sustituye debido a la activación de una regla. Consulte *Creación de una alerta* para obtener más instrucciones.
  - **Ver/ocultar**: sirve para mostrar u ocultar la vista previa del mensaje de alerta. Si se oculta la vista previa, al hacer clic en este vínculo se mostrará. Si se muestra la vista previa, al hacer clic en este vínculo se ocultará.
- 7 En **Reglas de filtrado de archivo y acciones asociadas**, seleccione una regla disponible en el menú desplegable **Reglas disponibles**. Si desea crear reglas de filtrado de archivos nuevas, seleccione **<Crear nueva regla...>**. Para obtener más instrucciones sobre cómo crear nuevas reglas de filtrado de archivos, véase *Configuración de las reglas de filtrado de archivos*.

La configuración de filtrado de archivos puede bloquear archivos restringidos como, por ejemplo, .exe, adjuntados a mensajes de correo electrónico. Si el archivo .exe se envía como archivo .zip protegido con contraseña, aunque el parámetro **Archivos protegidos con contraseña** esté configurado para permitir el archivo, la regla de filtrado de archivos puede bloquearlo.

A veces es preciso permitir que los archivos restringidos legítimos lleguen como archivos .zip protegidos con contraseña. Para permitir el archivo .zip protegido con contraseña que contiene archivos restringidos (por ejemplo, .exe), debe agregar **Regla para omitir protegido con contraseña** en la lista desplegable **Reglas disponibles**.

 Asegúrese de que esta regla sea la primera de la lista. Si la regla ya aparece, pero en un nivel diferente, elimínela y luego selecciónela en la lista desplegable **Reglas disponibles**.

 Asegúrese de crear reglas de filtrado de archivos diferentes para cada categoría, por ejemplo, nombre, tipo y tamaño de archivo.
- 8 Haga clic en **Cambiar** para especificar acciones que se deben llevar a cabo cuando un archivo/adjunto de un mensaje de correo electrónico activa el analizador.
- 9 Haga clic en **Eliminar** para eliminar reglas existentes de una directiva.
- 10 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de parámetros de reputación de URL de correo

Configure los parámetros de **Reputación de URL de correo** para detectar URL maliciosas en el cuerpo del mensaje de correo electrónico.

Cuando se ha activado, MSME analiza cada URL en el cuerpo del correo electrónico, obtiene la calificación de reputación, compara dicha calificación con el umbral definido, y realiza la acción pertinente según la configuración.

El software procesa el mensaje antes de que este entre en la organización quitando las URL del cuerpo del mensaje de correo electrónico. Si un mensaje de correo electrónico contiene varias URL, y una de ellas excede el umbral definido, la acción se realiza en el mensaje según la configuración.

La activación de esta función protege el sistema frente a amenazas como los ataques de denegación de servicio (DoS), los vínculos de phishing, y las URL no deseadas o que contienen malware.

La función de reputación de URL de correo está disponible para estas directivas:

- **En tiempo real**
- **Bajo demanda (predeterminado), y**
- **Bajo demanda (análisis completo)**

Según la opción de configuración que haya seleccionado durante la instalación del software, la reputación de URL de correo se activará o desactivará de forma predeterminada para las directivas:

- En la **configuración predeterminada**: desactivada para todas las directivas.
- En la **configuración mejorada**: activada para las directivas de análisis en tiempo real.

Al activar la **reputación de URL de correo** por primera vez, el software descarga la caché local de las URL del servidor de McAfee GTI.

Para cada URL, el software comprueba con la base de datos local la calificación de reputación y realiza la acción pertinente según la configuración. Si la calificación de reputación no está disponible en la base de datos local, el software obtiene la calificación del servidor de McAfee GTI. El software comprueba con el servidor de McAfee GTI y actualiza la base de datos local a intervalos regulares. Si la base de datos local no se actualiza en 30 días, el software descarga toda la base de datos durante la próxima actualización. De lo contrario, la actualización es incremental. De forma predeterminada, la base de datos local se actualiza una vez cada día. No se puede modificar la ubicación de almacenamiento de la base de datos.



No se puede actualizar la base de datos local mediante ePolicy Orchestrator porque el servidor necesita conexiones directas a Internet. Sin embargo, si se usa el servidor proxy para descargar reglas antispam, se puede usar la misma configuración para descargar la base de datos de URL.

## Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento en el menú secundario que tenga el analizador **Reputación de URL de correo**.



La protección **Reputación de URL de correo** está disponible solo para las directivas **En tiempo real**, **Bajo demanda (predeterminado)** y **Bajo demanda (análisis completo)**.

- 2 Haga clic en **Directiva principal** o cualquier **directiva secundaria** que desee configurar, haga clic en la ficha **Enumerar todos los analizadores**, a continuación, haga clic en **Reputación de URL de correo**.
- 3 En **Activación**, seleccione **Activar**.
  - Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva principal** para que herede la configuración de la directiva principal.
  - Si añade un analizador a la directiva, puede especificar una hora de activación del analizador mediante la lista desplegable **¿A qué hora desea que esto se aplique?**.
- 4 En la lista desplegable **Opciones**, puede seleccionar:
  - **Configuración predeterminada de URL de correo**: para aplicar los valores de umbral predeterminados.
  - **Crear nuevo grupo de opciones**: para definir valores de umbral según se necesiten.



Si edita la configuración existente, asegúrese de proporcionar un **Nombre de instancia** exclusivo para la configuración del analizador.

- 5 Para definir la configuración del analizador, seleccione **Crear nuevo grupo de opciones**.



6 En la página **Reputación de URL de correo**, defina estos valores y luego haga clic en **Guardar**.

- **Nombre de instancia**
- **Umbral de reputación de URL superior**
- **Umbral de reputación de URL inferior**
- **Número máximo de URL para cada correo electrónico**



El valor **Umbral de reputación de URL superior** siempre debe ser mayor que el valor **Umbral de reputación de URL inferior**.



Si una URL aparece varias veces, se cuenta una sola vez y no las que aparece. Por ejemplo, si el correo electrónico contiene 50 URL y una URL aparece 20 veces, la suma de URL es 31 y no 50.

7 En la sección **Acciones para realizar**, haga clic en **Editar** para definir las acciones.



También puede aplicar la configuración predeterminada.

8 En la página **Acciones de reputación de URL de correo**, defina estos parámetros para **Si la calificación de reputación de URL de correo supera el umbral superior**, **Si la calificación de reputación de URL de correo supera el umbral inferior**, y **Si el recuento de la búsqueda de URL de correo supera el límite**.

a En la lista desplegable **Realizar la siguiente acción**, seleccione:

- **Sustituir elemento por una alerta.**
- **Eliminar mensaje.**
- **Permitir paso.**

Cuando seleccione **Sustituir elemento por una alerta**, seleccione el formato de alerta:

- **Alerta predeterminada Reputación de URL de correo:** para usar el mensaje de alerta predeterminado.
- **Crear:** para definir el mensaje de alerta según se requiera. Escriba un nombre exclusivo para el **Nombre de la alerta**, defina el mensaje de alerta, defina el formato de texto en la lista desplegable **Mostrar** y luego haga clic en **Guardar**.



McAfee recomienda que se guarden las alertas en formato de texto simple para que el contenido de texto se pueda visualizar mediante un cliente de correo electrónico.

b En la sección **Y también**, defina estas opciones:

- |  |  |
|--|--|
| • <b>Registro</b>                                  | • <b>Notificar al remitente interno</b>    |
| • <b>Poner en cuarentena</b>                       | • <b>Notificar a remitente externo</b>     |
| • <b>Reenviar correo electrónico en cuarentena</b> | • <b>Notificar al destinatario interno</b> |
| • <b>Notificar al administrador</b>                | • <b>Notificar a destinatario externo</b>  |



Para obtener definiciones de cada una de estas opciones, consulte *Acciones que puede realizar en detecciones*.

- 9 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.
- 10 Haga clic en **Aplicar** para implementar la configuración en una directiva.



Puede ver las URL detectadas en la página **Elementos detectados | Reputación de URL de correo**. En la sección **Ver resultados**, puede ver la lista de URL detectadas. Haga clic en las **URL bloqueadas** en la columna **Expresiones prohibidas** para obtener una vista detallada.

### Ejemplos de umbral de reputación de URL superior y inferior

Establezca el valor del **Umbral de reputación de URL superior** en 80 y el del **Umbral de reputación de URL inferior** en 50. Si la calificación de reputación de la URL es:

La calificación de reputación de GTI es	Acción
Superior a 80	Se realiza una acción según la configuración de Reputación de URL de correo.
Inferior a 50	MSME permite el correo electrónico con la URL.
Entre 50 y 80	MSME sospecha que la URL podría ser maliciosa y realiza una acción según la configuración.



El valor de umbral de **Altamente sospechoso** detecta las URL maliciosas más peligrosas. A medida que se reduce el valor de umbral, aumentan las posibilidades de obtener falsos positivos. Falso positivo: una URL podría ser legítima, pero la base de datos la considera una URL potencialmente maliciosa.

## Comprobación de reputación de TIE para datos adjuntos de correo electrónico

MSME proporciona ahora capacidades de detección de amenazas adicionales; con este fin, emplea la comprobación de reputación de TIE para los datos adjuntos que proceden de mensajes de correo electrónico en los niveles de puerta de enlace, concentrador y buzón.

### ¿Qué es TIE?

Threat Intelligence Exchange aumenta las capacidades de protección y detección en tiempo real gracias a la realización de una comprobación de reputación de archivos exhaustiva y avanzada, además de impedir la propagación de las amenazas. El servidor de TIE analiza con rapidez los datos adjuntos en el nivel de puerta de enlace, concentrador y buzón. Para obtener información sobre Threat Intelligence Exchange, consulte la *Guía del producto de Threat Intelligence Exchange 2.0*.

La reputación de TIE se basa en dos variantes:

- Reputación de certificados
- Reputación de archivos

TIE valida el archivo con respecto a la calificación de reputación de certificados en primer lugar. Si la reputación de certificados es Conocido malicioso, se tiene en cuenta la calificación de reputación de archivos.

### Cómo funciona MSME con TIE

Cuando TIE está activado en la configuración de directiva, tras aplicar las reglas de filtrado de archivos MSME comprueba la reputación de los datos adjuntos de correo electrónico con el servidor de TIE. Según la reputación de TIE para el archivo, las calificaciones se asignan a una de estas categorías y MSME realiza una acción en función de la configuración definida para dicha categoría:

- Conocido de confianza: 99
- Probablemente de confianza: 85
- Posiblemente de confianza: 70
- Desconocido: 50
- Posiblemente malicioso: 30
- Probablemente malicioso: 15
- Conocido malicioso: 1

Cuando se configura una acción para una categoría específica, se aplica la misma acción a todas las categorías que tienen una calificación de reputación de TIE inferior a la de la categoría especificada. De forma predeterminada, la opción **Realizar acciones si es igual o peor que** se configura con el valor **Posiblemente malicioso**.

Por ejemplo, cuando se configura **Realizar acciones si es igual o peor que** con el valor **Desconocido** y la acción con el valor **Sustituir por una alerta** para los archivos con una calificación de 50, se reemplazan todos los archivos adjuntos con una calificación de reputación de TIE de 50 o menos por un mensaje de alerta. También es posible seleccionar acciones secundarias para la alerta.

Las calificaciones de reputación se almacenan en caché de forma local y MSME puede utilizar la caché local actualizada para las comprobaciones de reputación.

Cuando TIE está desactivado, se realiza una acción de análisis de acuerdo con la configuración de directiva. Cuando TIE está activado pero no es posible conectar con el servidor de TIE y la caché local no contiene entradas para el archivo, la comprobación de reputación de TIE se omite y el correo electrónico se analiza según la configuración de directiva.

Para obtener más información sobre cómo se asigna la calificación de reputación, consulte la *Guía del producto de TIE*.

MSME solo envía los siguientes tipos de archivos a la comprobación de reputación de TIE:

- exe
- pdf
- Documentos de Microsoft Office

Para ver la lista de tipos de archivos admitidos, véase [KB89578](#).



Cuando el correo electrónico contiene datos adjuntos comprimidos, el archivo comprimido se extrae y solo se envían los tipos de archivos admitidos a la comprobación de reputación de TIE. Para ver la lista de tipos de archivos comprimidos admitidos, véase [KB89577](#).

En el caso de otros tipos de archivos y tras la comprobación de reputación de TIE, MSME analiza los datos adjuntos de acuerdo con la configuración de directiva. Cuando se libera el elemento en cuarentena debido a las detecciones de TIE, el archivo solo se analiza en busca de virus antes de permitirlo. Puede consultar la información sobre el número de archivos detectados por TIE y el número de archivos enviados a la comprobación de ATD en la página Panel.

## Utilización de la reputación de Advanced Threat Defense

También puede activar la detección de Advanced Threat Defense en categorías de reputación de archivos concretas y en función del tamaño de los datos adjuntos.

Cuando se comprueba la reputación de TIE de un archivo, TIE devuelve la calificación de reputación y podría recomendar el análisis del archivo. MSME envía el archivo a Advanced Threat Defense en función de la categoría y el tamaño de archivo configurados. Si existe una calificación de reputación revisada para el archivo, la caché local se actualiza con esa calificación de reputación. La calificación revisada se utilizará a partir de la siguiente búsqueda. La configuración predeterminada para **Realizar acciones si es igual o peor que** es **Posiblemente malicioso** y el **Tamaño de archivo** es de 8 MB.

## Configuración recomendada de despliegue del servidor de TIE para MSME

McAfee recomienda hacer lo siguiente:

- Despliegue un servidor de TIE configurado como secundario a fin de procesar todas las solicitudes de reputación de TIE de MSME en el mismo centro de datos que su servidor de Exchange. Esto permite que el servidor de TIE procese el máximo de datos adjuntos de correo electrónico por segundo en una infraestructura dedicada.



En cada caso, los datos adjuntos de correo electrónico enviados para la reputación de TIE invocarán un máximo de dos solicitudes de TIE.

- El tráfico de reputación se reduce cuando los servidores de MSME almacenan en caché las reputaciones de forma local. No obstante, como MSME borra la caché local tras reiniciarse el servicio, podrían producirse picos.
- Calcule las solicitudes que proceden de MSME mediante los contadores de panel de MSME. Para obtener información sobre cómo medir las solicitudes por segundo que llegan a un servidor de TIE, consulte el **Rendimiento** en el apartado **Estado de rendimiento** de la página **Administración de la topología del Servidor de TIE**, correspondiente a la Configuración del servidor en McAfee ePO. También puede consultar los **Archivos nuevos del Servidor de TIE** en la página **Limpieza de datos del Servidor de TIE**.

## Configuración de TIE para analizar los datos adjuntos de correo electrónico

Active la comprobación de reputación de TIE para los datos adjuntos de correo electrónico en función de la categoría de reputación de archivos.

### Procedimiento

1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Configuración de TIE**.

2 Seleccione un elemento en la lista desplegable **Realizar acciones si es igual o peor que**.

- **Conocido de confianza:** la reputación del archivo es 99.
- **Probablemente de confianza:** la reputación del archivo es 85.
- **Posiblemente de confianza:** la reputación del archivo es 70.
- **Desconocido:** la reputación del archivo es 50.
- **Posiblemente malicioso:** la reputación del archivo es 30.



De forma predeterminada, está seleccionada la opción **Posiblemente malicioso**.

- **Probablemente malicioso:** la reputación del archivo es 15.
- **Conocido malicioso:** la reputación del archivo es 1.

3 En **Realizar la siguiente acción**, defina las opciones de configuración siguientes según corresponda.

- **Sustituir elemento por una alerta:** reemplaza el elemento por un mensaje de alerta y lo registra, lo pone en cuarentena o lo notifica de acuerdo con lo definido en **Y también**.
- **Eliminar elemento incrustado:** elimina los datos adjuntos de correo electrónico y los registra, los pone en cuarentena o los notifica según lo definido en **Y también**.
- **Eliminar mensaje:** elimina el correo electrónico y lo registra, lo pone en cuarentena o lo notifica según lo definido en **Y también**.

- 4 En **Y también**, configure las opciones siguientes según corresponda.
  - **Registro**
  - **Cuarentena**
  - **Reenviar correo electrónico en cuarentena**
  - **Notificar al administrador**
  - **Notificar al remitente interno**
  - **Notificar a remitente externo**
  - **Notificar al destinatario interno**
  - **Notificar a destinatario externo**
- 5 En **Enviar archivos a ATD si es igual o peor que**, seleccione la categoría y el tamaño de archivo para la reputación de Advanced Threat Defense.

## Configuración de antispam

Configure las opciones de una directiva para identificar mensajes de correo electrónico con spam y llevar a cabo las acciones necesarias.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione el elemento en el menú secundario **Gateway** que tenga el analizador **Antispam**.

Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Antispam**.
- 4 En **Activación**, seleccione **Activar** para activar la configuración del analizador antispam para el elemento del menú secundario seleccionado.



- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si añade un nuevo analizador a la directiva, puede especificar un intervalo de tiempo para que el analizador se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 5 En la lista desplegable **Opciones**, seleccione una configuración de analizador existente o **<crear nuevo grupo de opciones>**.

Aparecerá la página **Configuración antispam**.

- 6 En **Nombre de instancia**, introduzca un nombre único para la instancia de la configuración del analizador antispam. Este campo es obligatorio.

7 En la ficha **Opciones**, en **Calificación**, introduzca los valores para:

- **Umbral de calificación alta:** si la calificación de spam total es 15 o más.
- **Umbral de calificación media:** si la calificación de spam total es de 10 a 15.
- **Umbral de calificación baja:** si la calificación de spam total es de 5 a 10.



Para usar los valores predeterminados de las calificaciones de spam, seleccione la opción **Utilizar valores predeterminados**. Esta configuración predeterminada se ha optimizado cuidadosamente para mantener el equilibrio entre una clasificación alta y una baja de falso positivo de detección de spam. En el caso improbable de que necesite cambiar esta configuración, un aviso técnico está disponible en Soporte Técnico.

8 En **Informes**, en la lista desplegable **El umbral de informes de spam es**, seleccione **Alta, Media, Baja o Personalizada** para especificar cuándo un correo electrónico se debe marcar como spam.

9 En **Calificación personalizada**, introduzca una calificación de spam específica a partir de la que los correos electrónicos se deban marcar como spam. Este campo solo está activado si selecciona la opción **Personalizado** de la lista desplegable **El umbral de informes de spam es**.

10 Seleccione o quite la selección **Agregar prefijo al asunto de los mensajes de spam** según sea necesario.

11 En la lista desplegable **Agregar un indicador de calificación de spam**, seleccione:

- **Nunca:** sirve para que el encabezado de Internet de un correo electrónico no tenga el indicador de calificación de spam.
- **A mensajes de spam solo:** sirve para añadir un indicador de calificación de spam en el encabezado de Internet de los correos electrónicos spam solamente.
- **A mensajes que no son spam solo:** sirve para añadir un indicador de calificación de spam en el encabezado de Internet de los correos electrónicos que no son spam solamente.
- **A todos los mensajes:** sirve para añadir un indicador de calificación de spam en el encabezado de Internet de todos los correos electrónicos.



El indicador de calificación de spam es un símbolo usado en el informe de spam que se añade a los encabezados de Internet del correo electrónico para indicar la cantidad potencial de spam que contiene un correo electrónico.

12 En la lista desplegable **Adjuntar un informe de spam**, seleccione:

- **Nunca:** permite visualizar un correo electrónico sin el indicador de calificación de spam.
- **A mensajes de spam solo:** permite añadir un informe de spam solamente en correos electrónicos spam.
- **A mensajes que no son spam solo:** permite añadir un informe de spam solamente en correos electrónicos que no son spam.
- **A todos los mensajes:** permite añadir un informe de spam en todos los correos electrónicos.

13 Seleccione o quite la selección **Informe detallado** para especificar si el informe detallado es necesario o no. Informe detallado incluye los nombres y las descripciones de las reglas antispam activadas.



Si selecciona **Nunca** para **Adjuntar un informe de spam**, se desactiva **Informe detallado**.

14 En la ficha **Avanzada**, use:

- **Tamaño máximo de mensaje para analizar (KB):** permite especificar el tamaño máximo de un correo electrónico (en kilobytes) que puede ser analizado. Puede introducir un tamaño máximo de 999.999.999 kilobytes, aunque los correos electrónicos de spam típicos son bastante pequeños. El valor predeterminado es 250 KB.
- **Longitud máxima de los encabezados de spam (bytes):** permite especificar el tamaño máximo (en bytes) del encabezado del correo electrónico spam. La anchura mínima de encabezado que puede especificar es 40 caracteres y la máxima es 999 caracteres. El valor predeterminado es 76.



Los remitentes de spam agregan a menudo información adicional en los encabezados para sus propios propósitos.

- **Número máximo de reglas notificadas:** permite especificar el número máximo de reglas de spam que un informe de spam puede contener. El número mínimo de reglas que puede especificar es 1 y el máximo es 999. El valor predeterminado es 180.
- **Nombre del encabezado:** permite especificar un nombre diferente para el encabezado del correo electrónico. Puede usar este encabezado del correo electrónico y su valor de encabezado (abajo) al rastrear correos electrónicos y aplicar reglas a dichos mensajes. Estos campos son opcionales y admiten hasta 40 caracteres.
- **Valor del encabezado:** permite especificar un valor diferente para el encabezado del correo electrónico.
- **Agregar encabezado:** permite especificar que el encabezado no debe añadirse a ningún correo electrónico, a todos los correos electrónicos, solamente a correos electrónicos de spam o solamente a correos electrónicos que no son spam.
- Seleccione o quite la selección de la opción **Usar nombres de encabezado alternativos cuando el correo no es spam** según sea necesario.

