



Guía de instalación

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

1	Instalación y configuración	5
	Preinstalación	5
	Requisitos del sistema	6
	Funciones de Microsoft Exchange Server compatibles	7
	Contenido del paquete	7
	Instalación	8
	Instalación del software mediante el asistente de instalación	8
	Instalación manual del complemento McAfee Anti-Spam	11
	Cómo realizar una instalación silenciosa	11
	Ampliación de un despliegue independiente	14
	Configuración posterior a la instalación	15
	Configuración rápida	15
	Despliegue de clústeres	16
	Configuración del control de acceso de McAfee Security for Microsoft Exchange	17
	Editor de Sitelist	18
	Prueba de la instalación	21
2	Reparación de la instalación	23
3	Desinstalación del software	25
A	Preguntas frecuentes	27
	Índice	29

1

Instalación y configuración

Seleccione la opción para instalar y usar el software MSME, que mejor corresponda a sus requisitos.

Tipo de instalación		Descripción
Independiente	Basada en asistente	Al usar el archivo de instalación basada en asistente, seleccione una de estas opciones según sus requisitos: <ul style="list-style-type: none">• Típica: configurada para todas las funciones estándares, excepto el complemento McAfee Anti-Spam. Puede instalar el complemento McAfee Anti-Spam de manera separada en una etapa posterior.• Completa: configurada para todas las funciones estándares con el complemento McAfee Anti-Spam que proporciona protección contra ataques de spam o phishing.• Personalizada: configure esta opción mediante las opciones avanzadas para personalizar la instalación.
	Silenciosa	Instale el software sin avisos ni interacción del usuario. Modifique y ejecute el archivo <code>Silent.bat</code> , que permite grabar las selecciones para el proceso de instalación.
Administrada por ePolicy Orchestrator		Despliegue MSME en entornos de ePolicy Orchestrator para permitir la administración centralizada de directivas y la implementación en los servidores Microsoft Exchange Server.



También puede desplegar MSME en un clúster de Microsoft Exchange Server. Este despliegue requiere ciertas tareas de configuración después de la instalación.

Véase también

[Despliegue de clústeres](#) en la página 16

Contenido

- ▶ [Preinstalación](#)
- ▶ [Instalación](#)
- ▶ [Configuración posterior a la instalación](#)

Preinstalación



Utilice esta información para preparar la instalación de MSME.

Contenido

- ▶ [Requisitos del sistema](#)
- ▶ [Funciones de Microsoft Exchange Server compatibles](#)
- ▶ [Contenido del paquete](#)

Requisitos del sistema

Asegúrese de que el servidor cumpla con los requisitos.

Componente	Requisito
Sistema operativo	<ul style="list-style-type: none"> • Microsoft Windows 2008 Standard/Enterprise Server SP2 (64 bits) • Microsoft Windows 2008 Standard/Enterprise Server R2 (64 bits) • Microsoft Windows 2012 Standard/Enterprise Server (64 bits) • Microsoft Windows 2012 Standard/Enterprise Server R2 (64 bits) • Microsoft Windows Server 2016 (64 bits)
Microsoft Exchange Server	<ul style="list-style-type: none"> • Microsoft Exchange Server 2010 SP3 • Microsoft Exchange Server 2013 (Actualización acumulativa 12 y posteriores) • Microsoft Exchange Server 2016 (Actualización acumulativa 3 y posteriores)
Navegador	<ul style="list-style-type: none"> • Microsoft Internet Explorer versiones 10.0 y 11.1016 • Mozilla Firefox 54.0.1 • Google Chrome 59.0.3071.115 <p> Asegúrese de desactivar el bloqueador de ventanas emergentes en la configuración del navegador.</p>
Procesador	<ul style="list-style-type: none"> • Procesador de arquitectura básica Intel x64 compatible con la tecnología de memoria ampliada Intel 64 (Intel EM64T) • Procesador de arquitectura básica AMD x64 con tecnología AMD de 64 bits
Memoria	<p> Se requiere la misma cantidad de memoria para instalar MSME que para instalar Microsoft Exchange Server. Para obtener más información, consulte el sitio web de <i>Microsoft Exchange</i>.</p> <p>Microsoft Exchange Server 2010</p> <ul style="list-style-type: none"> • Mínimo: 4 GB de RAM • Recomendado: 4 GB de RAM para una única función y 8 GB para funciones múltiples <p>Microsoft Exchange Server 2013</p> <ul style="list-style-type: none"> • Mínimo: 8 GB de RAM • Recomendado: 8 GB de RAM <p>Microsoft Exchange Server 2016</p> <ul style="list-style-type: none"> • Mínimo: 8 GB de RAM • Recomendado: 8 GB de RAM
Espacio en disco	Mínimo: 740 MB
Red	Tarjeta Ethernet de 10/100/1000 Mbps
Resolución de pantalla	1024 x 768
Software de administración de McAfee	McAfee ePolicy Orchestrator 5.1.x, 5.3.x y 5.9.x
McAfee Agent	McAfee Agent 5.0.5 (número de compilación 658)

Componente	Requisito
Ruta de ampliación	McAfee Security for Microsoft Exchange 8.0 Parche 2 McAfee Security for Microsoft Exchange 8.5 Parche 1
Componentes de IIS	Si desea obtener información sobre los requisitos para los componentes de IIS, consulte KB77319 .