15 En la ficha **Listas de correo**, en **Remitentes en la lista negra**, **Remitentes en la lista blanca**, **Destinatarios en la lista negra** y **Destinatarios en la lista blanca**, introduzca las direcciones de correo electrónico de los remitentes y los destinatarios de las listas negras y blancas.

Los correos electrónicos enviados o recibidos de una dirección de correo electrónico en una lista negra se tratan como spam, aunque no contengan características de spam. Los correos electrónicos enviados o recibidos de direcciones de correo electrónico en una lista blanca no se tratan como spam, aunque contengan características de spam.



Haga clic en **Agregar** para añadir direcciones de correo electrónico a una lista y en la casilla de verificación ubicada al lado de cada dirección para especificar si está actualmente activada o no. Haga clic en **Eliminar todo** para quitar una dirección de correo electrónico de la lista. No puede agregar la misma dirección de correo electrónico más de una vez. Puede usar caracteres comodín para hacer coincidir varias direcciones.

16 En la ficha **Reglas**, introduzca el nombre de la regla y seleccione **Activar regla** para activarla. Haga clic en **Agregar** para que aparezca una lista de reglas disponibles.



Haga clic en **Restablecer** para volver a la configuración antispam predeterminada.

17 En la lista, en cada regla, haga clic en **Editar** para modificarla.

18 Haga clic en **Eliminar** para eliminar una regla.

19 Haga clic en **Guardar** para volver a la página de la directiva.

20 En **Acciones para realizar si se detecta spam**, haga clic en **Editar**. En las siguientes fichas, especifique las acciones de analizador antispam que se deben realizar al detectarse spam:

- **Calificación alta**
- **Calificación media**
- **Calificación baja**

21 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.

22 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

### Procedimientos

- *Importación o exportación de listas negras y listas blancas en la página 88*  
Importe o exporte listas negras y listas blancas para hacer copia de seguridad o para usarlas en otro Exchange Server.
- *Utilización de la protección antisuplantación en la página 89*  
La suplantación de correo electrónico es un ardid habitual empleado para engañar a los usuarios mediante la modificación de la dirección de correo electrónico del remitente; se convence a los usuarios para que abran los mensajes y respondan a ellos sin saber que realmente no proceden de un origen legítimo.
- *Configuración de la protección contra la suplantación en la página 89*  
Active la protección contra la suplantación a fin de proteger sus sistemas frente al correo electrónico de suplantación.

### Importación o exportación de listas negras y listas blancas

Importe o exporte listas negras y listas blancas para hacer copia de seguridad o para usarlas en otro Exchange Server.

#### Procedimiento

- 1 En **Administrador de directivas**, seleccione el elemento en el menú secundario **Gateway** que tenga el analizador antispam.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Antispam**.
- 4 En **Opciones**, haga clic en el vínculo **Lista de bloqueo y lista de permitidos**.  
Aparecerá la página **Configuración antispam**.
- 5 Haga clic en la ficha **Listas de correo**.
- 6 Seleccione la lista correspondiente de las opciones siguientes:
  - **Remitentes en la lista negra**
  - **Remitentes en la lista blanca**
  - **Destinatarios en la lista negra**
  - **Destinatarios en la lista blanca**
- 7 Para importar una lista, haga clic en **Importar**. En la ventana emergente, haga clic en **Examinar** para ir al archivo .cfg necesario, después haga clic en **Aceptar**.



8 Para exportar una lista, haga clic en el vínculo **Exportar**.



Haga clic en **Eliminar** para quitar una lista de la base de datos.

9 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.

## Utilización de la protección antisuplantación

La suplantación de correo electrónico es un ardid habitual empleado para engañar a los usuarios mediante la modificación de la dirección de correo electrónico del remitente; se convence a los usuarios para que abran los mensajes y respondan a ellos sin saber que realmente no proceden de un origen legítimo.

MSME ahora admite la función antisuplantación mediante el mecanismo denominado marco de directivas de remitente (SPF) del Grupo de trabajo de ingeniería de Internet (IETF). El marco SPF se basa en RFC 7208, que autoriza el uso de nombres de dominio en los mensajes de correo electrónico.

En función de la evaluación de SPF del dominio del remitente, el resultado se categoriza como sigue:

- Ninguno
- Neutro
- Correcto
- Error o Error grave
- Error leve
- Error temporal
- Error permanente

Mediante el filtro de SPF es posible configurar acciones para los errores leves y graves. A fin de reducir los falsos positivos, MSME considera las categorías restantes como correctas. Cuando se activa SPF, se puede ver el resultado de SPF en el encabezado del correo electrónico correspondiente a **Received-SPF**.

## Configuración de la protección contra la suplantación

Active la protección contra la suplantación a fin de proteger sus sistemas frente al correo electrónico de suplantación.

### Antes de empezar

Es necesario tener instalado el componente McAfee Anti-Spam en el servidor Exchange.

### Procedimiento

- 1 Navegue a **Configuración y diagnósticos | Antispam**.
- 2 En la sección **Filtro de SPF**, seleccione **Activar**.
- 3 Configure la acción para **Error grave** y **Error leve** según corresponda.
  - **Permitir acceso:** permite que el correo electrónico llegue al destinatario.
  - **Permitir acceso y poner en cuarentena:** permite que el correo electrónico llegue al destinatario y conserva una copia entre los elementos en cuarentena.
  - **Rechazar correo y poner en cuarentena:** bloquea el correo electrónico y lo pone en cuarentena.



La activación de esta opción podría afectar al rendimiento del producto, ya que la función antisuplantación envía consultas a los servidores DNS y depende de la latencia de la red.

## Configuración de antiphishing

Configure una directiva para bloquear mensajes de phishing mediante el motor y reglas antispam, y llevar a cabo las acciones necesarias.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione el elemento en el menú secundario **Gateway** que tenga el analizador **Antiphishing**.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Antiphishing**.
- 4 En **Activación**, seleccione **Activar** para activar la configuración del analizador antiphishing para el elemento del menú secundario seleccionado.



- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si añade un nuevo analizador a la directiva, puede especificar un intervalo de tiempo para que el analizador se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 5 En la lista desplegable **Opciones**, seleccione una configuración de analizador existente o **<crear nuevo grupo de opciones>**.  
Aparecerá la página **Configuración antiphishing**.
- 6 En **Nombre de instancia**, introduzca un nombre único para la instancia de la configuración del analizador antiphishing. Este campo es obligatorio.
- 7 En **Opciones de informes**, seleccione o quite la selección de estas opciones según sea necesario:
  - **Agregar prefijo al asunto de los mensajes de phishing**: permite especificar que quiere agregar texto al inicio de la línea de asunto de cualquier correo electrónico que probablemente contenga información de phishing.
  - **Agregar un encabezado indicador de phishing a los mensajes**: permite especificar si se ha agregado un indicador de phishing al encabezado de Internet de cualquier correo electrónico que probablemente contenga phishing.
  - **Adjuntar un informe de phishing**: permite especificar si se debe generar un informe de phishing y añadir a un correo electrónico detectado como phishing.
  - **Informe detallado**: permite especificar si deben incluirse los nombres y una descripción detallada de las reglas antiphishing activadas en el correo electrónico. Esta opción está solamente disponible si selecciona **Adjuntar un informe de phishing**.
- 8 Haga clic en **Guardar** para volver a la página de la directiva.
- 9 En **Acciones para realizar**, haga clic en **Editar** y especifique las acciones del analizador antiphishing que se deben realizar al detectarse phishing.
- 10 Haga clic en **Guardar** para aplicar la configuración y volver a la página de la directiva.
- 11 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Administración de configuraciones de filtros para una directiva

Active o desactive opciones del filtro y especifique llevar a cabo una acción adecuada sobre el elemento detectado cuando se activa una directiva.

Los filtros disponibles son:

- **Contenido dañado**
- **Contenido protegido**
- **Contenido cifrado**
- **Contenido firmado**
- **Archivos protegidos con contraseña**
- **Filtrado de tamaño de correo**
- **Control del analizador**
- **Configuración del correo MIME**
- **Archivos HTML**

### Procedimientos

- [Configuración de contenido dañado en la página 92](#)  
Configure las opciones de una directiva para identificar correos electrónicos con contenido dañado y llevar a cabo las acciones necesarias.
- [Configuración de contenido protegido en la página 92](#)  
Configure las opciones de una directiva para identificar correos electrónicos con contenido protegido y llevar a cabo las acciones necesarias.
- [Configuración de contenido cifrado en la página 93](#)  
Configure las opciones de una directiva para identificar correos electrónicos con contenido cifrado y llevar a cabo las acciones necesarias.
- [Configuración de contenido firmado en la página 93](#)  
Configure las opciones de una directiva para identificar correos electrónicos con contenido firmado y llevar a cabo las acciones necesarias.
- [Configuración de archivos protegidos con contraseña en la página 94](#)  
Configure las opciones de una directiva para identificar correos electrónicos con archivos protegidos con contraseña y llevar a cabo las acciones necesarias.
- [Configuración del filtrado según tamaño del correo en la página 94](#)  
La configuración del filtrado según tamaño del correo en una directiva detecta mensajes de correo electrónico según su tamaño, la cantidad de datos adjuntos y el tamaño de los datos adjuntos.
- [Configuración de las opciones de control del analizador en la página 96](#)  
Configure las opciones de una directiva para definir el nivel de anidación, el tamaño de archivo expandido y el tiempo máximo de análisis permitidos cuando se activa el análisis de un mensaje de correo electrónico.
- [Bloqueo manual de direcciones IP en la página 97](#)  
Es posible bloquear una dirección IP específica o un intervalo de direcciones IP de forma que no puedan enviar correo electrónico a su organización, independientemente de la reputación de IP. Para activar esta opción, es necesario actualizar la clave de Registro siguiente.
- [Configuración de correo MIME en la página 97](#)  
Configure las opciones de una directiva para identificar mensajes MIME codificados y llevar a cabo las acciones necesarias.
- [Configuración de archivos HTML en la página 99](#)  
Configure una directiva para analizar elementos o eliminar archivos ejecutables, como ActiveX, applets de Java, VBScripts en componentes HTML, de un correo electrónico.

## Configuración de contenido dañado

Configure las opciones de una directiva para identificar correos electrónicos con contenido dañado y llevar a cabo las acciones necesarias.

Es posible que el contenido de algunos mensajes de correo electrónico esté dañado y no se pueda analizar. Las directivas sobre contenido dañado especifican la manera de tratar los correos electrónicos con contenido dañado cuando se detectan.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Contenido dañado**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 4 En **Acciones**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se detecta contenido dañado.
- 5 Haga clic en **Guardar** para volver a la página de la directiva.
- 6 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de contenido protegido

Configure las opciones de una directiva para identificar correos electrónicos con contenido protegido y llevar a cabo las acciones necesarias.

Las directivas con contenido protegido especifican la manera de tratar los correos electrónicos con contenido protegido cuando se detectan.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Contenido protegido**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 4 En **Acciones**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se detecta contenido protegido.
- 5 Haga clic en **Guardar** para volver a la página de la directiva.
- 6 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de contenido cifrado

Configure las opciones de una directiva para identificar correos electrónicos con contenido cifrado y llevar a cabo las acciones necesarias.

Es posible cifrar correos electrónicos a fin de evitar el acceso no autorizado. El contenido cifrado usa una *clave* y algoritmos matemáticos de cifrado para descifrarlo. Las directivas de contenido cifrado especifican la manera de tratar los correos electrónicos cifrados cuando se detectan.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.

- 3 Haga clic en **Contenido cifrado**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 4 En **Acciones**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se detecta contenido cifrado.

- 5 Haga clic en **Guardar** para volver a la página de la directiva.



La configuración de contenido cifrado es aplicable a los datos adjuntos cifrados en correos electrónicos internos y a los mensajes de correo electrónico de Internet cifrados.

- 6 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de contenido firmado

Configure las opciones de una directiva para identificar correos electrónicos con contenido firmado y llevar a cabo las acciones necesarias.

Siempre que se envía información electrónicamente, puede ser alterada de manera accidental o voluntaria. Para evitar este problema, algunas herramientas de software de correo electrónico usan una firma digital (la forma electrónica de una firma manuscrita).

Una firma digital es una información adicional añadida al mensaje de un remitente que identifica y autentica al remitente y la información en el mensaje. Está cifrada y actúa como un resumen de datos único. Normalmente, una cadena de letras y números larga aparece al final del correo electrónico recibido. El software de correo electrónico entonces vuelve a analizar la información en el mensaje del remitente y crea una firma digital. Si esa firma es idéntica a la original significa que los datos no se han alterado.

Si el correo electrónico tiene contenido con virus, contenido dañino o es demasiado grande, el software puede limpiar o eliminar algunas partes del mensaje. El correo electrónico todavía sería válido y podría leerse, pero la firma digital original estaría "rota". El destinatario no podría confiar en el contenido del correo electrónico porque dicho contenido también podría haberse alterado de otras maneras. Las directivas de contenido firmado especifican la manera en que se deben gestionar los mensajes de correo que incluyan firmas digitales.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.

3 Haga clic en **Contenido firmado**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

4 En **Acciones**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se detecta contenido firmado.

5 Haga clic en **Guardar** para volver a la página de la directiva.



La configuración de contenido firmado es aplicable a los correos electrónicos de Internet firmados y a los datos adjuntos firmados.

6 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de archivos protegidos con contraseña

Configure las opciones de una directiva para identificar correos electrónicos con archivos protegidos con contraseña y llevar a cabo las acciones necesarias.

No se puede tener acceso a los archivos protegidos con contraseña sin una contraseña, ni tampoco se pueden analizar en busca de malware. Las directivas para estos archivos especifican la manera en que se gestionan los mensajes de correo electrónico que contienen uno de ellos.

### Procedimiento

1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.

3 Haga clic en **Archivos protegidos con contraseña**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

4 En **Acciones**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se detecta un correo electrónico con archivos protegidos con contraseña.



Si establece la acción como **Permitir paso**, cerciórese de que la **Regla para omitir protegida con contraseña** en **Reglas de filtrado de archivos y las acciones relacionadas** en la configuración de **Filtrado de archivos** del analizador sea la primera regla de la lista. Si la regla ya aparece, pero en un nivel diferente, elimínela y luego selecciónela en la lista desplegable **Reglas disponibles**.

5 Haga clic en **Guardar** para volver a la página de la directiva.

6 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración del filtrado según tamaño del correo

La configuración del filtrado según tamaño del correo en una directiva detecta mensajes de correo electrónico según su tamaño, la cantidad de datos adjuntos y el tamaño de los datos adjuntos.

### Antes de empezar

Asegúrese de que, en la página **Configuración en tiempo real**, estén seleccionadas las opciones **Analizar correos entrantes** y **Analizar correos salientes**.

Puede configurar parámetros de filtrado según el tamaño del correo para las directivas **Gateway** y **En tiempo real** por separado. Configure el parámetro **Gateway** para el correo electrónico entrante y el parámetro **En tiempo real** para el correo electrónico saliente. Por ejemplo:

- Para bloquear todo el correo electrónico entrante que contenga más de cinco archivos adjuntos, configure el parámetro **Filtrado según tamaño del correo** en la directiva **Gateway**.
- Para bloquear todo el correo electrónico saliente que contenga más de tres archivos adjuntos, configure el parámetro **Filtrado según tamaño del correo** en la directiva **En tiempo real**.



El filtrado según tamaño del correo para el análisis en tiempo real no es aplicable a la función de servidor de buzón de correo.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento en el menú secundario que tenga el analizador antivirus.  
  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Seleccione la directiva según sea preciso entre **En tiempo real** y **Gateway**:
- 3 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 4 Haga clic en **Filtrado de tamaño de correo**.
- 5 En **Activación**, seleccione **Activar** para activar la configuración del filtro de tamaño de correo electrónico para el elemento en el menú secundario seleccionado.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 6 En **Opciones**, puede usar:
  - **Configuración predeterminada**: permite ver un resumen del conjunto de opciones de tamaño de correo predeterminado.
  - **Configuración predeterminada de gateway**: permite ver un resumen de la opción predeterminada de tamaño de correo utilizada por la directiva de gateway.
  - **<create new set of options>**: permite configurar las opciones de filtrado según tamaño del correo. Las opciones son:
    - **Nombre de instancia**: permite introducir un nombre único para la instancia de la configuración del filtro de tamaño de correo. Este campo es obligatorio.
    - **Tamaño general máximo de correo (KB)**: permite especificar el tamaño máximo (en kilobytes) de un correo electrónico. Puede especificar un valor entre 2 KB y 2 GB; el valor predeterminado 20.000 KB.
    - **Tamaño máximo de archivo adjunto (KB)**: permite especificar el tamaño máximo (en kilobytes) de los datos adjuntos de un correo electrónico. Puede especificar un valor entre 1 KB y 2 GB; el valor predeterminado 4,096 KB.
    - **Número máximo de archivos adjuntos**: permite especificar el número máximo de archivos adjuntos que un correo electrónico puede tener. Puede especificar hasta 999; el valor predeterminado es 25.
  - **Editar**: permite editar el conjunto de opciones seleccionado.

- 7 En **Acciones**, haga clic en **Editar**. Especifique las acciones de filtrado según tamaño del correo, si el valor excede la configuración especificada para estas opciones:
  - **Tamaño del mensaje**
  - **Tamaño del archivo adjunto**
  - **Recuento de archivos adjuntos**
- 8 Haga clic en **Guardar** para volver a la página de la directiva.



El correo electrónico interno no es detectado por las reglas de filtrado según tamaño del correo.

## Configuración de las opciones de control del analizador

Configure las opciones de una directiva para definir el nivel de anidación, el tamaño de archivo expandido y el tiempo máximo de análisis permitidos cuando se activa el análisis de un mensaje de correo electrónico.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el analizador. Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Control del analizador**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 4 En **Opciones**, haga clic en **<crear nuevo grupo de opciones>**.
- 5 En **Nombre de instancia**, introduzca un nombre único para la instancia de configuración del filtro de control del analizador. Este campo es obligatorio.
- 6 En **Máximo nivel de anidamiento**, especifique el nivel en el que el analizador debe analizar, cuando los datos adjuntos contienen archivos comprimidos y otros archivos comprimidos dentro. Puede especificar un valor entre 2 y 100; el valor predeterminado es 10.
- 7 En **Tamaño máximo de archivo expandido (MB)**, especifique el tamaño máximo permitido en el caso de un archivo que se expande para su análisis. Puede especificar un valor entre 1 y 2047; el valor predeterminado es 10.
- 8 En **Tiempo máximo de análisis (minutos)**, especifique el tiempo máximo permitido para el análisis de un archivo. Puede especificar un valor entre 1 y 999; el valor predeterminado es 1.
- 9 Haga clic en **Guardar** para volver a la página de la directiva.
- 10 En **Selección de alertas**, puede seleccionar qué alerta usar cuando se activa una opción del control del analizador. Puede usar:
  - **Crear**: sirve para crear un nuevo mensaje de alerta para la directiva.
  - **Ver/ocultar**: sirve para mostrar u ocultar el texto de la alerta. Si se oculta el texto, al hacer clic en este vínculo se mostrará. Si se muestra el texto, al hacer clic en este vínculo se ocultará.



- 11 En **Acciones**, haga clic en **Editar** para especificar las acciones que se deben llevar a cabo si el valor excede las opciones especificadas para estas opciones:
  - **Máximo nivel de anidamiento**
  - **Tamaño máximo de archivo expandido (MB)**
  - **Tiempo máximo de análisis (minutos)**
- 12 Haga clic en **Guardar** para volver a la página de la directiva.
- 13 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Bloqueo manual de direcciones IP

Es posible bloquear una dirección IP específica o un intervalo de direcciones IP de forma que no puedan enviar correo electrónico a su organización, independientemente de la reputación de IP. Para activar esta opción, es necesario actualizar la clave de Registro siguiente.

### Antes de empezar

El bloqueo manual de direcciones IP solo se puede emplear con las funciones de Exchange de concentrador, de perímetro, de buzón y de concentrador+buzón. Para incluir manualmente direcciones IP en la lista negra, la detección McAfee Anti-Spam debe estar disponible en MSME.

### Procedimiento

- 1 En el sistema donde esté instalado MSME, navegue a esta clave de Registro:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState`
- 2 Agregue el valor de cadena `IPBlackList`.
- 3 Asigne la dirección IPv4 que desee bloquear para que no pueda enviar correo electrónico.  
Es posible bloquear varias direcciones IP mediante el uso del punto y coma. También se puede bloquear un intervalo de direcciones IP mediante el carácter comodín \*. Por ejemplo:
  - `10.21.22.*` — Bloquea todas las direcciones IP desde `10.21.22.0` hasta `10.21.22.255`
  - `10.21.*.*` — Bloquea todas las direcciones IP desde `10.21.0.1` hasta `10.21.255.255`

## Configuración de correo MIME

Configure las opciones de una directiva para identificar mensajes MIME codificados y llevar a cabo las acciones necesarias.

Análisis de Extensiones multipropósito de correo de Internet (MIME, Multipurpose Internet Mail Extensions) es un estándar de comunicaciones que permite la transferencia de formatos no ASCII a protocolos (como SMTP) que admiten solamente caracteres ASCII de 7 bits.

MIME define diferentes maneras de codificar los formatos no ASCII para poderlos representar mediante los caracteres del conjunto de caracteres ASCII de 7 bits.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.

3 Haga clic en **Configuración del correo MIME**.



Si añade un nuevo filtro a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

4 En **Opciones**, seleccione **<crear nuevo grupo de opciones>**.

Aparecerá la página **Configuración de correo**.

5 En **Nombre de instancia**, introduzca un nombre único para la instancia de la configuración del filtro de correo electrónico MIME. Este campo es obligatorio.

6 En la ficha **Opciones**, introduzca un **Prefijo en el asunto del mensaje**.

- a En **Nueva codificación recomendada de archivos adjuntos en un mensaje MIME**, seleccione un método para volver a codificar que se use al volver a codificar los archivos adjuntos de mensajes MIME entre las opciones disponibles.
- b En **Nueva codificación recomendada de encabezados de asunto modificados**, seleccione un método para volver a codificar que se use al volver a codificar los encabezados de asunto en los mensajes MIME entre las opciones disponibles.
- c En **Si se produce un error al volver a codificar un encabezado de asunto**, seleccione una de estas opciones:
  - **Tratar como error**: si se devuelve el mensaje MIME.
  - **Respaldo a UTF-8**: si el mensaje MIME se codifica en UTF-8.

7 En la ficha **Avanzadas**, seleccione uno de estos métodos de codificación que se usará al codificar la parte de texto de un correo electrónico:

- **Código imprimible**, es lo más adecuado para los mensajes que contienen principalmente caracteres ASCII, pero también valores de byte fuera del intervalo.
- **Base64**, tiene una sobrecarga fija y es más adecuado para datos que no sean de texto y para mensajes que no tengan mucho texto ASCII.
- **8 bits**, su uso es más adecuado con servidores SMTP que admiten la extensión SMTP para transporte MIME de 8 bits.



Puede realizar el *paso 6b* solamente seleccionando **Volver a codificar utilizando el esquema de codificación original** o **Volver a codificar utilizando el siguiente conjunto de caracteres** en **Nueva codificación recomendada de encabezados de asunto modificados**.

- a Seleccione o quite la selección **No codificar si el texto es de 7 bits** según sea necesario.
- b En **Conjunto de caracteres de decodificación predeterminado**, seleccione el conjunto de caracteres que haya que usar para decodificar, cuando los encabezados MIME no especifiquen ninguno.
- c En **Número máximo de partes MIME**, especifique el número máximo de partes MIME que un mensaje MIME puede contener. El valor predeterminado es 10.000 partes MIME.
- d En **Daño de encabezado en un mensaje MIME**, seleccione la opción necesaria.
- e En **Caracteres nulos en los encabezados de un mensaje MIME**, seleccione la opción necesaria.
- f En **Codificación de caracteres de código imprimible en un mensaje MIME**, seleccione la opción necesaria.

- 8 En la ficha **Tipos MIME**, especifique qué Tipos MIME se deben tratar como datos adjuntos de texto y cuáles como datos adjuntos binarios.



Haga clic en **Agregar** para agregar tipos MIME a la lista o **Eliminar** para eliminar un tipo MIME de una lista. No se permiten entradas duplicadas.

- 9 En la ficha **Conjuntos de caracteres**, seleccione **Conjunto de caracteres** y **Alternativas**, desactive la casilla de verificación **Solucionado** y haga clic en **Agregar** para especificar una asignación de juego de caracteres alternativa a la especificada en el mensaje MIME.



Haga clic en **Editar** para editar asignaciones de caracteres, en **Eliminar** para eliminar asignaciones de caracteres y en **Guardar** para aplicar cualquier cambio que haya realizado en las asignaciones de caracteres. La opción **Guardar** está disponible solamente cuando hace clic en **Editar**.

- 10 Haga clic en **Guardar**.

- 11 En **Selección de alertas**, puede seleccionar la alerta que se utilizará cuando se bloquee un tipo MIME. Puede usar:

- **Crear**: sirve para crear un nuevo mensaje de alerta para la directiva.
- **Ver/ocultar**: sirve para mostrar u ocultar el texto de la alerta. Si se oculta el texto, al hacer clic en este vínculo se mostrará. Si se muestra el texto, al hacer clic en este vínculo se ocultará.

- 12 En **Acciones de mensaje incompleto**, haga clic en **Editar** para especificar las acciones de filtro que deben realizarse cuando se encuentra un tipo MIME parcial o externo.

- 13 Haga clic en **Guardar** para volver a la página de la directiva.

- 14 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración de archivos HTML

Configure una directiva para analizar elementos o eliminar archivos ejecutables, como ActiveX, applets de Java, VBScripts en componentes HTML, de un correo electrónico.

Si ninguno de estos contenidos se encuentra en HTML, se quita el filtro. Este filtro funciona solamente si el analizador de contenido está activado.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el filtro.

Aparecerá la página de la directiva para el elemento del menú secundario.

- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.

- 3 Haga clic en **Archivos HTML**.

- 4 En **Opciones**, haga clic en **<crear nuevo grupo de opciones>**.

Aparecerá la página **Archivos HTML**.

- 5 En **Nombre de instancia**, introduzca un nombre único para la instancia de configuración del filtro. Este campo es obligatorio.

6 En **Analizar los siguientes elementos**, seleccione cualquiera de estas opciones:

- **Comentarios:** permite analizar en busca de elementos de comentario en el mensaje HTML. Por ejemplo:

```
<!-- comment text --!>
```

- **Metadatos:** permite analizar en busca de elementos de metadatos en el mensaje HTML. Por ejemplo:

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- **Direcciones URL de vínculo ("<ahref=... ")**: permite analizar en busca de elementos de direcciones URL en el mensaje HTML. Por ejemplo:

```
<a HREF= "McAfee.htm " >
```

- **Direcciones URL de origen ("<img src=...")**: permite analizar en busca de elementos de direcciones URL de origen en el mensaje HTML. Por ejemplo:

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- **JavaScript / VBScript:** permite analizar en busca de JavaScript o Visual Basic script en el mensaje HTML. Por ejemplo:

```
<script language="javascript" scr="mfe/mfe.js">
```

7 En **Eliminar los siguientes elementos ejecutables**, seleccione cualquiera de estas opciones:

- **JavaScript / VBScript:** permite eliminar elementos de JavaScript o Visual Basic script del mensaje HTML. Por ejemplo:

```
<script language="javascript" scr="mfe/mfe.js">
```

- **Subprogramas Java:** permite eliminar elementos de subprogramas Java del mensaje HTML. Por ejemplo:

```
<APPLET code="XYZApp.class" codebase="HTML ....."></APPLET>
```

- **Controles ActiveX:** permite eliminar elementos de controles ActiveX del mensaje HTML. Por ejemplo:

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan Image </OBJECT>
```

- **Macromedia Flash:** permite eliminar elementos de Macromedia Flash del mensaje HTML. Esta opción se activa si los controles ActiveX están seleccionados. Por ejemplo:

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 Haga clic en **Guardar** para volver a la página de la directiva.

9 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Administración de configuraciones varias para una directiva

Cree o edite configuraciones varias, como alertas y renuncias, que se aplican cuando se activa una directiva. Las opciones disponibles son las siguientes:

- **Configuración de alerta**
- **Texto de renuncia**

## Procedimientos

- *Configuración de mensajes de alerta en la página 101*  
Configure las opciones de una directiva para notificar al usuario final con un mensaje de alerta cuando se produce una detección.
- *Configuración del texto de renuncia en la página 102*  
Configure las opciones del texto de renuncia de una directiva. Se trata de un texto, generalmente de tipo legal, que se agrega a todos los mensajes de correo electrónico salientes.

## Configuración de mensajes de alerta

Configure las opciones de una directiva para notificar al usuario final con un mensaje de alerta cuando se produce una detección.

### Procedimiento

- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el analizador.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Configuración de alerta**.
- 4 Seleccione **Activar** para activar la configuración del mensaje de alerta para el elemento del menú secundario seleccionado.



- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si ha añadido un nuevo mensaje de alerta a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 5 En **Opciones**, seleccione la configuración de alerta predeterminada disponible o seleccione **<crear nuevo grupo de opciones>** para definir la configuración de alertas.



Para obtener instrucciones paso por paso sobre cómo crear una nueva alerta, consulte la sección *Creación de una nueva alerta*.

- 6 Haga clic en **Editar** para modificar la alerta existente.  
Aparecerá la página **Configuración de alerta**.
- 7 Seleccione **HTML** o **Texto sin formato** como **Formato de alerta**.
- 8 En el menú desplegable **Codificación de caracteres**, seleccione el conjunto de caracteres necesario.
- 9 En **Nombre de archivo de la alerta**, especifique el nombre de archivo para esta alerta, incluida la extensión de archivo apropiada de HTML (.htm) o de texto sin formato (.txt).
- 10 Seleccione o quite la selección **Activar encabezados de alerta** para activar el uso de un encabezado de alerta.
- 11 En el cuadro de introducción de texto **Encabezado de alerta**, introduzca el encabezado para la alerta.

- 12 En **Mostrar**, seleccione **Contenido HTML (WYSIWYG)** o **Contenido HTML (origen)** dependiendo de si el texto HTML se debe mostrar como código compilado o código fuente en el **Encabezado de alerta**.



La opción **Mostrar** solamente está disponible si tiene **HTML** seleccionado como el formato del mensaje de alerta.

- 13 Seleccione **Activar pies de alerta** para activar el uso de un pie de alerta según sea necesario.

- 14 En el cuadro de entrada de texto **Pie de alerta**, introduzca el pie para la alerta.

- 15 En **Mostrar**, seleccione **Contenido HTML (WYSIWYG)** o **Contenido HTML (origen)** dependiendo de si el texto HTML se debe mostrar como código compilado o código fuente en el **Pie de alerta**.



La opción **Mostrar** solamente está disponible si tiene **HTML** seleccionado como el formato del mensaje de alerta.

- 16 Haga clic en **Guardar** para volver a la página de la directiva.

- 17 Haga clic en **Aplicar** para configurar estas opciones en una directiva.

## Configuración del texto de renuncia

Configure las opciones del texto de renuncia de una directiva. Se trata de un texto, generalmente de tipo legal, que se agrega a todos los mensajes de correo electrónico salientes.

Cuando se asigna el texto de renuncia a una directiva, todos los correos electrónicos que se envían desde la organización de Exchange mediante el servidor de MSME contendrán dicho texto según las opciones de configuración seleccionadas.



Las opciones del texto de renuncia solamente se pueden aplicar en servidores de transporte de Microsoft Exchange.

### Procedimiento



- 1 En **Administrador de directivas**, seleccione un elemento del menú secundario que tenga el analizador.  
Aparecerá la página de la directiva para el elemento del menú secundario.
- 2 Haga clic en **Directiva principal** o en cualquier directiva secundaria que desee configurar y haga clic en la ficha **Enumerar todos los analizadores**.
- 3 Haga clic en **Texto de renuncia**.
- 4 Seleccione **Activar** para activar la configuración del texto de renuncia para el elemento del menú secundario seleccionado.



- Para configurar opciones de una directiva secundaria, seleccione **Usar configuración de la directiva padre** para que herede la configuración de la directiva principal.
- Si ha añadido un nuevo texto de renuncia a la directiva, puede especificar un intervalo de tiempo para que el filtro se active, mediante la lista desplegable **¿A qué hora desea que esto se aplique?**

- 5 En **Opciones**, seleccione **<crear nuevo grupo de opciones>**. Aparecerá la página **Texto de renuncia**.

- 6 En **Nombre de instancia**, introduzca un nombre único para la instancia de la configuración del texto de renuncia. Este campo es obligatorio.

- 7 En Formato de renuncia, puede seleccionar:
  - **HTML**: para especificar si desea que la renuncia aparezca con formato HTML en la notificación por correo electrónico.
  - **Texto sin formato**: para especificar si desea que la renuncia aparezca como texto sin formato en la notificación por correo electrónico.
- 8 En **Editar contenido de renuncia**, introduzca el mensaje del texto de renuncia.
- 9 En **Mostrar**, seleccione **Contenido HTML (WYSIWYG)** o **Contenido HTML (origen)** dependiendo de si el texto HTML se debe mostrar como código compilado o código fuente en el **Pie de alerta**.
  -  La opción **Mostrar** solamente está disponible si seleccionó **HTML** como el formato del texto de renuncia.
- 10 En el menú desplegable **Insertar renuncia**, seleccione **Delante de cualquier texto de mensaje**, **Detrás de cualquier texto de mensaje** o **Como archivo adjunto** dependiendo de dónde y cómo se inserte el texto de renuncia en el correo electrónico.
- 11 Haga clic en **Guardar** para volver a la página de la directiva.
  -  Las renunciaciones solamente son aplicables a los correos electrónicos salientes.
- 12 Haga clic en **Aplicar** para configurar estas opciones en una directiva.





# 5

## Configuración y diagnósticos

**Configuración y diagnósticos** tiene menús para activar y desactivar, configurar y gestionar funciones de MSME y sus registros. Configure estas opciones según las directivas de seguridad de la organización.

Para modificar o ver la configuración del producto de MSME, desde la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos**. Esta tabla explica brevemente cuándo debe definir esta configuración:

**Tabla 5-1 Configuración y diagnósticos**


Utilice	Para
<b>Configuración en tiempo real</b>  La <b>Configuración en tiempo real</b> está disponible solamente en Microsoft Exchange Server 2010. Dado que la compatibilidad con Microsoft VSAPI se ha eliminado en Microsoft Exchange 2013 y 2016, la función de configuración de análisis en segundo plano y VSAPI en tiempo real está desactivada en Exchange Server 2013 y 2016.	Definir qué hacer con el correo electrónico en caso de que ocurra un error durante el análisis. Las opciones son: <ul style="list-style-type: none"><li>• <b>Permitir acceso</b></li><li>• <b>Eliminar</b></li></ul> También cuenta con submenús para activar o desactivar configuraciones para: <ul style="list-style-type: none"><li>• <b>API de análisis de virus (VSAPI) de Microsoft</b></li><li>• <b>Configuración de análisis en segundo plano</b></li><li>• <b>Configuración de análisis de transporte</b></li></ul>
<b>Configuración bajo demanda</b>	Modifique la credencial de contraseña para el <b>MSMEODUser</b> y para sincronizar la actualización de la contraseña con Active Directory y otros servidores de Exchange.
<b>Configuración de la exclusión de buzón de correo</b>	Definir qué buzones de correo, carpetas o subcarpetas se excluirán del análisis de VSAPI en tiempo real.
<b>Notificaciones</b>	<ul style="list-style-type: none"><li>• Definir una cuenta de correo electrónico de administrador para recibir notificaciones o enviarlas por correo electrónico a revisores o listas de distribución cuando se detecte un correo electrónico.</li><li>• Generar notificaciones personalizadas para enviarlas por correo electrónico a usuarios cuando se ponga en cuarentena un correo electrónico.</li><li>• Definir alertas de estado de funcionamiento del producto que se envíen por correo electrónico al administrador a diario o inmediatamente después de ocurridos eventos específicos, como problemas con la base de datos de Postgres o errores en la carga de un servicio.</li></ul>

Tabla 5-1 Configuración y diagnósticos (continuación)

Utilice	Para
Antispam	<ul style="list-style-type: none"> <li>Definir la configuración de la carpeta de correo basura en la que se reenvía un spam en un servidor de transporte perimetral (gateway).</li> <li>Activar o desactivar la función <b>McAfee GTI message reputation</b> (Reputación de mensajes de McAfee GTI).</li> <li>Activar o desactivar la función <b>Filtro de SPF</b>.</li> <li>Activar o desactivar la función <b>Reputación de IP de McAfee GTI</b>.</li> </ul>
Configuración de TIE	<p>Configurar y administrar la configuración de detección de TIE mediante las opciones siguientes.</p> <ul style="list-style-type: none"> <li><b>Realizar acciones si es igual o peor que:</b> para activar una acción cuando la calificación de reputación sea inferior o igual al umbral definido.</li> <li><b>Realizar la siguiente acción</b> <ul style="list-style-type: none"> <li><b>Sustituir elemento por una alerta</b></li> <li><b>Eliminar elemento incrustado</b></li> <li><b>Eliminar mensaje</b></li> </ul> </li> <li><b>Y también:</b> proporciona diversas opciones tales como registro, cuarentena o notificación.</li> <li><b>Enviar archivos a ATD si es igual o peor que y Limitar archivos a:</b> para enviar archivos a la comprobación de reputación de Advanced Threat Defense con la coincidencia de límite de tamaño de archivo y el umbral de reputación de TIE.</li> </ul>
Elementos detectados	<p>Configurar y gestionar repositorios en cuarentena mediante:</p> <ul style="list-style-type: none"> <li><b>McAfee Quarantine Manager:</b> para configurar las opciones de comunicación entre MSME y el servidor de MQM (si corresponde).</li> <li><b>Base de datos local:</b> para gestionar y administrar actividades de la base de datos local en cuarentena, como la purga y la optimización.</li> </ul>
Preferencias de interfaz de usuario	<p>Defina la configuración en el <b>Panel</b> como el intervalo de actualización, la configuración de informes, la escala de unidad de los gráficos, el intervalo de informes y la configuración de gráficos.</p>
Diagnósticos	<p>Definir las configuraciones para eventos de depuración y registros de producto, por ejemplo, información sobre el tamaño máximo y la ubicación de almacenamiento de los registros. La configuración de diagnósticos incluye:</p> <ul style="list-style-type: none"> <li><b>Registro de depuración</b></li> <li><b>Registro de eventos</b></li> <li><b>Registro de producto</b></li> <li><b>Servicio de notificación de errores</b></li> </ul>
Registro de producto	<p>Vea el <b>Registro del producto</b> y filtre los resultados por fecha, tipo o descripción.</p>
Configuración de DAT	<p>Guardar los DAT antiguos en lugar de sobrescribirlos con cada actualización y definir cuántos archivos de definición de detecciones desea conservar.</p>

**Tabla 5-1 Configuración y diagnósticos** (continuación)

Utilice	Para
<b>Importar y exportar configuración</b>	Configurar el servidor actual de MSME con la misma configuración de uno ya creado, restaurar configuraciones predeterminadas o mejoradas, o generar Sitelists que lleven a sitios de descarga de DAT.
<b>Configuración de proxy</b>	Configurar o modificar la configuración de proxy para el <b>servicio Actualizador de reglas antispam de McAfee</b> .

Si modifica cualquiera de estas opciones de configuración, asegúrese de hacer clic en **Aplicar** para guardar los cambios. El color de fondo detrás de **Aplicar** cambia de la forma siguiente.



- Amarillo: si ha cambiado la configuración existente o si el cambio todavía no se aplicó.
- Verde: si no ha cambiado la configuración existente o si el cambio ya se aplicó.

### Contenido

- ▶ *Configuración en tiempo real*
- ▶ *Configuración bajo demanda*
- ▶ *Configuración de exclusión de buzones de correo*
- ▶ *Configuración de notificaciones*
- ▶ *Configuración de antispam*
- ▶ *Configuración de elementos detectados*
- ▶ *Configuración de preferencias de interfaz de usuario*
- ▶ *Configuración de diagnósticos*
- ▶ *Ver registros del producto*
- ▶ *Configuración de DAT*
- ▶ *Importación y exportación de opciones de configuración*
- ▶ *Configuración de proxy antispam*

## Configuración en tiempo real

El análisis en tiempo real se activa en la gateway o cada vez que se obtiene acceso a un mensaje de correo electrónico para determinar si la directiva en tiempo real detecta un elemento. El análisis en tiempo real también se conoce como análisis en tiempo real.

Cada análisis tiene su propio beneficio según la función de Exchange Server donde está instalado MSME. Esta tabla ayuda a comprender los tipos de análisis, su función y cuándo se aplica cada análisis:

Función de Exchange Server	Directivas aplicables	Tipo de análisis	Descripción
Transporte perimetral o transporte de concentradores	<ul style="list-style-type: none"> <li>• En tiempo real</li> <li>• Gateway</li> </ul>	Análisis de transporte en tiempo real	Realiza análisis en busca de amenazas antes de que lleguen al servidor de buzón de correo. Al activar esta opción, MSME puede detectar las amenazas en el perímetro de la organización y, por lo tanto, reducir la carga en el servidor de buzón de correo.
Buzón de correo	<ul style="list-style-type: none"> <li>• En tiempo real</li> </ul>	Análisis de VSAPI en tiempo real	Realiza análisis en busca de amenazas cuando el usuario obtiene acceso a un correo electrónico mediante un cliente de correo electrónico, como Outlook.
		Análisis proactivo	Realiza análisis en busca de amenazas antes de que un correo electrónico se grabe en el Almacén de información de Microsoft Exchange.

Función de Exchange Server	Directivas aplicables	Tipo de análisis	Descripción
		Análisis de elementos enviados	Realiza análisis en busca de amenazas en un correo electrónico que se encuentra en la carpeta de elementos enviados.
		Análisis en segundo plano	Un análisis de baja prioridad que realiza análisis en busca de amenazas en todas las bases de datos de Exchange en segundo plano.

Desde la sección **General**, defina una acción para que se lleve a cabo cuando se produzca un error de análisis.

Puede producirse un error de análisis por cualquiera de los motivos siguientes:

- **Error genérico:** el analizador no puede analizar un archivo particular.
- **Error de producto:** error de análisis debido a motor, archivo DAT o reglas de spam incorrectas.


Algunos de los motivos pueden ser problemas técnicos, como:

- Tiempo de espera del análisis
- Imposibilidad de carga del motor de análisis
- Problemas de DAT
- Correos electrónicos con formato incorrecto

Por ejemplo, si hay una falta de coincidencia de DAT en el registro y la ubicación real (\bin\DATs), se produce un error de análisis.

En caso de que se produzca un error de análisis, se activa una acción según la configuración especificada en **Configuración y diagnósticos | Configuración en tiempo real | General**.

**Tabla 5-2 Definiciones de las opciones**

Opción	Definición
<b>Error de análisis genérico</b>	<ul style="list-style-type: none"> <li>• <b>Permitir acceso:</b> permite el paso del mensaje de correo electrónico hacia el destinatario deseado cuando se produce un error de análisis.</li> <li>• <b>Quitar:</b> elimina el mensaje de correo electrónico cuando se produce un error de análisis.</li> </ul>
<b>Error de análisis de producto</b>	<ul style="list-style-type: none"> <li>• <b>Permitir acceso:</b> permite el paso del mensaje de correo electrónico hacia el destinatario deseado cuando se produce un error de análisis.</li> <li>• <b>Quitar:</b> elimina el mensaje de correo electrónico cuando se produce un error de análisis.</li> </ul>
	<p>McAfee recomienda que siempre se establezca esta opción en <b>Permitir acceso</b> para evitar que los correos electrónicos legítimos se pongan en cuarentena en caso de que se produzca un error. De forma predeterminada, la opción se establece en <b>Permitir acceso</b>, de modo que los correos electrónicos no se pierdan durante un error de análisis.</p>

Las otras categorías de la página **Configuración en tiempo real** son:

- **API de análisis de virus (VSAPI) de Microsoft**
- **Configuración de análisis en segundo plano**
- **Configuración de análisis de transporte**

En Configuración del análisis de transporte, puede excluir del análisis los mensajes de correo electrónico con el tamaño definido. Cuando se activa, el tamaño de archivo predeterminado para la exclusión es de 4 MB.



Para obtener más información acerca de los tipos de análisis, consulte el artículo de la base de conocimiento de McAfee KB51129.

## Configuración de API de análisis de virus (VSAPI) de Microsoft

Microsoft VSAPI permite que MSME analice correos electrónicos cuando el usuario final obtiene acceso a ellos mediante cualquier cliente de correo electrónico.

En Microsoft Exchange, los correos electrónicos se almacenan en una base de datos llamada Almacén de información de Exchange. Cuando se recibe un nuevo correo, Exchange Server notifica al cliente de Outlook acerca de un cambio. Esto sucede cuando se activa un análisis en tiempo real.



Esta función está disponible solo en Microsoft Exchange 2007/2010 Server con función de buzón de correo.


**Tabla 5-3 Definiciones de las opciones**

Opción	Definición
<b>Activar</b>	Seleccione esta opción para analizar mensajes de correo electrónico solo cuando el usuario final obtiene acceso a ellos mediante un cliente de correo electrónico, como Outlook. Esta función analiza correos electrónicos que ya están disponibles en el Almacén de información de Microsoft Exchange o si hay una falta de coincidencia en el sello antivirus.
<b>Análisis proactivo</b>	<p>Seleccione esta opción para analizar mensajes de correo electrónico antes de que se graben en el Almacén de información de Microsoft Exchange.</p> <p>Active esta función en estas situaciones:</p> <ul style="list-style-type: none"> <li>• Cuando MSME no está configurado en el servidor de transporte de concentradores y si un correo electrónico infectado alcanza el servidor de buzón de correo, se detectará antes de que se grabe en el Almacén de información de Exchange.</li> <li>• Por lo general, el contenido publicado en una base de datos de carpeta pública no se enruta mediante un servidor de transporte de concentradores. A fin de garantizar que el contenido se analice antes de que llegue al almacén, se recomienda activar el análisis proactivo para las bases de datos de carpetas públicas.</li> </ul>
<b>Análisis de bandeja de salida</b>	<p>Seleccione esta opción para analizar mensajes de correo electrónico en la carpeta de elementos enviados.</p> <p>MSME analiza el correo electrónico en la carpeta de elementos enviados en sí, incluso antes de que el correo electrónico llegue al servidor de transporte de concentradores, por lo que se reduce la carga en el servidor de concentradores.</p>
<b>Límite de antigüedad inferior (segundos)</b>	<p>Especifique un valor para que solo se analicen correos electrónicos recibidos en el transcurso de un plazo especificado. Los correos electrónicos recibidos antes del plazo especificado no se analizarán.</p> <p>De forma predeterminada, el valor se establece en 86400 segundos, el equivalente a un día.</p>
<b>Tiempo límite del análisis (segundos)</b>	<p>Tiempo máximo permitido para analizar un correo electrónico. Si el análisis de un correo electrónico supera el valor especificado, se realiza la acción que se especifica en <b>Configuración y diagnósticos   Configuración en tiempo real   General   Error durante el análisis</b>.</p> <p>De forma predeterminada, el valor se establece en 180 segundos.</p>
<b>Número de subprocesos de análisis</b>	<p>Especifique el número de subprocesos de grupo que se usa para procesar elementos en la cola de análisis proactivo y en tiempo real. El valor predeterminado es 2 * &lt;número de procesadores&gt; + 1. McAfee recomienda que seleccione la casilla de verificación <b>Predeterminado</b> para un mejor rendimiento.</p>

## Configuración de análisis en segundo plano

Analice de manera metódica los mensajes deseados almacenados en una base de datos. Para cada base de datos, un subproceso en ejecución con una prioridad por debajo de lo normal muestra todas las carpetas de la base de datos y, luego, solicita que MSME analice el contenido según corresponda.



**Tabla 5-4 Definiciones de las opciones**

Opción	Definición
<b>Activar</b>	Seleccione esta opción para analizar en segundo plano toda la base de datos después de un brote de virus. De forma predeterminada, esta opción está desactivada.
<b>Planificación</b>	<p>Seleccione esta opción para activar o desactivar el análisis en segundo plano.</p> <ul style="list-style-type: none"> <li>Haga clic en <b>Activar a las</b> para especificar cuándo iniciar el análisis en segundo plano.</li> <li>Haga clic en <b>Desactivar a las</b> para especificar cuándo detener el análisis en segundo plano.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> <li>  Programe el análisis para que se realice durante las horas de menos trabajo del día o durante los fines de semana.           </li> <li>Si no creó ninguna programación, el análisis en segundo plano comienza cuando se produce una actualización de DAT.</li> </ul> </div>
<b>Solo mensajes con adjuntos</b>	<p>Seleccione esta opción para analizar solamente los mensajes de correo electrónico con datos adjuntos. Esta función es útil si le preocupa que un virus específico se propague mediante datos adjuntos. Dado que los mensajes de correo electrónico con datos adjuntos son más vulnerables e incluyen contenido malicioso, en esta tarea se reemplaza cualquier virus o archivo ejecutable.</p> <p>Activar esta función ahorra tiempo, ya que MSME analiza solamente los correos electrónicos con datos adjuntos.</p>
<b>Solo elementos sin analizar</b>	Seleccione esta opción para analizar mensajes de correo electrónico que no hayan sido analizados. Active esta opción cuando Microsoft VSAPI esté desactivado en el servidor de buzón de correo durante un tiempo y se desee analizar elementos que no hayan sido analizados.
<b>Forzar analizar todo</b>	Seleccione esta opción para analizar los elementos independientemente de que tengan o no un sello de análisis antivirus.
<b>Actualizar sello de análisis</b>	Seleccione esta opción para actualizar mensajes de correo electrónico con el sello antivirus más reciente.
<b>Fecha desde</b>	Permite realizar análisis en segundo plano solo en los correos electrónicos recibidos a partir de la fecha especificada.
<b>Fecha hasta</b>	Permite realizar análisis en segundo plano solo en los correos electrónicos recibidos hasta la fecha especificada. Seleccione <b>Hasta la fecha</b> para analizar los correos electrónicos hasta la fecha actual del sistema.

## Configuración de análisis de transporte

El análisis de transporte le permite analizar el tráfico SMTP antes de que entre en el almacén de información de Exchange. El análisis de transporte SMTP puede analizar correos electrónicos enrutados no destinados al servidor local y puede detener la salida de mensajes.

**Tabla 5-5 Definiciones de las opciones**



Opción	Definición
<b>Activar</b>	<p>Seleccione esta opción para activar análisis a nivel de transporte de Exchange. De manera predeterminada, esta opción está activada.</p> <p> Dicha opción funciona únicamente con servidores Microsoft Exchange Server con las funciones de transporte perimetral, transporte de concentradores o buzón de correo y concentrador.</p>
<b>Sello de análisis de transporte</b>	<p>Seleccione esta opción para aplicar las firmas de DAT al encabezado del correo electrónico, de forma que los mensajes no se analicen de nuevo en la función de buzón de correo.</p> <p><b>Configuraciones recomendadas:</b> Si se ha activado el análisis de transporte, asegúrese de activar esta opción.</p>