Para conocer los requisitos actualizados del sistema, consulte [KB76903](#).

Funciones de Microsoft Exchange Server compatibles

La instalación de MSME depende de la función seleccionada durante la instalación de Microsoft Exchange Server.

Las funciones son compatibles con diferentes versiones de Microsoft Exchange Server:

- Microsoft Exchange Server 2010:
 - Servidor de transporte perimetral: se ejecuta en el perímetro de un dominio y proporciona higiene y seguridad en los mensajes. Se instala en un servidor independiente que no sea miembro de un dominio de Active Directory.
 - Servidor concentrador: gestiona el flujo de correo dentro de la organización, aplica reglas de transporte y envía mensajes al buzón de cualquier destinatario en un dominio de Active Directory.
 - Servidor de buzón de correo: contiene las bases de datos de Exchange con los buzones de los usuarios.
 - Una instalación con doble función: buzón de correo y concentrador.
- Microsoft Exchange Server 2013, 2013 SP1 y 2016 (Actualización acumulativa 2)
 - MBX Server: posee doble función de buzón de correo y concentrador.
 - Servidor de transporte perimetral. (solo para Microsoft Exchange Server 2013 SP1)

Contenido del paquete

El paquete de software contiene los archivos necesarios para instalar y configurar el software según sea necesario.

Descomprima el archivo `MSMEv86_x64.ZIP` para acceder a estos directorios.

Carpeta	Contenido
Independiente	<p>Contiene los archivos necesarios para realizar una instalación independiente del producto:</p> <ul style="list-style-type: none"> • <code>Setup_x64.exe</code>: archivo para instalar el software mediante un asistente. • <code>Silent.bat</code>: archivo de registro para instalar el software sin avisos ni asistente.
ePO	<p>Contiene los archivos de instalación y configuración necesarios para administrar el producto mediante ePolicy Orchestrator.</p> <ul style="list-style-type: none"> • <code>ePO_Extension_XX</code>: contiene las extensiones del producto para todas las configuraciones regionales en sus carpetas respectivas. Por ejemplo, <code>ePO_Extension_EN</code>. • <code>MSME_Deployment_x64_xxxx.zip</code>: paquete de despliegue para desplegar el software en los clientes gestionados. • <code>MSME_AS_Deployment_xxxx.zip</code>: paquete de despliegue para desplegar el componente McAfee Anti-Spam en los clientes gestionados. • <code>MSMEePOUpgrade.zip</code>: contiene el archivo ejecutable necesario para migrar las directivas de MSME 8.0.2 o 8.5.1 a MSME 8.6 en una ampliación. • <code>MSME86REPORTS.zip</code>: extensión para agregar la interfaz de generación de informes de MSME, como en el caso de los paneles y las consultas. • <code>help_msme_<número_versión>.zip</code>: la extensión de ayuda del producto.
AntiSpam	Contiene <code>ASAddon_x64.exe</code> para instalar el complemento McAfee Anti-Spam.



El instalador de MSME incluye McAfee Agent 5.0.5 (número de compilación 658). El agente recopila y envía información entre el servidor de ePolicy Orchestrator y los repositorios, además de administrar las instalaciones en la red.

Instalación

MSME se instala en un entorno compatible con funciones según la necesidad del usuario.

MSME se puede instalar en un servidor independiente o integrado con ePolicy Orchestrator.



Asimismo, asegúrese de poseer las credenciales de administrador de Windows para instalar el producto. La cuenta deberá ser un administrador de dominio y las credenciales son necesarias para iniciar el instalador del producto.

Véase también

Contenido

- ▶ [Instalación del software mediante el asistente de instalación](#)
- ▶ [Instalación manual del complemento McAfee Anti-Spam](#)
- ▶ [Cómo realizar una instalación silenciosa](#)
- ▶ [Ampliación de un despliegue independiente](#)


Instalación del software mediante el asistente de instalación

Instale el software en un sistema donde esté instalado Microsoft Exchange Server 2010, 2013 o 2016.

En Microsoft Exchange Server 2010, MSME ejecuta el análisis de transporte para las funciones de transporte perimetral y transporte de concentradores, y la API de VirusScan para la función de buzón de correo (según las funciones configuradas).