<b>Evitar analizar correos electrónicos cuyo tamaño supere</b>	<p>Los mensajes de correo electrónico se excluyen de los análisis en tiempo real en función del tamaño. El tamaño de archivo se puede definir en KB o MB.</p> <p> McAfee recomienda analizar todos los archivos antes de acceder a ellos para proteger los sistemas de cualquier amenaza potencial.</p>
<b>Análisis basado en la dirección</b>	<p>Configure las opciones de análisis en tiempo real según el flujo de correos electrónicos.</p>
<b>Analizar correos entrantes</b>	<p>Seleccione esta opción para analizar los mensajes de correo electrónico con destino en su servidor u organización de Exchange.</p>
<b>Analizar correos salientes</b>	<p>Seleccione esta opción para analizar los mensajes de correo electrónico que salen de su servidor u organización de Exchange. Se designa un correo electrónico como saliente si al menos un destinatario tiene una dirección externa de correo electrónico.</p>
<b>Analizar correos internos</b>	<p>Seleccione esta opción para analizar los mensajes de correo electrónico enrutados desde una ubicación interna de su dominio a otra ubicación del mismo dominio. Se considera dominio interno a cualquier elemento que se encuentre dentro del dominio autoritativo de Exchange Server. Se designa un correo electrónico como interno si se origina dentro del dominio y todos los destinatarios están ubicados dentro del mismo dominio.</p>

## Configuración bajo demanda

Acceda a la página **Configuración bajo demanda** para modificar las credenciales de contraseña de **MSMEODUser**. McAfee Security for Microsoft Exchange crea un usuario denominado **MSMEODuser** en Active Directory durante la instalación del producto en el servidor de buzón de correo. Este usuario es necesario para realizar análisis bajo demanda en buzones de correo.

Para cumplir la directiva de seguridad de su organización, quizás deba actualizar la contraseña de **MSMEODUser** de forma periódica.

En la interfaz, navegue hasta **Configuración y diagnósticos** | **Configuración bajo demanda**.

Opción	Definición
Nombre de usuario	<b>MSMEODUser:</b> el usuario que realiza el análisis bajo demanda.  Este es un campo de solo lectura.
Escriba la contraseña	Escriba la contraseña.
Confirmar contraseña	Confirme la contraseña.
Restablecer esta contraseña también en LDAP	Seleccione esta opción para sincronizar la actualización de la contraseña con Active Directory y otros servidores de Exchange.  Seleccione esta opción solo cuando inicie el restablecimiento de la contraseña desde la página <b>Configuración bajo demanda</b> .

Puede actualizar la contraseña de **MSMEODUser** de dos modos:

- Restablezca la contraseña en Active Directory y luego actualícela en la página **Configuración bajo demanda**.
- Restablezca la contraseña desde la página **Configuración bajo demanda**.

Restablecer la contraseña mediante Active Directory	Restablecer la contraseña mediante la página Configuración bajo demanda
<ol style="list-style-type: none"> <li>1 Actualice la contraseña en Active Directory.</li> <li>2 Vaya a cualquiera de los sistemas con función Buzón de correo dentro del mismo Active Directory.</li> <li>3 Inicie la interfaz de McAfee Security for Microsoft Exchange.</li> <li>4 Desde <b>Configuración y diagnósticos</b>, navegue hasta la página <b>Configuración bajo demanda</b> y actualice la contraseña.</li> <li>5 Anule la selección de la opción <b>Restablecer esta contraseña también en LDAP</b>.</li> <li>6 Haga clic en <b>Aplicar</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Inicie la interfaz de McAfee Security for Microsoft Exchange.</li> <li>2 Desde <b>Configuración y diagnósticos</b>, navegue hasta la página <b>Configuración bajo demanda</b> y actualice la contraseña.</li> <li>3 Seleccione la opción <b>Restablecer esta contraseña también en LDAP</b> para cerciorarse de que la actualización de la contraseña se sincronice con Active Directory.</li> <li>4 Haga clic en <b>Aplicar</b>.</li> </ol>



Puede actualizar la contraseña de **MSMEODUser** desde ePolicy Orchestrator.



Esta configuración puede tardar hasta un minuto en aplicarse en todos los servidores de intercambio dentro del dominio. Ejecute un análisis bajo demanda tras actualizar la contraseña para su verificación.

Para obtener más información sobre **MSMEODUser**, consulte el artículo de McAfee KnowledgeBase [KB82332](#).



## Configuración de exclusión de buzones de correo

Configure buzones de correo o carpetas que se excluirán de un análisis de VSAPI.

Configure la exclusión de buzones de correo durante escenarios específicos:

- Directivos de la compañía que no desean realizar un análisis de sus correos electrónicos.
- Directivas de la compañía que identifiquen carpetas que no requieren análisis.
- Carpetas que se excluirán del análisis.



McAfee no recomienda excluir buzones de correo y no será responsable en caso de existir buzones de correo infectados debido a las opciones de exclusión.

### Procedimiento

- 1 Haga clic en **Configuración y diagnósticos** | **Configuración de la exclusión de buzón de correo**. Aparecerá la página **Configuración de la exclusión de buzón de correo**.
- 2 Para excluir el buzón de correo o la subcarpeta:

Para excluir un buzón de correo	Para excluir una carpeta en el buzón de correo
<p><b>1</b> En el panel <b>Buzones de correo disponibles</b>;, seleccione un buzón de correo. y haga clic en &gt;&gt;.</p> <p>El buzón de correo seleccionado pasa al panel <b>Buzones de correo que excluir</b>. Repita este paso en todos los buzones de correo que deban ser excluidos de un análisis de VSAPI.</p> <p>Para quitar un buzón de correo de la lista de exclusión, seleccione un buzón en el panel <b>Buzones de correo que excluir</b> y haga clic en &lt;&lt; para mover el buzón a la lista de <b>Buzones de correo disponibles</b>.</p>	<p><b>1</b> En el panel <b>Buzones de correo disponibles</b>;, seleccione un buzón de correo.</p> <p><b>2</b> En el cuadro <b>Carpetas del buzón de correo que se excluirán</b>, escriba el nombre de la carpeta que se deba excluir y haga clic en &gt;&gt;.</p> <p>La carpeta de buzón de correo seleccionada pasa al panel <b>Buzones de correo que excluir</b>.</p> <p>También puede usar un carácter comodín para excluir varias carpetas del análisis de VSAPI. Para obtener más información, consulte <i>Uso de carácter comodín para excluir carpetas de buzón de correo</i>.</p>



Cuando se agrega un buzón de correo al panel **Buzones de correo que excluir**, se excluyen del análisis todas las carpetas en el buzón de correo.



Si va a configurar exclusiones de buzón de correo de ePolicy Orchestrator, debe proporcionar manualmente la ruta de acceso completa.

- 3 Haga clic en **Aplicar** para guardar la configuración.



Esta exclusión anula **Análisis de bandeja de salida** en la configuración de **API de análisis de virus (VSAPI) de Microsoft** en la página **Configuración en tiempo real** que ya haya configurado. Por ejemplo, si excluye el análisis de la bandeja de salida para un usuario, la configuración de la exclusión de buzón de correo anula el análisis de bandeja de salida global.




Para obtener más información acerca de la exclusión de buzón de correo, consulte *Ejemplos del uso de caracteres comodín para exclusiones de buzón de correo*.

## Ejemplos del uso de caracteres comodín para exclusiones de buzón de correo

Puede usar un separador de coma o el carácter comodín \* para excluir carpetas del análisis de VSAPI en el nivel de buzón de correo y el de base de datos.

**Tabla 5-6 Ejemplos**

Nivel...	Para excluir...	Configurar...
Nivel de base de datos	Las carpetas <b>Borradores</b> de todos los buzones de correo en la base de datos.	<ol style="list-style-type: none"> <li>Desde la interfaz del producto, haga clic en <b>Configuración y diagnósticos</b>   <b>Configuración de la exclusión de buzón de correo</b>.</li> <li>En el panel <b>Buzones de correo disponibles</b>, seleccione la base de datos.</li> <li>En el cuadro <b>Carpetas del buzón de correo que se excluirán</b>, escriba <b>Draft</b>, haga clic en &gt;&gt; y luego en <b>Aplicar</b>. La carpeta de buzón de correo seleccionada aparece en el panel <b>Buzones de correo que excluir</b>.</li> </ol> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  No se puede seleccionar una base de datos para su exclusión sin especificar carpetas que excluir.         </div>
	Todas las carpetas en todos los buzones de correo que comienzan con <b>person</b> en la base de datos.	<ol style="list-style-type: none"> <li>Desde la interfaz del producto, haga clic en <b>Configuración y diagnósticos</b>   <b>Configuración de la exclusión de buzón de correo</b>.</li> <li>En el panel <b>Buzones de correo disponibles</b>, seleccione la base de datos.</li> <li>En el cuadro <b>Carpetas del buzón de correo que se excluirán</b>, escriba <b>person*</b>, haga clic en &gt;&gt; y luego en <b>Aplicar</b>. La carpeta de buzón de correo seleccionada aparece en el panel <b>Buzones de correo que excluir</b>.</li> </ol>
Nivel de buzón de correo	Varias carpetas en un buzón de correo mediante un separador de coma. Por ejemplo, puede excluir las carpetas Data1, Project1 y Report1 ubicadas en <b>Bandeja de entrada</b> .	<ol style="list-style-type: none"> <li>Desde la interfaz del producto, haga clic en <b>Configuración y diagnósticos</b>   <b>Configuración de la exclusión de buzón de correo</b>.</li> <li>En el panel <b>Buzones de correo disponibles</b>, seleccione un buzón de correo.</li> <li>En el cuadro <b>Carpetas del buzón de correo que se excluirán</b>, escriba <code>Inbox\Data1, Inbox\Project1, Inbox\Report1</code>, haga clic en &gt;&gt; y luego en <b>Aplicar</b>.</li> </ol>
	Carpetas y sus subcarpetas. <ul style="list-style-type: none"> <li>Puede excluir correos electrónicos en subcarpetas y analizarlos en una carpeta.</li> <li>Puede excluir correos electrónicos y subcarpetas de una carpeta.</li> </ul>	<ol style="list-style-type: none"> <li>Desde la interfaz del producto, haga clic en <b>Configuración y diagnósticos</b>   <b>Configuración de la exclusión de buzón de correo</b>.</li> <li>En el panel <b>Buzones de correo disponibles</b>, seleccione un buzón de correo.               <ul style="list-style-type: none"> <li><code>Inbox\Personal*</code>: para excluir correos electrónicos y subcarpetas en la carpeta <b>Personal</b> del análisis de VSAPI.</li> <li><code>Inbox\Personal*</code>: para excluir todas las subcarpetas en la carpeta <b>Personal</b> del análisis de VSAPI. Los correos electrónicos en la carpeta <b>Personal</b> no se excluyen del análisis de VSAPI.</li> </ul> </li> </ol>

## Configuración de notificaciones

Permite configurar el contenido y la dirección SMTP para que el administrador envíe notificaciones vía correo electrónico cuando un correo electrónico se ponga en cuarentena.

En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Notificaciones** para configurar los parámetros de las notificaciones.

En la página **Notificaciones**, puede usar:

- **Configuraciones:** sirve para definir que una cuenta de correo electrónico reciba notificaciones cuando se ponga en cuarentena un mensaje de correo electrónico. Asimismo, será posible enviar notificaciones por correo electrónico a un revisor o a la lista de distribución cuando un filtro o un analizador específico ponga en cuarentena un mensaje de correo electrónico.



Asegúrese de que las direcciones de correo electrónico estén actualizadas para los sistemas o sistemas de grupo en la página **Notificación** para recibir notificaciones para los sistemas gestionados e independientes.



Para enviarle notificaciones por correo electrónico a una lista de distribución (LD), especifique la dirección SMTP de la lista de distribución.

- **Plantilla:** sirve para generar notificaciones personalizadas que se envían por correo electrónico a usuarios específicos cuando se pone en cuarentena un mensaje de correo electrónico.
- **Alertas de estado de funcionamiento del producto:** sirven para definir las alertas de estado de funcionamiento del producto que se envían por correo electrónico al administrador a diario o inmediatamente después de ocurridos eventos específicos, como problemas con la base de datos de Postgres o errores en la carga de un servicio.



Cuando configure el producto (p. ej., notificación o nombre de directiva), no use caracteres que puedan crear vulnerabilidad Cross Site Scripting (XSS). Para consultar la lista de caracteres que debe evitar, consulte el artículo de McAfee KnowledgeBase [KB82214](#).

## Configuración de las notificaciones

Configure una cuenta de correo electrónico para recibir notificaciones cuando se ponga en cuarentena un correo electrónico. También envíe correos electrónicos de notificación a revisores específicos o a listas de distribución cuando se detecte un correo electrónico.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Notificaciones**.
- 2 En la ficha **Notificaciones** | **Configuración**, puede usar:

Tabla 5-7 Definiciones de las opciones

Opción	Definición
General	Permite definir configuraciones sencillas de las notificaciones por correo electrónico.
Correo electrónico del administrador	<p>Permite notificar al administrador de Microsoft Exchange en caso de un evento, como una acción o una alerta de cuarentena.</p> <ul style="list-style-type: none"> <li>Para enviarles notificaciones por correo electrónico a varios usuarios, use punto y coma (;) como delimitador.</li> <li>Para enviarle notificaciones por correo electrónico a una lista de distribución (LD), especifique la dirección SMTP de la lista de distribución.</li> </ul>
Correo electrónico del remitente	<p>Permite especificar la dirección de correo electrónico del remitente en el campo <b>De</b> del correo electrónico de notificación.</p> <p>McAfee recomienda que no se modifique la dirección de <b>Correo electrónico del remitente</b> porque el software crea y utiliza esta dirección con varios propósitos. Si cambia esta dirección electrónica y no activa el conector de recepción <b>Anónimo</b> en Microsoft Exchange, no recibirá notificaciones de productos.</p>
Activar la notificación de los resultados de la tarea	Permite enviar correos electrónicos con los resultados de las tareas de actualización y análisis bajo demanda. El correo electrónico está en formato HTML y tiene los mismos datos y formato que la ventana <b>Resultados de tarea</b> en la interfaz de usuario. Esta función puede activarse o desactivarse con esta opción. De manera predeterminada, esta función está desactivada.
Avanzadas	Permite definir la configuración avanzada de las notificaciones, como especificar las direcciones de correo electrónico individuales y la línea de asunto para cada analizador o filtro.
Cuerpo del correo	Permite definir un cuerpo de mensaje de correo electrónico genérico para todas las notificaciones.

3 Haga clic en **Aplicar** para guardar la configuración.



MSME proporciona mayor seguridad al no admitir etiquetas HTML con vulnerabilidad XSS. McAfee recomienda quitar las etiquetas HTML con vulnerabilidad XSS de la plantilla de notificación existente antes de la actualización. De lo contrario, después de la actualización, si intenta modificar las plantillas de notificación que contienen etiquetas no admitidas, se le pedirá que las quite de la plantilla o que utilice esta última sin modificación. Para consultar la lista de etiquetas HTML no admitidas, consulte el artículo de McAfee KnowledgeBase [KB82214](#).

## Edición de la plantilla de notificación

Permite ver o editar el cuerpo del mensaje de notificación enviado al usuario final mediante correo electrónico.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Notificaciones**.
- 2 En la ficha **Notificaciones** | **Plantilla**, puede usar:

**Tabla 5-8 Definiciones de las opciones**

Opción	Definición
<b>Plantilla</b>	Permite ver la plantilla de notificación para un usuario final específico. Las opciones disponibles son las siguientes: <ul style="list-style-type: none"> <li>• <b>Remitente interno</b></li> <li>• <b>Destinatario interno</b></li> <li>• <b>Remitente externo</b></li> <li>• <b>Destinatario externo</b></li> </ul> Es posible definir un texto de notificación específico para cada tipo de usuario.
<b>Asunto</b>	Permite especificar la línea de asunto del correo electrónico de notificación. El asunto predeterminado de la notificación es <b>Alerta de McAfee Security for Microsoft Exchange</b> .
<b>Texto de notificación</b>	Permite obtener una vista previa del cuerpo del mensaje del correo electrónico de notificación, según la selección de <b>Plantilla</b> . El texto de notificación contiene información acerca del elemento en cuarentena, por ejemplo, día y hora, asunto, acción tomada, etc.
<b>Editar</b>	Permite modificar el texto de notificación mediante HTML en formato de texto simple. Después de editar la notificación según el requisito de la compañía, haga clic en <b>Guardar</b> para aplicar los cambios.

3 Haga clic en **Aplicar** para guardar la configuración.

Ha visto o modificado satisfactoriamente la plantilla de notificación. Para obtener más información sobre los campos de notificación disponibles, consulte la sección *Campos de notificación que puede usar*.

## Campos de notificación que puede usar

Incluya estos campos en las notificaciones que genera. Por ejemplo, si desea incorporar el nombre del elemento detectado y la acción que se llevó a cabo al ser detectado, use **%vrs%** y **%act%** en la página **Configuración y diagnósticos | Notificaciones | Plantilla**.

**Tabla 5-9 Campos de notificación que puede usar**

Opciones del campo de notificación	Descripción
%dts%	Fecha y hora
%sdr%	Remitente
%ftr%	Filtro
%fln%	Nombre de archivo
%rul%	Nombre de regla
%act%	Acción realizada
%fdr%	Carpeta
%vrs%	Nombre de detección
%trs%	Estado (estado de preparación)
%tik%	Número de ficha
%idy%	Analizado por
%psn%	Nombre de directiva
%svr%	Servidor
%avd%	DAT antivirus
%ave%	Motor antivirus

**Tabla 5-9 Campos de notificación que puede usar** (continuación)

Opciones del campo de notificación	Descripción
%rpt%	Destinatario
%rsn%	Motivo
%sbj%	Asunto
%ssc%	Calificación de spam
%ase%	Motor antispam
%asr%	Reglas antispam

## Activación de alertas de estado de funcionamiento del producto

Envíe notificaciones inmediata o diariamente al administrador de Microsoft Exchange, cuando se produzca un error en un producto o una tarea específicos.


### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Notificaciones**.
- 2 En la ficha **Notificaciones** | **Product Health Alerts** (Alertas de estado de funcionamiento del producto), puede usar:

**Tabla 5-10 Definiciones de las opciones**

Opción	Definición
<b>Activar</b>	Permite activar el envío de notificaciones de alerta de información del estado de funcionamiento del producto al administrador cuando se produce un error en una tarea específica del producto.
<b>Alertar a ePolicy Orchestrator</b>	Permite alertar al servidor de McAfee ePolicy Orchestrator que administra este servidor de MSME cuando se produce un error en una tarea específica del producto.
<b>Alertar al administrador</b>	Permite enviar alertas de estado de funcionamiento del producto al correo electrónico especificado en <b>Configuración y diagnósticos</b>   <b>Notificaciones</b>   <b>Configuración</b>   <b>Correo electrónico del administrador</b> .

**Tabla 5-10 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Notify when</b> (Notificar cuando)	<p>Permite notificar al administrador cuando se produzca un error en alguna de las tareas específicas del producto seleccionado. Puede seleccionar estas opciones para enviar alertas del estado de funcionamiento del producto al administrador.</p> <p> Estas opciones pueden variar según la función de Exchange Server.</p> <ul style="list-style-type: none"> <li>• <b>Error al descargar archivos DAT/motor antivirus</b></li> <li>• <b>Error al descargar reglas antispam</b></li> <li>• <b>Error al cargar el motor antivirus</b></li> <li>• <b>Error al cargar el módulo TransportScan</b></li> <li>• <b>Error al cargar el módulo VSAPI</b></li> <li>• <b>El proceso RPCServ se cierra de forma inesperada</b></li> <li>• <b>El proceso DLLHost se cierra de forma inesperada</b></li> <li>• <b>Error en el proceso Postgres</b></li> <li>• <b>Postgres no ha podido poner en cuarentena o registrar las detecciones</b></li> <li>• <b>Error de inicialización de la base de datos de Postgres</b></li> <li>• <b>Postgres no ha podido almacenar un registro</b></li> <li>• <b>Error en el análisis bajo demanda</b></li> <li>• <b>Database diskpace goes below the threshold</b> (El espacio en disco de la base de datos queda por debajo del umbral)</li> <li>• <b>Error al iniciar el servicio del producto</b></li> <li>• <b>Error del análisis de la reputación de archivos de McAfee Global Threat Intelligence</b></li> </ul>
<b>Inmediatamente</b>	Permite enviar una notificación al administrador inmediatamente después de que se produce el error en la tarea.
<b>Diariamente</b>	Permite enviar una notificación al administrador diariamente, en un horario específico, cuando se produce el error en la tarea.

3 Haga clic en **Aplicar** para guardar la configuración.

Ha activado correctamente la función **Product Health Alerts** (Alertas de estado de funcionamiento del producto).

## Configuración de antispam


Defina la configuración de la carpeta de correo basura en la que se reenvía un spam detectado en un servidor de transporte perimetral o de transporte de concentradores. También debe activar o desactivar configuraciones para la reputación de mensajes de McAfee GTI y la función de reputación de IP de McAfee GTI.

**Tabla 5-11 Definiciones de las opciones**

Opción	Definición
<b>Dirección de la carpeta de correo basura de sistema</b>	Especifica la dirección de correo electrónico al que se envían todos los correos electrónicos categorizados como spam.
<b>Reputación de mensajes de McAfee GTI</b>	<p>Reputación de mensajes de McAfee Global Threat Intelligence es el servicio de reputación de remitentes y mensajería basado en la nube, en tiempo real e integral de McAfee que permite a MSME proteger su Exchange Server contra amenazas basadas en mensajería tanto conocidas como nuevas, como el spam.</p> <p>MSME recibe millones de consultas de correo electrónico diariamente, toma las huellas digitales del contenido del mensaje (contra el contenido mismo por razones de privacidad) y lo analiza en varias dimensiones. La reputación de mensajes se combina con factores, como los patrones de envío de spam y el comportamiento de la IP, para determinar la probabilidad de que el mensaje sea malicioso.</p> <p>La calificación se basa no solo en la inteligencia colectiva de sensores que consultan la nube de McAfee, así como el análisis realizado por los investigadores y las herramientas automatizadas de McAfee Labs, sino también en la correlación de inteligencia de vectores cruzados de datos de amenaza de archivos, la Web y las redes. MSME usa esta calificación para determinar una acción según la directiva <b>Administrador de directivas   Gateway</b>.</p>
<b>Activar</b>	Permite bloquear mensajes de correo electrónico en la gateway según la calificación de la reputación del mensaje.
<b>Efectuar reputación de mensajes tras antispam</b>	Permite realizar un análisis de reputación de mensajes de McAfee GTI después de realizar un análisis basado en la directiva de MSME local.
<b>Umbral de reputación de mensajes</b>	Especifica un valor de umbral para bloquear mensajes de correo electrónico basados en la calificación de reputación de mensajes. De forma predeterminada, el valor se establece en 80.
<b>Acción que se va a realizar</b>	<p>Seleccionar:</p> <ul style="list-style-type: none"> <li>• <b>Desechar y poner en cuarentena:</b> para desechar un correo electrónico y ponerlo en cuarentena en la base de datos. Cuando se desecha un correo electrónico mediante esta configuración, el remitente no será notificado en el estado de entrega del correo electrónico.</li> <li>• <b>Pasar calificación a motor antispam:</b> para enviar la calificación de reputación del mensaje detectado por McAfee GTI al motor antispam. Esta opción está disponible solamente cuando se activa la opción <b>Efectuar reputación de mensajes tras antispam</b>.</li> </ul>
<b>Reputación de IP de McAfee GTI</b>	La reputación de IP actúa como primer nivel de protección para su entorno de Exchange al proteger su Exchange Server de orígenes de correo electrónico inseguros. Le permite aprovechar la información sobre amenazas recopilada por McAfee Global Threat Intelligence con el fin de impedir que sus datos sufran daños o robos mediante el bloqueo de correos electrónicos en la gateway según la dirección IP de origen.
<b>Activar</b>	Permite bloquear mensajes de correo electrónico en la gateway según la dirección IP de origen.