Procedimiento

- 1 Como administrador, inicie sesión en el sistema en el que está instalado Microsoft Exchange Server.
- 2 Cree un directorio temporal en la unidad local.
- 3 Descargue el paquete de software archivado y extráigalo al directorio temporal creado anteriormente.
- 4 En la carpeta para la instalación, haga doble clic en **setup_x64.exe** (se trata de la aplicación de la instalación para un sistema operativo de 64 bits).
- 5 Seleccione un idioma en la lista desplegable, después haga clic en **Aceptar**.
- 6 En la pantalla **Preparando la instalación**, se prepara el asistente de instalación y se extraen todos los archivos de instalación necesarios. Cuando se completa el proceso, aparece la pantalla **Bienvenido**. Haga clic en **Siguiente**.
- 7 La pantalla **Detección de funciones de Exchange Server** muestra las funciones seleccionadas durante la instalación de Microsoft Exchange Server. Haga clic en **Siguiente**.
- 8 Seleccione un tipo de instalación y, después, haga clic en **Siguiente**.
 - **Típica**: se instalan las funciones de uso general con Configuración del producto basada en web. El complemento McAfee Anti-Spam no se instala.
 - **Completa** (recomendada): se instala la configuración del producto basada en web y el complemento McAfee Anti-Spam. Si el nodo es compatible con clústeres, también se instalan los servicios y los componentes de instalación de clúster necesarios.
 - **Personalizada**: seleccione las funciones de la aplicación que desea instalar y su ubicación de instalación (recomendada solo para usuarios avanzados). Si selecciona este tipo de instalación, un cuadro de diálogo muestra las funciones que se pueden instalar. Para cambiar la carpeta de destino de los archivos de instalación, haga clic en **Cambiar**.
- 9 Acepte los términos del acuerdo de licencia, después haga clic en **Siguiente**.
- 10 En la pantalla **Opciones de configuración adicionales**, complete estas opciones y, después, haga clic en **Siguiente**.
 - a Seleccione **Importar configuración existente** para importar la configuración de MSME desde una instalación existente en el mismo sistema o uno diferente. La configuración se guarda como un archivo .cfg. Para importar dicha configuración, haga clic en **Importar**, navegue al archivo .cfg y después haga clic en **Abrir**.

 Primero debe exportar el archivo de configuración desde la interfaz del producto.
 - b En **Seleccionar mecanismo de cuarentena**, seleccione una ubicación para almacenar los elementos en cuarentena, después complete las opciones de la ubicación seleccionada.
 - c Si selecciona **Base de datos local**, haga clic en **Examinar** para cambiar la ubicación predeterminada (opcional). Si selecciona **McAfee Quarantine Manager**, introduzca la dirección IP del servidor de McAfee

Quarantine Manager, el número de puerto y el número de puerto de devolución de llamada. Asegúrese de que el servidor de McAfee Quarantine Manager esté funcionando y disponible para la cuarentena.

- **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 la conexión de red no está disponible, se interrumpirán 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 McAfee Quarantine Manager 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.
- **HTTTPs:** 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/HTTTPs porque las conexiones sin estado garantizan que el software pueda comunicarse a la perfección con McAfee Quarantine Manager.

d En **Dirección de correo electrónico del administrador**, introduzca la dirección de correo electrónico a la que se enviarán todas las notificaciones, los informes de configuración y los informes de estado.

11 Seleccione un perfil de protección y haga clic en **Siguiente**.

- **Predeterminado:** este perfil proporciona el máximo rendimiento con una protección óptima.
- **Mejorado:** este perfil activa las reglas de filtro de archivo predeterminadas y proporciona una protección máxima. También ofrece protección en tiempo real mediante la reputación de archivos y mensajes de McAfee Global Threat Intelligence.
- **Usar existente** (solamente en ampliación): esta opción utiliza el perfil de protección.

12 Seleccione **Crear accesos directos en el Escritorio** si desea que el asistente de instalación cree accesos directos de la aplicación en el Escritorio. Luego haga clic en **Siguiente**.

13 En la pantalla **Listo para instalar el programa**, verifique la configuración seleccionada y haga clic en **Instalar**. La pantalla **Instalación de McAfee Security for Microsoft Exchange** muestra la funciones que se copian, se inicializan y se instalan.



MSME crea un usuario denominado **MSMEODuser** en Active Directory. Este usuario es necesario para realizar análisis bajo demanda.

14 Cuando finalice la instalación, aparecerá la pantalla **Finalización** en el asistente de instalación. Seleccione las opciones necesarias y, después, haga clic en **Finalizar**.



Puede que se le soliciten las credenciales de administrador de dominio.

- **Iniciar la interfaz de usuario del producto:** inicia la interfaz de usuario independiente de MSME tras salir del asistente de instalación.
- **Mostrar archivo ReadMe:** para ver las Notas de la versión del producto (**Readme.pdf**) con información sobre cualquier adición o cambio de última hora del producto, problemas conocidos o problemas resueltos.
- **Actualizar ahora** (recomendado): actualiza MSME con las últimas actualizaciones de archivos DAT, motores y antispam.

- **Registrarse en McAfee Business Community para mantenerse actualizado:** para recibir información relativa al producto, las nuevas versiones, las actualizaciones y cualquier otra información relevante.
- **Mostrar registros de instalación de Windows:** muestra el archivo de registro del proceso de instalación.



Es recomendable reiniciar el equipo tras la finalización del proceso de instalación.

El software MSME se instaló correctamente en el sistema.

Instalación manual del complemento McAfee Anti-Spam

Si no ha instalado McAfee Anti-Spam durante la instalación personalizada o completa de MSME, instale el complemento manualmente.

Procedimiento

- 1 Como administrador, inicie sesión en el sistema en el que está instalado Microsoft Exchange Server.
- 2 Vaya a la carpeta `\AntiSpam` del paquete de software y haga doble clic en `ASAddOn_x64_Eval.exe`.
- 3 Seleccione un idioma en la lista desplegable, después haga clic en **Aceptar**.
- 4 En la pantalla **Bienvenido**, haga clic en **Siguiente** para ver la pantalla **Acuerdo de licencia de usuario final**.
- 5 Acepte los términos del acuerdo de licencia, después haga clic en **Siguiente**.
- 6 En la pantalla **Listo para instalar el programa**, verifique la configuración seleccionada y haga clic en **Instalar**. Aparece la pantalla **Installing McAfee Anti-Spam add-on for Microsoft Exchange** (Instalación del complemento McAfee Anti-Spam for Microsoft Exchange), que muestra las funciones que se copian, inicializan e instalan.
- 7 Cuando la instalación finalice, aparecerá la pantalla **Finalizada**. Seleccione **Mostrar registros de instalación de Windows** para ver el archivo de registro del proceso de instalación (si es necesario) y haga clic en **Finalizar**.

El complemento McAfee Anti-Spam se ha instalado correctamente en el sistema.

Cómo realizar una instalación silenciosa



Se puede automatizar la instalación mediante el archivo `Silent.bat`, que permite registrar las selecciones para el proceso de instalación.



Para instalar el producto con la configuración predeterminada, haga doble clic en el archivo `Silent.bat`, disponible en el paquete de descarga.



`Silent.bat` se invoca internamente desde el archivo de configuración de MSME. Asegúrese de que `setup_x64.exe` esté disponible en el mismo directorio, ya que la instalación solo se realizará correctamente con `Silent.bat`.

Para personalizar la instalación, modifique estos parámetros en el archivo de proceso por lotes, antes de ejecutarlo:

Parámetro	Valor	Descripción
ADMIN_EMAIL_ID	<admin>@<msme>.com	Especifique la dirección de correo electrónico del administrador para las notificaciones. Por ejemplo, SET ADMIN_EMAIL_ID=admin@msme.com MSME envía notificaciones a esta dirección electrónica cuando se activa la opción Enviar notificación para directivas.
AUTO_UPDATE	1 o 0	Active o desactive las actualizaciones automáticas: <ul style="list-style-type: none"> • 1 = activado • 0 = desactivado Cuando se ha activado, la actualización de archivos DAT y del motor se produce inmediatamente después de la instalación del software. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee recomienda activar la actualización automática para cerciorarse de que los archivos DAT y del motor estén actualizados. </div>
INSTALL_DIR	%SystemDrive%\MSME	Especifique la ruta de instalación. Por ejemplo, si especifica C:\MSME, se creará una carpeta MSME en la unidad de disco C.
NEED_DESKTOP_SHORTCUT	1 o 0	Especifique si se debe crear un acceso directo en el escritorio después de la instalación correcta: <ul style="list-style-type: none"> • 1 = sí • 0 = no El valor predeterminado es 1.
DB_PATH_CHANGED	1 o 0	Especifique si es necesario cambiar la ruta de acceso de la base de datos de Postgres: <ul style="list-style-type: none"> • 1 = sí • 0 = no <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Puede modificar la ruta de acceso a la base de datos en cualquier momento posterior a la instalación. Si se cambia la ruta de acceso, se crea una base de datos para almacenar los elementos detectados. Sin embargo, los elementos detectados y almacenados en la base de datos anterior no estarán disponibles en la nueva base de datos. </div>
DATABASEDIR	<Nueva ubicación de base de datos Postgres>	Especifique la nueva ubicación de la base de datos de Postgres. Por ejemplo, C:\BDdePrueba.

Parámetro	Valor	Descripción
QUARANTINE_MECHANISM	1 o 2	<p>Especifique la ubicación de los elemento en cuarentena:</p> <ul style="list-style-type: none"> • 1 = Base de datos local • 2 = McAfee Quarantine Manager <p>Base de datos local: sirve para poner en cuarentena elementos detectados en el sistema local.</p> <p>Servidor de McAfee Quarantine Manager: sirve para poner en cuarentena elementos detectados en el servidor de MQM, un servidor de almacenamiento centralizado.</p> <p>Si selecciona McAfee Quarantine Manager, asegúrese de definir también las opciones de configuración MQMIPADDRESS, MQMPORTNUMBER y MQM_COMMUNICATION_MECHANISM.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Puede modificar la configuración desde la interfaz del software en cualquier momento posterior a la instalación. </div>
MQMIPADDRESS	Dirección IPv4 o IPv6	Especifique la dirección IP del servidor de MQM. MSME es compatible con los formatos IPv4 e IPv6.
MQM_COMMUNICATION_MECHANISM	0, 1 o 2	<p>Especifique el canal de comunicación para comunicarse con el servidor de MQM:</p> <ul style="list-style-type: none"> • 0 = RPC • {1} HTTP • {2} HTTP <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  McAfee recomienda el uso de un canal de comunicación HTTP/HTTPs porque las conexiones sin estado garantizan que el software se pueda comunicar a la perfección con el servidor de MQM. </div>
MQMPORTNUMBER	80, 443 o 49500	<p>Especifique números de puerto para los canales de comunicación:</p> <ul style="list-style-type: none"> • 80 = protocolo HTTP • 443 = protocolo HTTPs • 49500 = protocolo RPC
AGREE_TO_LICENSE	Sí o No	Acepte los términos de la licencia para instalar el software. Por ejemplo, SET AGREE_TO_LICENSE = sí.



La instalación silenciosa incluye todas las funciones estándar, excepto el complemento McAfee Anti-Spam. El complemento McAfee Anti-Spam se debe instalar por separado. Para obtener detalles, véase *Instalación manual del complemento McAfeeAnti-Spam*.