**Tabla 5-11 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Umbral de reputación de IP</b>	<p>Especifique un valor de umbral para bloquear los mensajes de correo electrónico de acuerdo con la calificación de reputación de la dirección IP.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  La acción se aplicará a todas las direcciones IP que tengan una calificación de reputación superior al umbral seleccionado. Todos los demás mensajes de correo electrónico se permitirán.         </div> <p>Puede incluir en la lista blanca las direcciones IP legítimas que son bloqueadas por el parámetro <b>Umbral de reputación de IP</b> en la página <b>Configuración antispam</b> modificando los valores de registro. Una vez que haya incluido en la lista blanca las direcciones IP, se permitirá la entrada de mensajes de correo electrónico provenientes de las direcciones IP en la lista blanca, independientemente de su calificación de reputación.</p> <p><b>Importante:</b> la inclusión de direcciones IP en la lista blanca solo omite el parámetro <b>Umbral de reputación de IP</b>. MSME también analiza el correo electrónico en busca de contenido dañado o cifrado, filtro de archivo, análisis de contenido, reputación de URL y antimalware. Si se detecta algo, se realiza una acción según la configuración del producto.</p> <p>Antes de incluir la dirección IP en la lista blanca, McAfee recomienda verificar la calificación de reputación de la misma en <a href="http://www.trustedsource.org">www.trustedsource.org</a> para corroborar su legitimidad.</p> <p>McAfee no será responsable si alguno de sus buzones de correo quedara infectado a causa de la dirección IP incluida en la lista blanca.</p> <p>Para más información sobre la configuración de listas blancas para direcciones IP utilizando el registro, consulte el artículo de McAfee KnowledgeBase <a href="#">KB82216</a>.</p>
<b>Acción que se va a realizar</b>	<p>Seleccione una de estas opciones para realizar una acción en un mensaje de correo electrónico según la calificación de reputación de su dirección IP de origen:</p> <ul style="list-style-type: none"> <li>• <b>Suprimir conexión y registro:</b> permite desechar un correo electrónico de una dirección IP de origen detectada y registrar la acción realizada con el elemento.</li> <li>• <b>Rechazar conexión y registro:</b> permite rechazar un correo electrónico de una dirección IP de origen, enviar una notificación al remitente y registrar la acción realizada con el elemento.</li> </ul>
<b>Filtro de SPF</b>	<p>Protege sus sistemas del correo electrónico de suplantación; es posible configurar acciones en los mensajes de error grave y error leve.</p>

## Configuración de elementos detectados

Permite especificar la configuración del repositorio para almacenar elementos detectados por MSME.

Configure y gestione repositorios en cuarentena mediante:

- **McAfee Quarantine Manager:** sirve para poner en cuarentena elementos detectados en el servidor de MQM.
- **Base de datos local:** sirve para poner en cuarentena elementos detectados en el servidor local de MSME.

## Cómo poner elementos en cuarentena mediante McAfee Quarantine Manager

Especifique la configuración del repositorio para poner elementos en cuarentena detectados por MSME en un servidor de McAfee Quarantine Manager.

Los productos de McAfee como McAfee Security for Microsoft Exchange y McAfee Email Gateway utilizan un número de puerto preasignado para enviar la información de detección a McAfee Quarantine Manager. McAfee Quarantine Manager, a su vez, usa el mismo número de puerto de manera predeterminada para liberar o enviar información de configuración de los correos electrónicos detectados al producto de McAfee.



El puerto de comunicación mencionado en la interfaz de usuario de McAfee Security for Microsoft Exchange debería ser el mismo que en McAfee Quarantine Manager.

Puede usar McAfee Quarantine Manager para consolidar las funciones de gestión de cuarentena y antispam. Le ofrece un punto central desde el que se pueden analizar correos electrónicos y archivos en cuarentena, y actuar en consecuencia.



En esta guía no se proporciona información detallada sobre la instalación y utilización del software McAfee Quarantine Manager. Consulte la documentación del producto de McAfee Quarantine Manager para obtener más información.

### Procedimiento

- 1 Instale el software McAfee Security for Microsoft Exchange en <server 1>.
- 2 Instale el software McAfee Quarantine Manager compatible en <server 2>.
- 3 Inicie la interfaz de usuario de MSME desde <server 1>.
- 4 Desde la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Elementos detectados**. Aparecerá la página **Elementos detectados**.
- 5 En la sección **McAfee Quarantine Manager**, seleccione **Activar**.
- 6 En **Modo de comunicación**, seleccione el modo.
  - **RPC**: la llamada a procedimiento remoto (o RPC, del inglés Remote Procedure Call) es un mecanismo de comunicación que requiere una conexión ininterrumpida para comunicarse con el servidor de McAfee Quarantine Manager. Si se produce un error de comunicación con el servidor de McAfee Quarantine Manager, se interrumpen los procesos como la puesta en cuarentena y el levantamiento de cuarentena.
  - **HTTP**: un mecanismo de comunicación sin estado para comunicarse con el servidor de McAfee Quarantine Manager. Si se produce un error de comunicación con el servidor de McAfee Quarantine Manager, los elementos se almacenan en la base de datos local hasta que se restaure la conexión. MSME intenta enviar los elementos en cuarentena a MQM tres veces. Si se produce un error las tres veces, se crea una entrada en el registro del producto y el elemento se almacena en la base de datos local.
  - **HTTPs**: un mecanismo de comunicación HTTP segura en el que los datos se transfieren en formato cifrado.



McAfee recomienda el uso de un canal de comunicación HTTP/HTTPs porque las conexiones sin estado garantizan que el software pueda comunicarse a la perfección con McAfee Quarantine Manager.

- 7 En **Dirección IP**, especifique la dirección IP del servidor de MQM.

8 En **Puerto y Puerto de devolución de llamada**, especifique los valores predeterminados.

Modo de comunicación	Valor de puerto	Puerto de devolución de llamada	Intervalo de actualización de listas blancas y negras (horas)
RPC	49500	49500	-
HTTP	80	-	4
HTTPs	443	-	4



Modifique este valor solamente si ha configurado un valor de puerto diferente en el servidor de McAfee Quarantine Manager.

9 Haga clic en **Aplicar** para guardar la configuración.

Acaba de configurar satisfactoriamente el servidor de MSME para iniciar la puesta en cuarentena de elementos detectados en el servidor de MQM.

## Poner elementos en cuarentena mediante la base de datos local

Especifique la configuración del repositorio para poner elementos en cuarentena detectados por MSME en una base de datos de PostgreSQL del servidor local de MSME.

### Procedimiento

1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Elementos detectados**.

Aparece la página **Elementos detectados**.

2 En la sección **Base de datos local**, puede utilizar lo siguiente:



**Tabla 5-12 Definiciones de las opciones**

Opción	Definición
<b>Specify location of database</b> (Especificar la ubicación de la base de datos)	Permite que la <b>Database location</b> (Ubicación de la base de datos) almacene los elementos en cuarentena detectados por MSME.
<b>Database location</b> (Ubicación de la base de datos)	<p>Permite especificar la ruta de acceso a la ubicación de base de datos, donde se pueden almacenar los elementos detectados por MSME. Puede seleccionar:</p> <ul style="list-style-type: none"> <li>• <b>&lt;Carpeta de instalación&gt;</b>: para crear las subcarpetas de base de datos en el directorio de instalación de MSME.</li> <li>• <b>&lt;Unidad del sistema&gt;</b>: para crear las subcarpetas de base de datos en el directorio C:\Windows\system32.</li> <li>• <b>&lt;Archivos de programa&gt;</b>: para crear las subcarpetas de base de datos en el directorio C:\Archivos de programa (x86) de Windows.</li> <li>• <b>&lt;Carpeta de Windows&gt;</b>: para crear las subcarpetas de base de datos en el directorio C:\Windows.</li> <li>• <b>&lt;Carpeta de datos&gt;</b>: para crear las subcarpetas de base de datos en el directorio C:\ProgramData\.</li> <li>• <b>&lt;Ruta completa&gt;</b>: para almacenar la base de datos de MSME en la ruta de acceso completa especificada.</li> </ul>



Especifique la ruta de acceso a la subcarpeta en el campo ubicado junto a la lista desplegable. La ruta de acceso de la subcarpeta predeterminada es McAfee\MSME\Data\

Tabla 5-12 Definiciones de las opciones (continuación)

Opción	Definición
<b>Maximum item size (MB)</b> (Tamaño máximo de elemento [MB])	Permite especificar el tamaño máximo de un elemento en cuarentena que se puede almacenar en la base de datos. Puede especificar un valor entre 1 y 999; el valor predeterminado es 100.
<b>Tamaño máximo de consulta (registros)</b>	Permite especificar la cantidad de registros o elementos en cuarentena que puede consultar desde la página <b>Elementos detectados</b> . Puede especificar un valor entre 1 y 20000; el valor predeterminado es 1000.
<b>Maximum item age (days)</b> (Antigüedad máxima de elemento [días])	Permite especificar la cantidad máxima de días que se puede almacenar un elemento en la base de datos local de cuarentena, antes de que se lo marque para su eliminación. Puede especificar un valor entre 1 y 365; el valor predeterminado es 30.
<b>Disk size check interval (Minute)</b> (Intervalo de comprobación de tamaño de disco [minutos])	Permite especificar con qué frecuencia MSME debe comprobar la disponibilidad de espacio en el disco. Puede especificar un valor entre 6 y 2880; el valor predeterminado es 6.
<b>Disk space threshold (MB)</b> (Umbral de espacio en disco [MB])	Permite especificar el valor de umbral en el cual se debe enviar al administrador una notificación de advertencia de poco espacio en disco. Puede especificar un valor entre 1 y 512000; el valor predeterminado es 2048.   Asegúrese de que <b>Database disk space goes below the threshold</b> (Espacio en disco de base de datos por debajo del umbral) en <b>Configuración y diagnósticos   Notificaciones   Product Health Alerts (Alertas de estado de funcionamiento del producto)   Notify when (Notificar cuando)</b> esté activada.
<b>Purge of old items frequency</b> (Frecuencia de purga de elementos antiguos)	Permite especificar con qué frecuencia se eliminan los elementos antiguos marcados para su eliminación de la base de datos de MSME. El valor predeterminado es <b>Mensualmente</b> .
<b>Optimization frequency</b> (Frecuencia de optimización)	Permite recuperar espacio en disco ocupado por registros de bases de datos eliminadas. Según el valor establecido en <b>Maximum item age (days)</b> (Antigüedad máxima de elemento [días]), los registros antiguos se eliminan si programó una tarea de purga. Una vez que elimina estos registros antiguos, MSME seguirá usando el espacio en disco especificado en el campo <b>Disk space threshold (MB)</b> (Umbral de espacio en disco [MB]), incluso si la base de datos en cuarentena no alcanzó su límite de tamaño. Para optimizar y reducir la base de datos, programe una tarea de optimización. El valor predeterminado es <b>Mensualmente</b> .   Siempre programe una tarea de optimización unas horas antes de que lleve a cabo la tarea de purga.
<b>Edit Schedule</b> (Editar programación)	Permite modificar el programa de la tarea de optimización o de purga. Haga clic en <b>Guardar</b> después de modificar el programa.

3 Haga clic en **Aplicar** para guardar la configuración.

Ha configurado satisfactoriamente su servidor de MSME para comenzar a poner en cuarentena elementos detectados en la base de datos local.

## Configuración de preferencias de interfaz de usuario

Defina la configuración del **Panel**, por ejemplo, intervalos de actualización, configuraciones de informes, unidades de la escala de gráficos, intervalo de informes y configuraciones de gráficos y cuadros.

### Configuración de las opciones del panel

Permite configurar las opciones de **Panel**, como estadísticas, unidad de la escala de gráficos, elementos visualizados en **Elementos recientemente analizados** e intervalo de informe de estado.

#### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Preferencias de interfaz de usuario**.

Aparece la página **Preferencias de interfaz de usuario**.

- 2 Haga clic en la ficha **Configuración de panel**. Puede usar:

**Tabla 5-13 Definiciones de las opciones**

Opción	Definición
<b>Actualización automática</b>	Permite especificar si la información desplegada en el contador <b>Panel   Estadísticas</b> se actualizará de forma automática.
<b>Intervalo de actualización (segundos)</b>	Permite especificar el intervalo (en segundos) de actualización de la información del panel. Puede especificar un valor entre 30 y 3600; el valor predeterminado es 60.
<b>Máximo de elementos analizados recientemente</b>	Permite especificar el máximo de elementos que aparecerán en la sección <b>Panel   Informes   Elementos recientemente analizados</b> . Puede especificar un valor entre 10 y 100; el valor predeterminado es 10.
<b>Escala del gráfico (unidades)</b>	Permite especificar las unidades de medida de la escala del gráfico de barras que se generará en la sección <b>Panel   Gráfico</b> . Puede especificar un valor entre 100 y 500; el valor predeterminado es 100.
<b>Número de horas para informar</b>	Permite especificar un intervalo de generación de informes (en horas), por ejemplo, informes de estado y de configuración. Puede especificar un valor entre 1 y 24; el valor predeterminado es 7.

- 3 Haga clic en **Aplicar** para guardar la configuración.

## Configuración de gráficos y cuadros

Configure las opciones de la sección **Panel | Gráfico** para mejorar la configuración de gráficos y cuadros.

### Procedimiento

- 1 Haga clic en **Configuración y diagnósticos | Preferencias de interfaz de usuario**.
- 2 Haga clic en la ficha **Configuración de gráficos**. Puede usar:

**Tabla 5-14 Definiciones de las opciones**

Opción	Definición
<b>3D</b>	Permite especificar si el gráfico se debe mostrar en el panel como un gráfico en tres dimensiones (3D).
<b>Dibujar transparente</b>	Permite especificar si las barras del gráfico de barras en tres dimensiones deben ser opacas o transparentes. Una barra opaca oculta parte de cualquier barra situada detrás de ella. Una barra transparente permite ver a través de ella y ver otras barras transparentes detrás de ella.
<b>Anti-alias</b>	Permite especificar si se usan técnicas de suavizado (de anti-alias) cuando se muestran gráficos de sectores. Si se usa dicha técnica, las curvas de los gráficos circulares se suavizan. Si no se usa, las curvas de los gráficos circulares aparecen dentadas.
<b>Separar segmentos</b>	Permite especificar si los segmentos deben permanecer dentro del círculo del gráfico circular o como segmentos separados.
<b>Ángulo del sector (grados)</b>	Permite especificar el ángulo que hay que utilizar al crear gráficos circulares. Puede especificar un valor entre 1 y 360; el valor predeterminado es 45.

- 3 Haga clic en **Aplicar** para guardar la configuración.

## Configuración de diagnósticos

Permite determinar las causas de los síntomas, la mitigación de problemas y las soluciones a inconvenientes encontrados durante la ejecución de MSME.

En la página **Configuración y diagnósticos | Diagnósticos**, puede usar:

- **Registro de depuración:** sirve para configurar el registro de depuración, por ejemplo, especificar el nivel de registro de depuración, el tamaño máximo de los archivos del registro de depuración y dónde deben guardarse.
- **Registro de eventos:** sirve para configurar la captura de registros relacionados con el producto o eventos según la información, las advertencias o los errores.
- **Registro del producto:** sirve para configurar el archivo de registro del producto MSME (`productlog.bin`). Los cambios realizados a esta configuración se verán reflejados en la página **Configuración y diagnósticos | Registro del producto**.
- **Servicio de informe de errores:** sirve para configurar la captura de excepciones, como bloqueos del sistema, y enviar notificaciones al usuario.

### Configuración de registro de depuración

Defina la configuración para especificar el nivel del registro de depuración, el límite de tamaño de archivo máximo y la ubicación del archivo de registro. Utilice esta configuración cuando desee solucionar un problema

relacionado con el producto y proporcionar los registros al Soporte técnico de McAfee para realizar análisis adicionales.



Configure las opciones de **Debug Log** (Registro de depuración) para solucionar problemas y solamente por una duración limitada. Cuando capture suficientes registros para solucionar problemas, defina el valor de **Nivel** en **Ninguno**. El uso indiscriminado del registro de depuración podría ocupar demasiado espacio en el disco duro y afectar al rendimiento general del servidor. Actívalo por una duración limitada según lo aconsejado por el personal autorizado (ingeniero de soporte técnico de McAfee).


### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Diagnósticos**.



Aparece la página **Diagnósticos**.

- 2 En la ficha **Registro de depuración**, puede usar:

**Tabla 5-15 Definiciones de las opciones**

Opción	Definición
<b>Nivel</b>	<p>Para activar o desactivar el registro de depuración y especificar el nivel de información que se debe capturar en el archivo de registro de depuración. Puede seleccionar:</p> <ul style="list-style-type: none"> <li>• <b>Ninguno</b>: para desactivar el registro de depuración.</li> <li>• <b>Bajo</b>: para registrar eventos de importancia, como errores, excepciones y valor devueltos de funciones, en el archivo de registro de depuración. Seleccione esta opción si desea guardar un archivo de registro de depuración pequeño.</li> <li>• <b>Medio</b>: para registrar los eventos mencionados en el estado <b>Bajo</b> e información adicional que podría ser de ayuda para el equipo de soporte técnico.</li> <li>• <b>Alto</b>: para registrar todos los errores críticos, las advertencias y los mensajes de depuración en el archivo de registro de depuración. Contiene información sobre todas las actividades realizadas por el producto. Este es el nivel más detallado de registro admitido por el producto.</li> </ul>
<b>Activar límite de tamaño</b>	Si desea especificar un límite de tamaño de archivo máximo para cada archivo de registro de depuración.
<b>Especificar el tamaño máximo de archivo</b>	<p>Para especificar el tamaño máximo de los archivos de registro de depuración. Puede especificar un valor entre 1 KB y 2000 MB.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Si los archivos de registro de depuración superan el tamaño de archivo especificado, se reescribirán los eventos anteriores debido al registro circular, donde las nuevas entradas de registro se agregan al archivo eliminando las entradas de registro más antiguas.                 </div>

**Tabla 5-15 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Activar registro de depuración</b>	<p>Si desea modificar la ubicación predeterminada del registro de archivo de depuración.</p> <p> Si esta opción se desactiva, los archivos de registro de depuración se almacenan en el directorio predeterminado <code>&lt;Install Folder&gt;\bin\debuglogs</code>.</p>
<b>Especificar ubicación del archivo</b>	<p>Permite especificar la ruta del archivo de registro de depuración donde se pueden almacenar los eventos activados por MSME. Puede seleccionar:</p> <ul style="list-style-type: none"> <li>• <b>&lt;Carpeta de instalación&gt;</b>: para crear los archivos de registro de depuración en el directorio de instalación de MSME.</li> <li>• <b>&lt;Unidad del sistema&gt;</b>: para crear los archivos de registro de depuración en el directorio <code>C:\Windows\system32</code>.</li> <li>• <b>&lt;Archivos de programa&gt;</b>: para crear los archivos de registro de depuración en el directorio <code>C:\Archivos de programa (x86)</code> de Windows.</li> <li>• <b>&lt;Carpeta de Windows&gt;</b>: para crear los archivos de registro de depuración en el directorio <code>C:\Windows</code>.</li> <li>• <b>&lt;Carpeta de datos&gt;</b>: para crear los archivos de registro de depuración en el directorio <code>C:\ProgramData\</code>.</li> <li>• <b>&lt;Ruta completa&gt;</b>: para almacenar los archivos de registro de depuración en la ruta completa especificada en el cuadro de texto adyacente.</li> </ul> <p> Para almacenar los archivos de registro de depuración en una ubicación o subcarpeta personalizada, especifique el nombre de la subcarpeta o ruta de acceso en el campo junto a la lista desplegable.</p>



Asegúrese de que la carpeta que recopila los registros de depuración tiene permisos de escritura para la cuenta SERVICIO DE RED.

3 Haga clic en **Aplicar** para guardar la configuración.



Para obtener más información sobre la generación del registro de envoltorio de Exchange Web Services (EWS) para la tarea de análisis bajo demanda, consulte el artículo de McAfee KnowledgeBase [KB82215](#).

Ya ha configurado satisfactoriamente las opciones de registro de depuración que puede usar para la solución de problemas.

## Configuración del registro de eventos

Permite configurar el registro de los tipos de eventos de MSME en el **Registro del producto** y en el Visor de eventos de Windows.

Un evento es una posible acción que se realiza, bajo la supervisión de MSME. **Registro de eventos** proporciona información útil para realizar diagnósticos y auditorías. Los diferentes tipos de eventos son:

- Error
- Información
- Advertencia

Permite a los administradores del sistema obtener información sobre problemas de una forma más fácil.



### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Diagnósticos**.

Aparece la página **Diagnósticos**.

- 2 Haga clic en la ficha **Registro de eventos**. Puede usar:

**Tabla 5-16 Definiciones de las opciones**

Opción	Definición
<b>Registro del producto</b>	Para registrar eventos de MSME en el <b>Registro del producto</b> . Los eventos se podrán visualizar en <b>Configuración y diagnósticos</b>   <b>Registro del producto</b>   <b>Ver resultados</b> .
<b>Registro de eventos</b>	Para registrar eventos de MSME en el Visor de eventos de Windows. Para buscar eventos relacionados con MSME en el Visor de eventos de Windows: <ol style="list-style-type: none"><li>1 Vaya a <b>Visor de eventos (local)</b>   <b>Registros de Windows</b>   <b>Aplicación</b>.</li><li>2 En el panel <b>Aplicación</b>, los eventos relacionados con el producto aparecerán como <b>MSME</b> en la columna <b>Origen</b>.</li></ol>
<b>Registrar eventos de información</b>	Permite registrar eventos que se categorizan como <b>Información</b> .
<b>Registrar eventos de advertencia</b>	Permite registrar eventos que se categorizan como <b>Advertencia</b> .
<b>Registrar eventos de error</b>	Permite registrar eventos que se categorizan como <b>Error</b> .

- 3 Haga clic en **Aplicar** para guardar la configuración.

## Configuración de las opciones del registro del producto

Configure las opciones de la página **Configuración y diagnósticos** | **Registro del producto** mediante los parámetros requeridos para generar registros de productos.




### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Diagnósticos**.

Aparece la página **Diagnósticos**.

- 2 Haga clic en la ficha **Registro del producto**. Puede usar:

Tabla 5-17 Definiciones de las opciones

Opción	Definición
<b>Ubicación</b>	Si desea configurar una ubicación para almacenar el registro del producto. Seleccione <b>Activar</b> para especificar una ubicación personalizada.
<b>Especificar ubicación de base de datos</b>	<p>Permite especificar la ruta de la ubicación del archivo de registro del producto donde se pueden almacenar eventos de registro del producto. Puede seleccionar:</p> <ul style="list-style-type: none"> <li>• <b>&lt;Carpeta de instalación&gt;</b>: para crear el archivo de registro del producto en el directorio de instalación de MSME.</li> <li>• <b>&lt;Unidad del sistema&gt;</b>: para crear el archivo de registro del producto en el directorio C:\Windows\system32.</li> <li>• <b>&lt;Archivos de programa&gt;</b>: para crear el archivo de registro del producto en el directorio C:\Archivos de programa (x86) de Windows.</li> <li>• <b>&lt;Carpeta de Windows&gt;</b>: para crear el archivo de registro del producto en el directorio C:\Windows.</li> <li>• <b>&lt;Carpeta de datos&gt;</b>: para crear el archivo de registro del producto en el directorio C:\ProgramData\.</li> <li>• <b>&lt;Ruta completa&gt;</b>: para almacenar el archivo de registro del producto en la ruta completa especificada en el cuadro de texto adyacente.</li> </ul> <p> Para almacenar el archivo de registro del producto en la ubicación personalizada o en un subdirectorio, especifique el nombre del subdirectorio o la ruta en el campo que se encuentra junto a la lista desplegable.</p>
<b>Nombre de archivo</b>	Si desea especificar un nombre de archivo diferente donde almacenar el registro del producto. Seleccione <b>Activar</b> para especificar un nombre de archivo personalizado.