Ampliación de un despliegue independiente

MSME 8.6 admite la ampliación de la configuración a partir de las versiones anteriores 8.0 Parche 2 y 8.5 Parche 1.

Antes de empezar

Coloque a Microsoft Exchange Server en modo de mantenimiento, ya que la base de datos o los servicios de transporte de Exchange pueden reiniciarse durante el proceso de instalación.

Si había instalado la versión anterior compatible del módulo McAfee Anti-Spam por separado anteriormente, asegúrese de desinstalar el módulo McAfee Anti-Spam antes de actualizar el software. Puede instalar la versión más reciente de McAfee Anti-Spam después de la Ampliación.

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 ampliación. 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](#).

Para ampliar a una nueva versión, no debe desinstalar la versión existente. El programa de instalación actualiza la instalación a la nueva versión.

Procedimiento

- 1 Como administrador, inicie sesión en el sistema en el que está instalado Microsoft Exchange Server.
 - 2 En la carpeta para la instalación, haga doble clic en **setup_x64.exe** (se trata de la aplicación de la instalación para un sistema operativo de 64 bits).
 - 3 En la pantalla **Preparando la instalación**, se prepara el asistente de instalación y se extraen todos los archivos de instalación necesarios. Cuando se completa el proceso, aparece la pantalla **Bienvenido**. Haga clic en **Siguiente**.
 - 4 La pantalla **Detección de funciones de Exchange Server** muestra las funciones seleccionadas durante la instalación de Microsoft Exchange Server. Haga clic en **Siguiente**.
 - 5 En la pantalla **Tipo de instalación**, la opción **Personalizada** está seleccionada de forma predeterminada. Haga clic en **Siguiente**.
 - 6 La pantalla **Instalación personalizada** muestra las funciones instaladas en la instalación existente. Seleccione las funciones que desea actualizar con McAfee Security for Microsoft Exchange y haga clic en **Siguiente**.
 - 7 Acepte los términos del acuerdo de licencia, después haga clic en **Siguiente**.
 - 8 La pantalla **Opciones de configuración adicionales** muestra la configuración del mecanismo de cuarentena y la base de datos de cuarentena aplicada en la instalación existente. Si es necesario, cambie la configuración; después haga clic en **Siguiente**. Para migrar directivas desde una versión anterior, seleccione la opción **Importar configuración existente**. Luego busque el archivo de configuración y selecciónelo.
 - 9 En la pantalla **Perfil de protección de instalación**, seleccione **Predeterminado**, **Mejorado** o **Usar existente** según sea necesario. A continuación, haga clic en **Siguiente**.
-
- Si seleccionó **Importar configuración existente**, todas las selecciones de esta pantalla aparecen inactivas. La opción **Usar existente** está seleccionada de manera predeterminada.
- 10 Seleccione **Crear accesos directos en el Escritorio** si desea que el asistente de instalación cree accesos directos de la aplicación en el Escritorio. Luego haga clic en **Siguiente**.

- 11 En la pantalla **Listo para instalar el programa**, verifique la configuración seleccionada y haga clic en **Instalar**. La pantalla **Instalación de McAfee Security for Microsoft Exchange** muestra las funciones que se copian, se inicializan y se instalan.



Durante la ampliación, el software comprueba la versión de DAT existente en el sistema y se amplía solo si la versión de DAT empaquetada con el software es posterior a la disponible en el sistema.

- 12 Cuando se completa la instalación, aparece la pantalla **Finalizado en el asistente de instalación** con la opción **Migrar datos en cuarentena** seleccionada de manera predeterminada. Haga clic en **Finalizar**.



Si tenía una configuración de proxy en la versión anterior, deberá volver a realizar la configuración de proxy tras la ampliación. Es recomendable reiniciar el equipo tras la instalación.

El software McAfee Security for Microsoft Exchange se amplía correctamente.

Configuración posterior a la instalación

Una vez instalado MSME, realice una configuración adicional determinada según el entorno.

Configuración rápida

Estos son los pasos para establecer la configuración rápida de MSME y para proteger el entorno de Exchange Server.

Como administrador, realice estas tareas una vez instalado MSME en su Exchange Server.

Procedimiento

- 1 Actualice el software con una actualización de motor/DAT. Para obtener detalles, consulte la sección *Programación de una actualización de software*.
- 2 Si ha instalado MSME en un servidor de transporte perimetral o de transporte de concentradores, asegúrese de que los agentes de MSME estén cargados en Exchange Power Shell (Exchange Management Shell), usando el siguiente comando:
`Get-TransportAgent`
El estado de "Activado" debe ser true (verdadero) para los agentes que comienzan con "McAfee".
- 3 Asegúrese de instalar el complemento McAfee Anti-Spam para poner en cuarentena los mensajes de correo electrónico de phishing o spam.
- 4 Actualice la dirección de correo electrónico del administrador desde la ficha **Configuración y diagnósticos | Notificaciones | Configuración**.
- 5 Programe una tarea de informe de estado. Para obtener detalles, consulte la sección *Programación de un nuevo informe de estado*.
- 6 Programe una tarea de informe de configuración. Para obtener detalles, consulte la sección *Programación de un nuevo informe de configuración*.
- 7 Programe análisis bajo demanda según sus necesidades. Para obtener detalles, consulte la sección *Análisis bajo demanda y sus vistas*.
- 8 Configure el análisis en tiempo real según sus necesidades desde la página **Configuración y diagnósticos | Configuración en tiempo real**. Para obtener detalles, consulte la sección *Configuración en tiempo real*.
- 9 Configure el analizador **Conformidad y DLP**, y las reglas según las directivas de su empresa. Para obtener detalles, consulte la sección *Administrador de directivas* para obtener instrucciones sobre la configuración de directivas, analizadores y filtros.