<b>Especificar nombre de archivo de la base de datos</b>	<p>Para especificar un nombre de archivo personalizado para el registro del producto. El nombre de archivo predeterminado es <code>productlog.bin</code> en el directorio <code>&lt;Carpeta de instalación&gt;\Data\</code>.</p> <p> Si modifica la ruta o el nombre predeterminados del archivo de registro del producto, las entradas del registro de la página <b>Configuración y diagnósticos   Registro del producto</b> se restablecerán y no aparecerán las entradas anteriores del registro.</p>
<b>Límite de tamaño</b>	Si desea especificar un límite de tamaño diferente para el archivo de registro del producto, seleccione <b>Activar límite de tamaño de base de datos</b> para especificar un tamaño de archivo personalizado.
<b>Especificar el tamaño máximo de base de datos</b>	<p>Permite especificar el tamaño del archivo de registro del producto. Puede especificar un valor que va de 1 KB a 2000 MB.</p> <p> Si el archivo de registro del producto supera el tamaño de archivo especificado, se sobrescriben eventos de registro anteriores debido al registro circular, donde se eliminan del archivo las entradas de registro más antiguas para añadir nuevas entradas.</p>
<b>Limitar la antigüedad de las entradas</b>	Si desea que se eliminen las entradas del registro del producto transcurrido un periodo de tiempo definido.
<b>Antigüedad máxima de la entrada</b>	Permite especificar el número de días que una entrada debe permanecer en el archivo de registro del producto antes de eliminarse. Puede especificar un valor de 1 a 365.

**Tabla 5-17 Definiciones de las opciones** (continuación)

Opción	Definición
<b>Tiempo de espera de consulta</b>	Si desea limitar el tiempo permitido para responder una consulta de registro del producto, seleccione <b>Activar</b> para especificar la duración.
<b>Especificar tiempo de espera de consulta (segundos)</b>	Permite especificar el número máximo de segundos permitidos cuando se responde a una consulta de registro del producto. Puede especificar un valor de 1 a 3600.

- Haga clic en **Aplicar** para guardar la configuración.

Ha configurado correctamente las opciones de la página **Registro del producto**.

## Configuración del servicio de informe de errores

Permite configurar los informes de errores o excepciones del producto para McAfee.

### Procedimiento

- En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Diagnósticos**.

Aparece la página **Diagnósticos**.

- Haga clic en la ficha **Servicio de informe de errores**. Puede usar:

**Tabla 5-18 Definiciones de las opciones**

Opción	Definición
<b>Activar</b>	Permite activar o desactivar el servicio de informe de errores.
<b>Atrapar excepciones</b>	Permite capturar información sobre eventos excepcionales, como bloqueos del sistema.
<b>Informar excepciones al usuario</b>	Permite especificar si se deberán notificar las excepciones al administrador.

- Haga clic en **Aplicar** para guardar la configuración.

## Ver registros del producto

Consulte el estado del producto mediante las entradas del registro sobre eventos, información, advertencias y errores. Por ejemplo, puede ver información acerca del inicio o la finalización de una tarea, errores del servicio del producto, etc.

Puede usar los filtros de búsqueda disponibles para encontrar las entradas del registro que le interesen.



Para modificar la configuración relacionada con la página de consulta de registros del producto, vaya a **Configuración y diagnósticos** | **Diagnósticos** | **Registro del producto**.


### Procedimiento

- En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Registro del producto**.

Aparece la página **Registro del producto**.

- En la sección **Registro del producto**, puede usar:

Tabla 5-19 Definiciones de las opciones

Opción	Definición
<b>ID</b>	Permite especificar el número que identifica una entrada del registro del producto concreta. Por ejemplo, si desea ver registros del producto solo con ID superiores a 2000, especifique: 200*
<b>Nivel</b>	Permite seleccionar <b>Información</b> , <b>Advertencia</b> o <b>Error</b> de la lista desplegable, según el tipo de registro que desee ver.
<b>Descripción</b>	Permite especificar una descripción pertinente. Por ejemplo, si desea ver registros según el inicio o la detención del servicio, escriba: *servicio*
<b>Todas las fechas</b>	Permite incluir eventos de todas las fechas según la entrada en el archivo del registro del producto.
<b>Rango de fechas</b>	Permite buscar un elemento en un rango de fechas definido según sus requisitos. Aquí puede especificar el día, el mes, el año y la hora con los parámetros <b>Desde</b> y <b>Hasta</b> . También puede usar el icono del calendario para especificar el rango de fechas.
<b>Borrar filtro</b>	Permite recuperar la configuración de búsqueda predeterminada.
<b>Exportar a archivo CSV</b>	Permite exportar y guardar información sobre todos los eventos devueltos por la búsqueda en formato .csv. Si hay miles de eventos en el registro, en lugar de navegar por varias páginas, puede usar esta opción para descargar estos eventos a un archivo con formato CSV y generar informes personalizados más tarde en Microsoft Excel. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Si no encuentra un campo específico en los resultados de búsqueda del archivo CSV, asegúrese de activar el campo necesario en la opción <b>Columnas para mostrar</b>.</p> <p>• Use la opción Importar datos de Microsoft Excel para abrir el archivo CSV en una ubicación distinta.</p> </div>

### 3 Haga clic en **Buscar**.



La cantidad máxima de registros que se pueden almacenar en el registro del producto depende del tamaño del archivo de registro.

Una lista de eventos que coinciden con sus criterios de búsqueda se muestra en la sección **Ver resultados**.

## Configuración de DAT

Permite especificar el número de DAT antiguos que se pueden conservar en el sistema.

Los archivos DAT son archivos de definición de detecciones, también llamados archivos de firma, que identifican código antivirus y/o software antispyware, que detectan para reparar virus, troyanos y PUP. Para obtener información sobre archivos .DAT, consulte el siguiente glosario: <http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat>

### Procedimiento

1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Configuración de DAT**.

Aparece la página **Configuración de DAT**.

- 2 Use **Número máximo de DAT antiguos** para especificar el número máximo de generaciones de DAT que se conservarán en el sistema durante los análisis regulares. MSME conserva los DAT recientes y antiguos en el directorio <Carpeta de instalación>\bin\DATs. Cuando se realiza una actualización de DAT nuevos, MSME comprueba el número disponible de DAT. Si el total de DAT disponibles es mayor que el número de DAT conservados, los DAT antiguos se eliminan. Puede especificar un valor entre 3 y 10; el valor predeterminado es 10.
- 3 Haga clic en **Aplicar** para guardar la configuración.


## Importación y exportación de opciones de configuración

Defina opciones para exportar la configuración existente de MSME (configuración y directivas) para importarla y usarla en otro servidor de MSME. Importe también listas Sitelist para especificar la ubicación desde la que se descargan las actualizaciones automáticas.

En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Importar y exportar configuración**. En la página **Importar y exportar configuraciones**, puede usar estas fichas:

- **Configuración:** sirve para exportar, importar o restaurar configuraciones del producto.

**Tabla 5-20 Ficha Configuración. Definiciones de las opciones**

Opción	Definición
<b>Exportar</b>	Para copiar la configuración (configuraciones y directivas) de MSME de este servidor y guardarla en una ubicación desde donde se pueda importar en otros servidores de MSME. El archivo de configuración de MSME predeterminado es <code>McAfeeConfigXML.cfg</code> .
<b>Restaurar valor predeterminado</b>	Para restablecer la configuración de MSME al rendimiento máximo.
<b>Restauración mejorada</b>	Para restablecer la configuración de MSME al rendimiento máximo.
<b>Examinar</b>	Para localizar el archivo de configuración ( <code>McAfeeConfigXML.cfg</code> ) que desee importar.
<b>Importar</b>	<p>Para aplicar la configuración de otro servidor de MSME a este servidor. Por ejemplo, para instalar MSME 8.5 en 5 sistemas:</p> <ol style="list-style-type: none"> <li>1 Instale MSME en el sistema 1.</li> <li>2 Configure los parámetros según sea preciso.</li> <li>3 Exporte la configuración al archivo <code>cfg</code>.</li> </ol> <p>Para obtener más información sobre la importación de la configuración, consulte el paso 10 en <i>Instalar el software mediante el asistente</i>.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Debe importar la configuración en la misma versión de producto. Por ejemplo, no es posible importar configuraciones de un servidor de MSME 8.7.6 u 8.0 a un servidor de MSME 8.5.                 </div>

- **Sitelist:** permite importar una Sitelist que especifique la ubicación desde donde se pueden descargar actualizaciones automáticas.

**Tabla 5-21 Ficha Sitelist. Definiciones de las opciones**

Opción	Definición
<b>Examinar</b>	Permite ubicar el archivo de Sitelist ( <code>SiteList.xml</code> ) que desea utilizar.
<b>Importar</b>	Para aplicar las opciones de configuración de la lista Sitelist especificadas en el archivo para descargar las actualizaciones de DAT.

## Exportación de la configuración existente de MSME

Permite exportar la configuración de un servidor de MSME y guardarla en una ubicación desde donde pueda ser importada por otros servidores de MSME.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Importar y exportar configuración**.  
Aparece la página **Importar y exportar configuraciones**.
- 2 Haga clic en la ficha **Configuración**.
- 3 Haga clic en **Exportar**.
- 4 Especifique una ubicación en la que desea guardar el archivo de configuración. El nombre predeterminado del archivo de configuración es `McAfeeConfigXML.cfg`.
- 5 Haga clic en **Guardar**.

Ha exportado satisfactoriamente la configuración y las directivas existentes de MSME a un archivo de configuración, que podrá ser importando por otros servidores de MSME.

## Importación de configuración desde otro servidor de MSME

Aplicar opciones de configuración de MSME desde otro servidor a este servidor de MSME.

Puede importar la configuración de dos modos:

- Importar la configuración mientras instala el software.
- Importar la configuración después de instalar el software mediante la opción **Importar y exportar configuración** en la página **Configuración y diagnósticos**.



- Debe importar la configuración en la misma versión de producto. Por ejemplo, no es posible importar configuraciones de servidor de MSME de un servidor de MSME 7.6 a un servidor de MSME 8.0.
- Se recomienda importar configuraciones desde un servidor de MSME que tenga las mismas funciones de Exchange.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos | Importar y exportar configuración**.  
Aparece la página **Importar y exportar configuraciones**.
- 2 Haga clic en la ficha **Configuración**.
- 3 En la sección **Importar configuración**, haga clic en **Examinar** para ubicar el archivo de configuración. El nombre predeterminado del archivo de configuración es `McAfeeConfigXML.cfg`.
- 4 Haga clic en **Importar**.  
Aparecerá un cuadro de diálogo con el mensaje **The operation completed successfully** (La operación finalizó correctamente).
- 5 Haga clic en **Aceptar**.

Acaba de importar satisfactoriamente las opciones de configuración desde otro servidor de MSME a este servidor.

## Importación de Sitelist

Importe Sitelists que especifican la ubicación desde la cual se descargan las actualizaciones automáticas.

Una lista Sitelist específica de dónde descargar las actualizaciones automáticas. De manera predeterminada, MSME usa **Editor de Sitelist** que se dirige a una URL de McAfee para las actualizaciones automáticas.

Si el servidor de MSME es administrado por McAfee ePO, se usa la Sitelist de ePolicy Orchestrator para realizar las actualizaciones automáticas. Si no usa ePolicy Orchestrator para administrar el servidor de MSME, cree una Sitelist que dirija el servidor de MSME a un repositorio local.

Se pueden crear Sitelists alternativas mediante el software McAfee AutoUpdate Architect o McAfee ePO.

### Procedimiento

- 1 Haga clic en **Configuración y diagnósticos** | **Importar y exportar configuración**. Aparecerá la página **Importar y exportar configuraciones**.
- 2 Haga clic en la ficha **Sitelist**.
- 3 En la sección **Importar Sitelist**, haga clic en **Examinar** para ubicar el archivo de Sitelist `SiteList.xml`. Este archivo contiene información relativa a la configuración del repositorio, como el nombre del repositorio o la URL del servidor.



Puede hallar el archivo `SiteList.xml` en el directorio `C:\ProgramData\McAfee\Common Framework\`. La aplicación **Editor de Sitelist**, que está en **Inicio** | **Todos los programas** | **McAfee** | **Security for Microsoft Exchange**, usa este archivo para mostrar la configuración del repositorio en la aplicación.

- 4 Haga clic en **Importar**.

Aparece un cuadro de diálogo con el mensaje **The operation completed successfully** (La operación finalizó correctamente).

- 5 Haga clic en **Aceptar**.

Ha importado correctamente la Sitelist que se dirige a una nueva ubicación del repositorio para descargar actualizaciones de productos.

---

## Configuración de proxy antispam

Permite configurar dichas opciones si la organización utiliza un servidor proxy para conectarse a Internet, para que MSME descargue las reglas antispam.

El software también puede usar este proxy para obtener la reputación de IP, la reputación de mensajes, y descargar la base de datos de URL local del servidor de GTI.



Esta función se aplica solamente si ha instalado el complemento McAfee Anti-Spam.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Configuración de proxy**. Aparecerá la página **Configuración de proxy**.
- 2 Seleccione **Utilizar proxy**. En la sección **Detalles del servidor proxy**, puede usar:

**Tabla 5-22 Definiciones de las opciones**

Opción	Definición
Dirección IP	Permite especificar la dirección IP del servidor proxy.
Puerto	Permite especificar el puerto utilizado para comunicaciones mediante Internet.
Detalles de autenticación	Permite especificar el tipo de autenticación. Puede usar: <ul style="list-style-type: none"><li>• <b>Anónimo</b>: sirve para tener acceso al equipo con proxy sin especificar ningún detalle de autenticación.</li><li>• <b>NTLM</b>: sirve para tener acceso al equipo con proxy usando credenciales de NT LAN Manager.</li><li>• <b>Autenticación básica</b>: sirve para proporcionar al sistema un <b>Nombre de usuario</b> y una <b>Contraseña</b> para acceder al equipo con proxy. Vuelva a escribir la contraseña en <b>Confirmar contraseña</b>.</li></ul>

- 3 Haga clic en **Aplicar** para guardar la configuración.



# 6

## Mantenimiento del programa

Permite realizar tareas de mantenimiento del producto, por ejemplo, modificar la instalación, reparar, desinstalar, restaurar configuraciones predeterminadas, y purgar y optimizar la base de datos.

### Contenido

- ▶ *Modificación de la instalación*
- ▶ *Restauración de configuraciones predeterminadas*
- ▶ *Purga y optimización*

---

## Modificación de la instalación

Modifique los componentes del programa MSME según sea necesario y cambie la forma en que se instalan dichos componentes en el equipo o si ha modificado la función de Exchange Server.



También puede modificar la instalación de MSME en la consola **Panel de control | Programas y características | Desinstalar un programa** mediante un clic en **Desinstalar/Modificar**.

### Procedimiento

- 1 En la carpeta que contiene los archivos de instalación, haga doble clic en `setup_x64.exe`.
- 2 En la pantalla Bienvenido, haga clic en **Siguiente**.  
Aparecerá la pantalla **Mantenimiento del programa**.
- 3 Seleccione **Modificar** y, luego, haga clic en **Siguiente**.
- 4 Seleccione los componentes del programa que quiere modificar y haga clic en **Siguiente**.
- 5 Seleccione **Acepto los términos del acuerdo de licencia**, después haga clic en **Siguiente**.
- 6 Haga clic en **Instalar** para finalizar la instalación con los componentes modificados del programa.
- 7 Haga clic en **Finalizar** cuando se complete la instalación.

## Restauración de configuraciones predeterminadas

Restaurar el producto a la configuración predeterminada y obtener un rendimiento máximo.

### Procedimiento

- 1 En la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Importar y exportar configuración**. Aparecerá la página **Importar y exportar configuración**.
- 2 En la ficha **Configuración**, haga clic en **Restaurar valor predeterminado**.



La restauración a los valores predeterminados elimina todas las opciones de directivas principales y secundarias que hayan sido configuradas. Se recomienda realizar una copia de seguridad de las configuraciones existentes para realizar una restauración más tarde.

Aparecerá un cuadro de diálogo para que confirme la configuración.

- 3 Haga clic en **Aceptar**.

Aparecerá un cuadro de diálogo que confirma que se están aplicando las opciones de configuración predeterminadas.

- 4 Haga clic en **Aceptar**.

Ha restaurado satisfactoriamente el servidor de MSME a la configuración predeterminada para obtener un rendimiento máximo.

## Purga y optimización

Elimina de la base de datos elementos antiguos marcados para su eliminación y ejecuta la tarea de optimización para recuperar espacio en el disco ocupado por los registros de la base de datos eliminados.

### Procedimiento

- 1 Desde la interfaz de usuario del producto, haga clic en **Configuración y diagnósticos** | **Elementos detectados**. Aparecerá la página **Elementos detectados**.
- 2 En la sección **Base de datos local**, puede usar:

- **Purge of old items frequency** (Frecuencia de purga de elementos antiguos): especifica la frecuencia de eliminación de la base de datos de MSME de los elementos antiguos marcados para su eliminación. El valor predeterminado es **Mensualmente**.
- **Optimization frequency** (Frecuencia de optimización): recupera el espacio en disco ocupado con registros de bases de datos eliminados. Según el valor establecido en **Maximum item age (days)** (Antigüedad máxima de elemento [días]), los registros antiguos se eliminan si programó una tarea de purga. Una vez que elimina estos registros antiguos, MSME seguirá usando el espacio en disco especificado en el campo **Disk space threshold (MB)** (Umbral de espacio en disco [MB]), incluso si la base de datos en cuarentena no alcanzó su límite de tamaño. Para optimizar y reducir la base de datos, programe una tarea de optimización. El valor predeterminado es **Mensualmente**.



Siempre programe una tarea de optimización unas horas antes de que lleve a cabo la tarea de purga.

- 3 Haga clic en **Editar programación** (Editar programación) para modificar la programación.



Estas tareas deben realizarse regularmente para mantener el espacio libre suficiente en la base de datos.

# 7

## Solución de problemas

Detecte y solucione problemas al usar MSME. Conozca los contadores de rendimiento disponibles y las claves de registro importantes que se asocian con el producto.

### Contenido

- ▶ *Configuración predeterminada en comparación con la configuración mejorada*
- ▶ *Claves de registro importantes*

## Configuración predeterminada en comparación con la configuración mejorada

En función de sus requisitos, puede configurar MSME para lograr un rendimiento máximo o una protección máxima.

Para modificar las opciones de configuración de MSME, vaya a **Configuración y diagnósticos | Importar y exportar configuración**. Puede usar:

- **Restaurar valor predeterminado:** para configurar MSME para alcanzar un rendimiento máximo.
- **Restauración mejorada:** para configurar MSME para alcanzar una protección máxima.

**Tabla 7-1 Diferencias entre configuración predeterminada y mejorada**

Función	Predeterminada	Mejorada
Reputación de mensajes	Desactivada	Activada
Reputación de IP	Desactivada	Activada
Máximo nivel de anidamiento	10	50
Archivo protegido con contraseña	Permitir paso	Reemplazar y poner en cuarentena
Archivo protegido	Permitir paso	Reemplazar y poner en cuarentena
Filtro de archivos	Desactivada	Activado con regla predeterminada (*.exe, *.com, *.bat, *.scr)
Archivo cifrado	Permitir paso	Reemplazar y poner en cuarentena
Archivo dañado	Permitir paso	Reemplazar y poner en cuarentena
Reputación de URL de correo	Desactivada	Activada para las directivas de análisis en tiempo real.

## Claves de registro importantes

Cree estas claves de registro cuando la significancia coincida con sus necesidades.

**Tabla 7-2 Claves de registro importantes de MSME**

Clave de registro	Ruta	Significancia
Nombre: DigestMail Tipo: DWORD Valor 1	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME ADUserCache	Conserva en caché el alias de usuario y la dirección SMTP, que se utilizan cuando MSME se integra con MQM, y se emplea la misma dirección para la función Correo de resumen.
Nombre: ODUserID Tipo: REG_SZ Valor [Por ejemplo: <admin@dominio.com>]	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME E2007	Solo es válida para los servidores de buzones de correo de Exchange. Debe ser la dirección de correo electrónico del usuario bajo demanda creada por el producto; se utiliza para la interacción con los servicios web de Exchange a fin de obtener los datos de correo de la base de datos de Exchange.
Nombre: EWSUrl Tipo: REG_SZ Valor https://<dirección IP>/EWS/Exchange.asmx	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME OnDemand	Solo es válida para los servidores de buzones de correo de Exchange 2010. Es la dirección URL empleada para conectar con los servicios web de Exchange alojados por el servidor CAS. Este valor se rellena mediante el script de PowerShell GetHubTxDetails.ps1 durante la instalación y también siempre que se reinicia el servicio de MSME.
Nombre: SCLJunkThreshold Tipo: DWORD Valor predeterminado: 4	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Solo es válida para los servidores de buzones de correo de Exchange 2010. Es el umbral de correo no deseado de SCL, que se recupera de AD y corresponde al nivel de organización. Cualquier calificación que supere este valor se tratará como correo no deseado, lo cual contribuye al enrutamiento del correo electrónico no deseado en los servidores de concentradores de Exchange 2007/2010. Este valor se rellena mediante el script de PowerShell GetSCLJunkThreshold.ps1 durante la instalación, y también posteriormente según una frecuencia.
Nombre: IPBlackList Tipo: REG_SZ Valor: [Ejemplo: 10.0.0.1]	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME SystemState	Permite bloquear una dirección IP específica o un intervalo de direcciones IP de forma que no puedan enviar correo electrónico a su organización independientemente de la reputación de IP.
Nombre: SPFMaxTimeSec Tipo: DWORD Valor predeterminado: 5	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Tiempo máximo que se permite la ejecución de SPF. Si el tiempo supera el tiempo definido, el resultado es un <i>error temporal</i> y el correo se entrega.
Nombre: SPFCacheTimeoutSec Tipo: DWORD Valor predeterminado: 43200	HKEY_LOCAL_MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Cantidad de tiempo que debe transcurrir para que la entrada en caché quede obsoleta. El valor predeterminado es de 12 horas.

**Tabla 7-2 Claves de registro importantes de MSME (continuación)**

Clave de registro	Ruta	Significancia
Nombre: SPFCacheMaxEntries Tipo: DWORD Valor predeterminado: 5000	HKEY_LOCAL MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Número máximo de entradas en caché.
Nombre: SPFDNSTimeoutMS Tipo: DWORD Valor predeterminado: 1000	HKEY_LOCAL MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Tiempo de espera para cada solicitud DNS en milisegundos.
Nombre: CacheTimeOutForNullRecords Tipo: DWORD Valor predeterminado: 60	HKEY_LOCAL MACHINE SOFTWARE Wow6432Node McAfee\MSME AntiSpam	Tiempo de espera para registros nulos (en caso de error temporal) en segundos.



Las claves de Registro SPFMaxTimeSec, SPFCacheTimeoutSec, SPFCacheMaxEntries, SPFDNSTimeoutMS y CacheTimeOutForNullRecords se crean solo si se ha instalado el componente McAfee Anti-Spam o se ha instalado el software mediante la opción de instalación Completa.



# 8

## Preguntas frecuentes

Proporciona repuestas a situaciones comunes que el usuario puede enfrentar al instalar o utilizar el producto, y contiene información para solucionar problemas con el formato de preguntas frecuentes.



Para ver una lista actualizada de preguntas asociadas con esta versión, consulte el artículo [KB76886](#) de McAfee KnowledgeBase.

### Contenido

- ▶ *General*
- ▶ *Administrador de directivas*
- ▶ *Configuración y diagnósticos*
- ▶ *Complemento McAfee Anti-Spam*
- ▶ *Expresiones regulares (regex)*

---

## General

A continuación, se presentan respuestas a preguntas frecuentes generales.