- 10 Para crear excepciones en una directiva, cree directivas secundarias basadas en las necesidades de su organización.
- 11 Envíe mensajes de correo electrónico de prueba para verificar la configuración.

Despliegue de clústeres

Se necesitan configuraciones adicionales para instalar MSME en despliegues de clúster de Microsoft Exchange Server 2010, 2013 y 2016 (Actualización acumulativa 2).

Utilidad de replicación de clústeres para Microsoft Exchange 2010, 2013 y 2016 (Actualización acumulativa 2)

La **utilidad Configuración de replicación de clúster** ayuda a la replicación de la base de datos de cuarentena, configuraciones de directivas, motores y archivos DAT.

Esta utilidad está disponible solamente para la instalación de MSME, reconocida por un *Grupo de disponibilidad de la base de datos* (DAG), en cuyo caso también está disponible el servicio de replicación de MSME. Dependiendo de las opciones de configuración, esta utilidad replica elementos en cuarentena de un servidor a otro, volviéndolos muy accesibles.

El componente principal en un Grupo de disponibilidad de la base de datos se llama Active Manager. Microsoft Exchange Server 2010 se basa en Active Manager para gestionar las conmutaciones y las conmutaciones en caso de error entre los servidores de buzón de correo que forman parte de un Grupo de disponibilidad de la base de datos. Active Manager se ejecuta en todos los servidores de buzón de correo en un Grupo de disponibilidad de la base de datos dado y se puede instalar con dos funciones:

- Primary Active Manager (PAM)
- Standby Active Manager (SAM)

Para obtener detalles sobre dichas funciones, consulte la documentación relevante de Exchange 2010.

Configuración de opciones de replicación

Configure las opciones de replicación para la base de datos de cuarentena, las configuraciones de directivas, los motores y los archivos DAT.

Procedimiento

- 1 En el menú **Inicio**, haga clic en **Todos los programas | McAfee | Security for Microsoft Exchange | Configuración de replicación de clúster**. Aparecerá un cuadro de diálogo con las distintas opciones que se deben definir para este servicio.



Si la función Buzón de correo está instalada en Microsoft Exchange Server 2010, 2013 o 2016, el servicio **Configuración de replicación de clúster** se instala automáticamente en los tres tipos de instalación: Típica, Completa y Personalizada.

- 2 En **Nombre de servidor**, recupere los servidores de replicación disponibles que formen parte del Grupo de disponibilidad de la base de datos y tengan MSME instalado con Exchange Server en la función de buzón de correo.
 - **Servidores disponibles** presenta una lista de servidores que se pueden añadir para replicar la base de datos de cuarentena, las configuraciones de directivas, los motores y los archivos DAT.
 - **Servidores de replicación** presenta una lista de servidores que se han configurado como servidores de replicación para la base de datos de cuarentena, las configuraciones de directivas, los motores y los archivos DAT.
- 3 Seleccione el servidor en **Servidores disponibles** y haga clic en >> para añadirlo a la lista Servidores de replicación.

- 4 Seleccione **Detener servicio de replicación** para detener el servicio de replicación de clústeres de MSME.
- 5 Seleccione **Iniciar Servicio de replicación para** a fin de administrar el servicio de replicación de clústeres de MSME. Seleccione las opciones adecuadas:
 - **Configuración de directivas**
 - **Motor/DAT**
 - **Base de datos de cuarentena**
- 6 Haga clic en **Aplicar** para guardar y aplicar las configuraciones de la replicación de clúster.
- 7 Cuando se le solicite, seleccione la opción para reiniciar el servicio de MSME, necesario para el funcionamiento de la replicación.

Configuración del control de acceso de McAfee Security for Microsoft Exchange

Permitir o denegar el acceso a la interfaz de usuario de MSME para usuarios o grupos específicos.

Procedimiento

- 1 En el menú **Inicio**, haga clic en **Programas | McAfee | Security for Microsoft Exchange | Control de acceso**. Aparecerá el cuadro de diálogo **Permisos de acceso**.

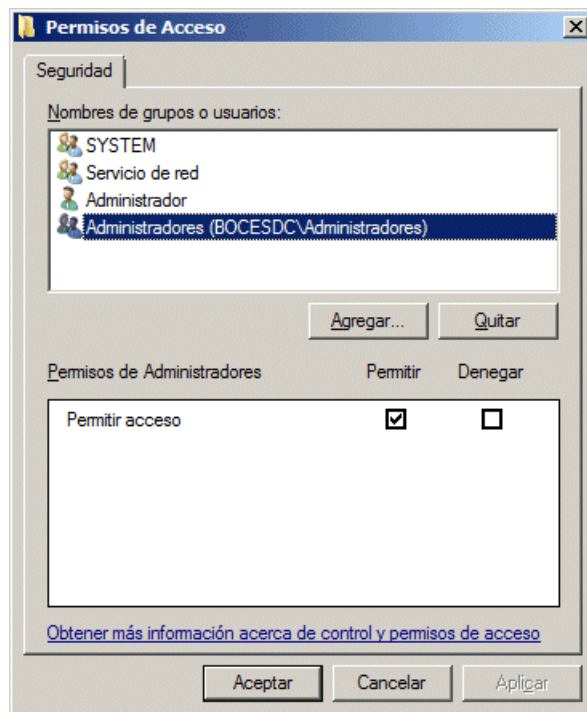


Figura 1-1 Permisos de acceso

- 2 En **Nombres de grupos o usuarios**, seleccione el usuario al que quiere permitir o denegar el acceso a la interfaz de usuario de MSME.
- 3 Haga clic en **Aceptar**.

Editor de Sitelist

La **lista Sitelist** especifica la ubicación desde la que se descargan las actualizaciones automáticas (incluidos motores de análisis y archivo DAT).

Acceso al editor de SiteList

- En el menú **Inicio**, haga clic en **Programas | McAfee | Security for Microsoft Exchange | Editor de SiteList**.

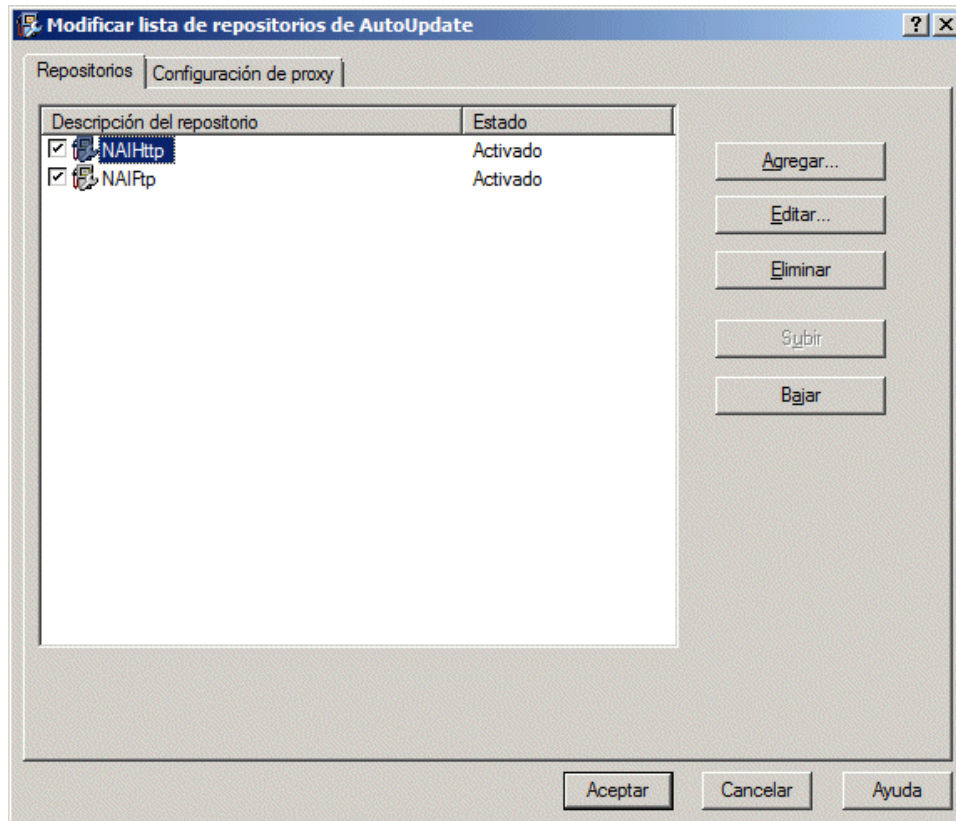


Figura 1-2 Editar la lista de repositorios de AutoUpdate

Puede utilizar las siguientes fichas:

- **Repositorios:** para configurar las opciones del repositorio desde donde se pueden descargar actualizaciones automáticas de MSME.
De forma predeterminada, MSME utiliza una Sitelist que lleva a un sitio de McAfee para actualizaciones automáticas, pero puede usar listas de sitios que lleven a una ubicación distinta. Por ejemplo, es posible que haya copiado las actualizaciones automáticas en un repositorio local y creado una Sitelist que lleve los sistemas MSME a ese repositorio local.
- **Configuración de proxy:** para configurar las opciones del servidor proxy, de manera tal que MSME se pueda conectar a internet mediante dicho servidor y pueda descargar actualizaciones de manera automática.



Las configuraciones aplicadas en el editor de SiteList se guardan en el archivo `SiteList.xml` en el directorio `C:\ProgramData\McAfee\Common FrameWork\`.

Configuración del repositorio de Sitelist

En **Sitelist** se especifica desde dónde se descargan las actualizaciones automáticas.

De manera predeterminada, McAfee Security for Microsoft Exchange usa una Sitelist que dirige un sitio de McAfee a las actualizaciones automáticas, pero se puede usar una lista Sitelist que dirija a una ubicación diferente. Por ejemplo, puede copiar las actualizaciones automáticas en un repositorio local y crear una Sitelist que dirija los sistemas de McAfee Security for Microsoft Exchange al repositorio local.