### ¿Se puede priorizar la entrega del correo electrónico?

No. No es posible priorizarlo porque se trata de una tarea de Exchange Server.

### ¿Tengo que activar igualmente el acceso anónimo al conector de recepción de Exchange Server?

MSME no requiere acceso anónimo al conector de recepción de Exchange Server. El usuario bajo demanda se encarga de estas funciones. Para obtener más información acerca de la configuración de las opciones de acceso anónimo, consulte el artículo de la base de conocimiento de McAfee [KB81752](#).

### Si se analiza un mensaje de correo electrónico en el servidor de transporte de concentradores, ¿se analizará en el servidor de buzones de correo?

Depende. Si el correo electrónico se analiza en el servidor de concentradores y tiene el mismo sello de antivirus, no se analiza en el servidor de buzones de correo. Si el sello de antivirus difiere en el proveedor de antivirus o presenta una versión de motor/DAT distinta, sí se analiza en el servidor de buzones de correo.

### ¿Por qué debo usar la opción "Ejecutar como administrador" en Windows 2008 para abrir la interfaz de usuario de MSME?

Por razones de seguridad, MSME no podrá comunicarse con los servidores RPC. Esto se debe a que el SID no tiene permiso para efectuar comunicaciones entre procesos (IPC) con procesos RPC.

### ¿Con qué ejecutable se cargan los módulos de análisis de MSME en todas las versiones de Exchange?

El proceso `RPCserv.exe` carga todos los archivos binarios de análisis. Para buscar el ID de proceso del analizador, revise la línea de comandos del **Administrador de tareas** y verifique qué proceso `RPCserv.exe` tiene el parámetro de línea de comandos `/EVENTNAME:Global\MSME_scanner_RPCEvent`.

### ¿Cuál es la configuración óptima de MSME?

Las configuraciones son para **Protección mejorada** y **Rendimiento máximo**. La configuración predeterminada permite disfrutar de un rendimiento máximo.

**¿Qué debería excluir si tengo MSME y un antivirus de nivel de archivos instalados en el mismo servidor?**

Excluya todas las carpetas y subcarpetas binarias de MSME, la base de datos de Postgres, las carpetas de replicación, las carpetas de Exchange, la carpeta de eventos de McAfee ePO y el registro del producto.

**¿Dónde puedo encontrar más información sobre la seguridad del correo electrónico?**

Para obtener información sobre soluciones relacionadas con la seguridad del correo electrónico, véase <http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx>.

**¿Cómo se accede a la interfaz del producto del sistema remoto?**

Para obtener acceso a la interfaz autónoma y remota de MSME:

- 1 Inicie **McAfee Security for Microsoft Exchange - Configuración del producto**.
- 2 En el menú **Cambiar servidor**, haga clic en **Nueva conexión**.
- 3 En el cuadro de diálogo **Buscar equipo**, escriba la dirección IP del sistema remoto y haga clic en **Aceptar**.

Para obtener acceso a la interfaz web remota de MSME:

- 1 Inicie **McAfee Security for Microsoft Exchange - Configuración del producto (interfaz web)**.
- 2 En la barra de dirección, escriba: `https://<Remote system IP Address>/MSME/0409/html/index.htm`
- 3 Proporcione las credenciales de inicio de sesión cuando se le pidan.

**¿Cómo conecta MSME con el servidor de TIE?**

MSME conecta con el servidor de TIE a través de Data Exchange Layer (DXL) desde McAfee ePO. La instancia de McAfee ePO que gestiona MSME también debe gestionar el servidor de TIE.

**¿Cómo se configura el servidor de TIE en MSME?**

No es posible configurar el servidor de TIE directamente desde MSME. No obstante, el servidor de McAfee ePO que gestiona MSME debería gestionar también el servidor de TIE. Para integrar el servidor de TIE con McAfee ePO, véase la *Guía del producto de McAfee Threat Intelligence Exchange*.

---

## Administrador de directivas

Aquí encontrará respuestas a las preguntas frecuentes sobre el **Administrador de directivas**.

**¿Cómo se crean y se usan las directivas de correo electrónico?**

Siempre cree directivas en servidores gateway usando direcciones SMTP y en servidores de buzón de correo usando grupos de Active Directory (AD). En los servidores de buzón de correo, diseñar directivas basadas en direcciones SMTP es muy costoso, ya que el producto no obtiene direcciones SMTP y para resolverlo se realizan consultas de AD. Esto reduce el rendimiento en servidores de buzón de correo.

**¿Los nombres de dominio en las directivas afectan el rendimiento?**

Sí. Para obtener una explicación detallada, vea la consulta anterior, *¿Cómo se crean y se usan las directivas de correo electrónico?*

**¿Cómo funcionan las directivas por prioridad?**

Cada vez que se cumple primero una directiva secundaria basada en la prioridad de resolución, la siguiente directiva nunca se evalúa.

**¿Es bueno tener varias directivas? ¿Esto afecta el rendimiento del servidor?**

Sí, esto afecta al rendimiento. Durante la evaluación de la directiva, cuando la primera directiva secundaria no se cumple y se evalúa la siguiente directiva, es posible que se deban realizar consultas de AD, lo cual genera un rendimiento lento.

**¿Cómo se configura MSME para bloquear archivos ejecutables en un nivel granular?**



Puede hacerlo usando la opción **Reglas de filtrado de archivos**. Por ejemplo, veamos cómo filtrar archivos ejecutables específicos, como los ejecutables de Windows.

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | En tiempo real (directiva principal)**.
- 2 En **Analizadores principales**, haga clic en **Filtrado de archivos** y active esta opción.
- 3 En **Options (Core Anti-Spam Settings)** (Opciones [Configuración antispam principal]), haga clic en **Editar**.
- 4 En la lista desplegable **Reglas disponibles**, seleccione **<Crear nueva regla...>**.
- 5 Especifique un nombre de regla y en **Filtrado de categorías de archivos**, seleccione **Activar filtrado de categoría de archivo**.
- 6 En la lista **Categorías de archivo**, seleccione **Otros formatos específicos**.
- 7 En la lista **Subcategorías**, seleccione **Ejecutables de Windows**.
- 8 Haga clic en **Guardar**.

### ¿Qué tipo de archivo se detecta como herramienta de compresión o PUP? ¿Desde dónde se controla esta opción?

Las herramientas de compresión y PUP pertenecen a la categoría de contenido malicioso que se detecta según la categoría. Las herramientas de compresión son generalmente archivos que se comprimen con un algoritmo y se descomprimen al ejecutarse.

Controle esta opción desde **Configuración antivirus** en la interfaz de usuario de MSME.

---

## Configuración y diagnósticos

Aquí encontrará respuestas a las preguntas frecuentes sobre **Configuración y diagnósticos**.

### ¿La activación de McAfee GTI genera latencia de correo electrónico?

Sí, habrá latencia debido a que McAfee GTI valida el correo electrónico.

### ¿Cómo se verifica si el analizador de transporte está buscando spam?

Puede verificar esto desde la interfaz de usuario del producto de alguna de las siguientes maneras:

- En la página **Elementos recientemente analizados**, consulte los correos analizados y revise la política utilizada para analizar el correo electrónico. Debe mostrar **Gateway** en el campo **Analizado por**.
- Desde la base de datos de **Elementos detectados**, verifique si se detectó spam. Por último, verifique si los correos electrónicos no atraviesan sesiones autenticadas, que se registran en **Registro de depuración** de MSME.

### ¿Es posible exportar las listas negras y las listas blancas de un servidor de MSME a otro?

Sí, puede exportar las listas negras y las listas blancas de un servidor de MSME a otro. Para ello:

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Gateway (Directiva principal)**.
- 2 En **Analizadores principales**, haga clic en **Antispam**.
- 3 En **Options (Core Anti-Spam Settings)** (Opciones [Configuración antispam principal]), haga clic en **Editar**.
- 4 Haga clic en la ficha **Listas de correo** y, luego, haga clic en **Exportar** para guardar todos los remitentes y los destinatarios en lista negra o blanca en un archivo CSV.

## Complemento McAfee Anti-Spam

Estas son respuestas a las preguntas frecuentes sobre el complemento antispam.

### ¿Cómo actualizo el motor antispam manualmente?

Actualice la clave de registro y coloque el nuevo motor en el directorio especificado que se detalla en el registro, en la clave de registro `SpamEngineVersion` del registro `MSME\SystemState`. Estos dos valores deben estar sincronizados. Por ejemplo, si la versión del motor es 9039, cree un directorio con el nombre 9039 en `MSME\Bin\AntiSpam\Engine` y copie el archivo `masecore.dll` del motor en ese directorio.

### ¿Puedo editar las reglas antispam manualmente?

No.

### ¿Qué debo tener en cuenta antes de añadir una dirección de correo electrónico a la lista negra?

- Asegúrese de que el complemento McAfee Anti-Spam esté instalado.
- Microsoft Exchange Server debe ser un servidor de transporte. Por ejemplo, tenga un Exchange Server con función de transporte perimetral o de transporte de concentradores.
- Tenga una conexión no autenticada, donde los correos electrónicos lleguen al servidor directamente desde Internet.

### ¿Cómo incluyo una dirección de correo electrónico en una lista negra o en una lista blanca?

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas | Gateway (Master Policy)** (Gateway [Directiva principal]).
- 2 En **Analizadores principales**, haga clic en **Antispam**.
- 3 En **Options (Core Anti-Spam Settings)** (Opciones [Configuración antispam principal]), haga clic en **Editar**.
- 4 Haga clic en la ficha **Listas de correo** y luego en **Agregar** para ver las opciones necesarias, como destinatarios o remitentes en lista blanca o negra.

### ¿Qué debo hacer cuando algunos correos electrónicos no se detectan como spam?

En **Configuración y diagnósticos | Antispam**, seleccione **Activar reputación de mensajes** y aplique la configuración. Además, ajuste la calificación de spam a un valor entre 51 y 79, que ayudará con la tasa de detección.



Los correos electrónicos con una calificación de spam menor (entre 51 y 59) pueden ser legítimos de todas maneras, así que es necesario ajustar detalladamente la calificación.

### ¿Dónde puedo obtener la licencia del complemento antispam?

Puede descargar el archivo `MSMEASA.ZIP` del sitio de descarga de McAfee, si tiene un número de concesión válido de McAfee Anti-Spam. Si no tiene un número de concesión válido, llame al equipo de Servicio de atención al cliente de McAfee.

## Expresiones regulares (regex)

A continuación, se presentan respuestas a las preguntas frecuentes sobre expresiones regulares (regex).

### ¿La activación de regex genera latencia de correo electrónico?

Sí, la activación de las expresiones regulares causa latencia de correo electrónico, ya que el análisis de contenido es una configuración de uso intensivo de procesos.

### ¿Dónde puedo encontrar más información sobre regex?

Varios sitios web en Internet proporcionan información sobre expresiones regulares.

Por nombrar algunos, consulte:

- <http://www.regular-expressions.info/reference.html>
- <http://www.regexbuddy.com/regex.html>

### ¿Cómo hago para bloquear ciertos números de tarjeta de crédito y de seguro social con regex?

- 1 En la interfaz de usuario del producto, haga clic en **Administrador de directivas** | **Recurso compartido**. Aparecerá la página **Recursos compartidos**.
- 2 En la pestaña **Diccionarios de conformidad y DLP**, haga clic en **Nueva categoría** y especifique un nombre de categoría.
- 3 Haga clic en **Aceptar**.
- 4 En **Reglas de conformidad y DLP**, haga clic en **Crear nueva**.
- 5 Especifique el **Nombre de regla**, la **Descripción** y, en **Palabra o frase**, especifique la expresión regular.

**Tabla 8-1 Ejemplo de cómo validar números de tarjeta de crédito**

Tipo de tarjeta	Expresión regular	Descripción
Visa	<code>^4[0-9]{12}(?:[0-9]{3})?\$</code>	Todos los números de tarjeta Visa comienzan con el número 4. Las tarjetas nuevas tienen 16 dígitos. Las tarjetas viejas tienen 13.
MasterCard	<code>^5[1-5][0-9]{14}\$</code>	Todos los números de MasterCard comienzan con el número 51 a 55. Todas tienen 16 dígitos.
American Express	<code>^3[47][0-9]{13}\$</code>	Los números de las tarjetas American Express comienzan con el número 34 o 37, y tienen 15 dígitos.
Diners Club	<code>^3(?:0[0-5] 68[0-9])[0-9]{11}\$</code>	Los números de las tarjetas Diners Club comienzan con 300 a 305, 36 o 38. Todas tienen 14 dígitos. Hay tarjetas Diners Club que comienzan con el número 5 y tienen 16 dígitos. Estas son de una empresa conjunta entre Diners Club y MasterCard, y se deben procesar como una tarjeta MasterCard.
Discover	<code>^6(?:011 5[0-9]{2})[0-9]{12}\$</code>	Los números de las tarjetas Discover comienzan con 6011 o 65. Todas tienen 16 dígitos.
JCB	<code>^(?:2131 1800 35\d{3})\d{11}\$</code>	Las tarjetas JCB que comienzan con 2131 o 1800 tienen 15 dígitos. Las tarjetas JCB que comienzan con 35 tienen 16 dígitos.

Según el ejemplo mencionado, puede crear una expresión regular similar para los números de seguridad social. Para obtener más ejemplos sobre expresiones regulares, consulte <http://www.regular-expressions.info/examples.html>.

- 6 Seleccione la opción **Expresión regular** y haga clic en **Guardar**.
- 7 Agréguela a la directiva de **Conformidad y DLP** en **Administrador de directivas** haciendo clic en **Administrador de directivas** | **En tiempo real (directiva principal)** | **Conformidad y DLP**.
- 8 En **Activación**, seleccione **Activar**.
- 9 En **Directivas y acciones asociadas de conformidad y DLP**, haga clic en **Agregar regla**.
- 10 En **Seleccionar grupo de reglas**, seleccione, en la lista desplegable, la regla regex que creó anteriormente.
- 11 Especifique la acción por realizar cuando la regla se activa.
- 12 Haga clic en **Guardar**.



# Índice

## A

- acción para realizar
  - elementos detectados [48](#)
- acciones
  - para realizar [61](#)
  - principal [61](#)
  - secundaria [61](#)
- actualización
  - software [22](#)
- actualización automática
  - programar [22](#)
- actualización de software
  - programar [22](#)
- Administrador de directivas
  - P+F [144](#)
- administrar
  - configuración de filtro [91](#)
  - configuración del analizador [72](#)
  - configuraciones varias [100](#)
  - datos en cuarentena [39](#)
- agregar
  - analizador [60](#)
  - filtro [60](#)
- alerta
  - creación de nueva [65](#)
- alertas
  - activación del estado de funcionamiento del producto [118](#)
  - configuración [64](#)
- alertas de estado de funcionamiento del producto
  - activación [118](#)
- amenazas
  - para su organización [10](#)
- amenazas para su organización [10](#)
- análisis bajo demanda [23](#)
  - creación [25](#)
  - programación [25](#)
  - vista [24](#)
- análisis de transporte
  - configuración en tiempo real [111](#)
- análisis en segundo plano
  - configuración en tiempo real [110](#)
- analizador
  - agregar [60](#)

- analizador antiphishing
  - opciones de configuración [90](#)
- analizador antispam
  - opciones de configuración [85](#)
- analizador antivirus
  - opciones de configuración [73](#)
- Analizador de conformidad y DLP
  - opciones de configuración [76](#)
- analizador principal
  - opciones de administración [72](#)
- analizador, control
  - opciones de configuración [96](#)
- analizadores [55](#)
  - configuración [63](#)
  - disponible [57](#)
- analizadores y filtros
  - cuadro comparativo [57](#)
  - lista [59](#)
- antispam
  - configuración [120](#)
- archivo prohibido, mensajes [40](#)
- archivo prohibido, tipos [40](#)
- archivos HTML
  - opciones de configuración [99](#)
- archivos protegidos con contraseña
  - opciones de configuración [94](#)
- asunto [35](#)
- avanzada
  - vista de directiva [52](#)

## B

- bajo demanda
  - análisis [23](#)
- base de datos
  - optimización [138](#)
  - PostgreSQL [123](#)
  - purga [138](#)
- base de datos de PostgreSQL [123](#)
- base de datos local
  - poner en cuarentena usando [123](#)
- base de datos local en comparación con MQM [39](#)
- bloquear manualmente
  - dirección IP [97](#)

buscar  
elementos detectados [47](#)

## C

calificación de spam [35](#)

campos de notificación  
mediante [117](#)

campos que puede usar, notificación [117](#)

caracteres comodín  
ejemplos [114](#)

claves  
registro [140](#)

claves de registro  
MSME [140](#)

complemento antispam  
P+F [146](#)

compresor [35](#)

comprobación de reputación  
mediante TIE [82](#)

configuración  
analizador antiphishing [90](#)  
analizador antispam [85](#)  
analizador antivirus [73](#)  
Analizador de conformidad y DLP [76](#)  
analizador, control [96](#)  
archivos HTML [99](#)  
archivos protegidos con contraseña [94](#)  
base de datos local [123](#)  
configuración de antispam [120](#)  
configuración de base de datos local [123](#)  
configuración de cuadros [126](#)  
configuración de diagnóstico [126](#)  
configuración de gráficos [126](#)  
configuración de McAfee Quarantine Manager [122](#)  
configuración de preferencias de interfaz de usuario [125](#)  
configuración de registro de eventos [128](#)  
configuración del panel [125](#)  
configuración del registro de depuración [126](#)  
configuración del registro del producto [129](#)  
configurar elementos detectados [121](#)  
configurar en tiempo real [107](#)  
contenido cifrado [93](#)  
contenido dañado [92](#)  
contenido firmado [93](#)  
contenido protegido [92](#)  
DAT [132](#)  
desde otro servidor [134](#)  
exportar [133](#)  
filtrado de archivos [78](#)  
filtro de tamaño de correo [94](#)  
importar [133](#)  
McAfee Quarantine Manager [122](#)  
mensaje de alerta [101](#)  
MIME, correo [97](#)

configuración (*continuación*)  
notificación [115](#)  
predeterminada y mejorada [139](#)  
servicio informe de errores, configuración [131](#)  
texto de renuncia [102](#)  
configuración de DAT  
configuración [132](#)  
configuración de directivas  
administrar analizador principal [72](#)  
administrar filtros [91](#)  
administrar varias [100](#)  
configuración de proxy  
configuración de antispam [135](#)  
configuración de VSAPI  
configuración [109](#)  
configuración en tiempo real  
configurar VSAPI [109](#)  
configuración existente  
exportación [134](#)  
configuración predeterminada  
restauración [138](#)  
configuración y diagnósticos  
descripción general [105](#)  
P+F [145](#)  
configurar  
alertas [64](#)  
analizadores [63](#)  
configuración de las notificaciones [115](#)  
configuración de proxy antispam [135](#)  
Reglas de conformidad y DLP [67](#)  
Reglas de filtrado de archivo [70](#)  
ubicación de cuarentena [39](#)  
configurar opciones en tiempo real  
análisis de transporte [111](#)  
análisis en segundo plano [110](#)  
conformidad y DLP [40](#)  
contenido cifrado  
opciones de configuración [93](#)  
contenido dañado  
opciones de configuración [92](#)  
contenido firmado  
opciones de configuración [93](#)  
contenido no deseable [40](#)  
contenido protegido  
opciones de configuración [92](#)  
correo electrónico de suplantación  
configurar error grave [89](#)  
configurar error leve [89](#)  
correo electrónico entrante  
análisis [13](#)  
correos electrónicos  
análisis de correos electrónicos [13](#)  
correos electrónicos internos  
análisis [15](#)

correos electrónicos salientes  
análisis 14

crear  
alerta, nueva 65  
análisis bajo demanda, tarea 25  
directiva secundaria 54  
nueva regla para usuario nuevo 60

cuadro comparativo  
analizadores y filtros 57

cuadros  
configuración 126

## D

datos en cuarentena  
administración 39

denegación de servicio 35

detección  
tiempo real 11

detección, tipos 40

diagnósticos  
configuración 126

Directiva principal 53

directiva secundaria 53

directivas  
orden 52  
prioridad 52

directivas secundarias  
creación 54

disponible  
analizadores y filtros 57

## E

editar  
plantilla de notificación 116

elementos detectados  
acción para realizar 48  
búsqueda 47  
cuadro comparativo 45  
filtros de búsqueda principales 42  
opciones adicionales de búsqueda 46  
opciones de configuración 121  
resultados de búsqueda 48  
vista 39

elementos en cuarentena  
acción para realizar 48

especificar  
usuario 60

estadísticas 17

Exchange Server  
protección de su 11

excluir buzones de correo 113

exclusión de buzón de correo  
opciones de configuración 113

exclusión de carpetas  
opciones de configuración 113

exportar  
configuración existente 134  
listas blancas 88  
listas negras 88  
opciones de configuración 133

expresiones regulares  
P+F 146

## F

filtro  
agregar 60  
opciones de administración 91

filtro de archivos  
opciones de configuración 78

filtro de tamaño de correo  
opciones de configuración 94

filtros 55  
disponible 57

filtros de búsqueda  
cuadro comparativo 45  
principal 42

filtros de búsqueda avanzada 35

filtros de búsqueda simple 34

funciones  
producto 7

funciones del producto 7

## G

general  
P+F 143

gráficos  
configuración 126

## H

herencia  
vista de directiva 52

## I

importar  
configuraciones desde otro servidor 134  
listas blancas 88  
listas negras 88  
opciones de configuración 133  
sitelists 133, 135

incluir en lista negra  
dirección IP 97

información estadística 17

informes  
gráficos 34

informes de configuración 31  
notificación por correo electrónico 33

informes de configuración 31 (*continuación*)  
 programación 32  
 vista 31

informes de estado 27  
 notificación por correo electrónico 30  
 programación 28  
 vista 27

informes gráficos 34

instalar  
 modificación 137

interfaz de usuario, preferencias  
 configuración 125

intervalos de tiempo 71

introducción 7

## L

lista  
 analizadores 59  
 filtros 59

lista blanca  
 exportación 88  
 importación 88

lista negra  
 exportación 88  
 importación 88

## M

McAfee Quarantine Manager  
 poner en cuarentena usando 122

mensaje de alerta  
 opciones de configuración 101

MIME 35

MIME, correo  
 opciones de configuración 97

modificar  
 instalación 137

MQM en comparación con base de datos local 39

## N

nombre de detección 35

notificación  
 configuración 115

notificaciones  
 configurar 115  
 informe de configuración 33  
 informe de estado 30

número de ficha 35

## O

opciones de búsqueda  
 elementos detectados 46

optimizar  
 base de datos 138

ordenar  
 directivas 52

## P

P+F  
 complemento antispam 146  
 configuración y diagnósticos 145  
 expresiones regulares 146  
 general 143  
 regex 146

panel  
 configuración 125

Panel 17

phishing 35, 40

plantilla de notificación  
 edición 116

predeterminada y mejorada  
 configuración 139

preguntas frecuentes 143

preguntas más frecuentes  
 Administrador de directivas 144

principal  
 acciones 61  
 analizadores 55  
 filtros 55

priorizar  
 directivas 52

programa  
 mantenimiento del 137

programa potencialmente no deseado 35

programar  
 actualización automática 22  
 análisis bajo demanda, tarea 25  
 informes de configuración 32  
 informes de estado 28

programas potencialmente no deseados 40

proteger  
 Exchange Server 11

purgar  
 base de datos 138

## R

recurso compartido 63  
 configuración de alertas 64  
 configuración de analizadores 63  
 configuración de reglas de conformidad y DLP 67  
 configuración de reglas de filtrado de archivos 70

regex  
 P+F 146

registro de depuración  
 configuración 126

registro de eventos  
 configuración 128



- registro del producto
  - configuración [129](#)
- registros del producto
  - vista [131](#)
- regla
  - creación de nuevas reglas para usuarios específicos [60](#)
- reglas
  - Conformidad y DLP [67](#)
  - filtrado de archivos [70](#)
- Reglas de conformidad y DLP
  - configuración [67](#)
- Reglas de filtrado de archivo
  - configuración [70](#)
- reputación de URL de correo [40](#)
  - configuración [79](#)
- restaurar
  - configuración predeterminada [138](#)

## S

- secundaria
  - acciones [61](#)
- servicio de informe de errores
  - configuración [131](#)
- sitelist
  - importación [133](#)
- Sitelist
  - importación [135](#)
- spam [40](#)
- suplantación
  - configurar protección [89](#)

## T

- texto de renuncia
  - opciones de configuración [102](#)
- tiempo real
  - detección [11](#)

- tiempo real, en, configuraciones [107](#)
- tipo de análisis
  - análisis bajo demanda [23](#)
- tipos de
  - directiva [53](#)
- tipos de análisis
  - bajo demanda [23](#)
- tipos de análisis en tiempo real
  - elementos enviados [107](#)
  - proactivo [107](#)
  - segundo plano [107](#), [110](#)
  - transporte [107](#), [111](#)
  - VSAPI [107](#)
- tipos de detección [40](#)

## U

- ubicación de cuarentena
  - configuración [39](#)
- usuario
  - especificar [60](#)
- usuario bajo demanda
  - restablecer contraseña [111](#)

## V

- varias
  - opciones de administración [100](#)
- ver
  - análisis bajo demanda [24](#)
  - elementos detectados [39](#)
  - informes de configuración [31](#)
  - informes de estado [27](#)
  - registros del producto [131](#)
- virus [40](#)
- vista de directiva
  - avanzada [52](#)
  - herencia [52](#)