Procedimiento

- 1 Haga clic en **Inicio | Programas | McAfee | Security for Microsoft Exchange | Editor de Sitelist**. Aparecerá el cuadro de diálogo **Editar la lista de repositorios de AutoUpdate**.
- 2 En la ficha **Repositorios**, haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Configuración del repositorio**.

Figura 1-3 Configuración del repositorio

- 3 Seleccione entre las siguientes opciones:
 - **Descripción del repositorio:** describe brevemente el repositorio.
 - **Recuperar archivos desde:** especifica de qué tipo de repositorio recuperar los archivos. Las opciones disponibles son **Repositorio HTTP**, **Repositorio FTP**, **Ruta de recurso UNC** y **Ruta local**.
 - **URL:** especifica la URL del repositorio.
 - **Puerto:** especifica el número de puerto del repositorio.
 - **Usar autenticación:** permite a la autenticación del usuario acceder al repositorio.
- 4 Especifique un nombre de usuario y una contraseña para la autenticación del repositorio y confirme la contraseña volviéndola a introducir.
- 5 Haga clic en **Aceptar** para agregar el nuevo repositorio a la lista **Descripción del repositorio**.
- 6 Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Editar la lista de repositorios de AutoUpdate**.

Configuración de proxy de Sitelist

Permite configurar dichas opciones si la organización utiliza un servidor proxy para conectarse a Internet, para que MSME descargue las actualizaciones del producto.

Si su organización usa servidores proxy para conectarse a Internet, puede seleccionar la opción **Configuración de proxy**.

Procedimiento

1 Haga clic en **Inicio | Programas | McAfee | Security for Microsoft Exchange | Editor de Sitelist**.

Aparecerá el cuadro de diálogo **Editar la lista de repositorios de AutoUpdate**.

2 Haga clic en la ficha **Configuración de proxy**.

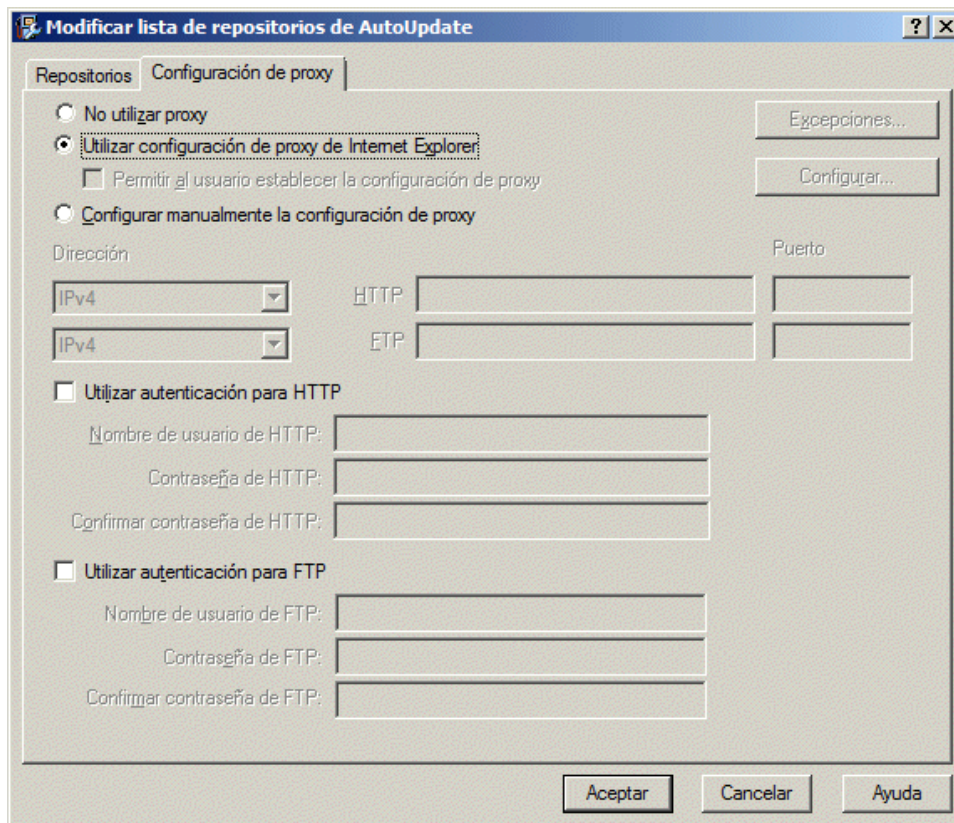


Figura 1-4 Configuración de proxy

3 Seleccione la opción **Usar configuración de proxy de Internet Explorer** o **Configurar el servidor proxy de forma manual** según sea necesario.

4 Introduzca la dirección IP y el número de puerto del servidor HTTP o FTP.

5 Puede usar las siguientes opciones:

- **Usar autenticación:** permite a la autenticación del usuario acceder al servidor proxy.
- **Nombre de usuario:** permite especificar un nombre de usuario para que la autenticación tenga acceso al servidor proxy.
- **Contraseña:** permite especificar una contraseña.

- **Confirmar contraseña:** permite volver a confirmar la contraseña especificada.
 - **Excepciones:** permite omitir un servidor proxy para los dominios específicos. Haga clic en **Excepciones**, después seleccione **Especificar excepciones** e introduzca el dominio que se debe omitir.
- 6 Haga clic en **Aceptar**.

Prueba de la instalación

Cuando se ha completado la instalación de MSME, se recomienda realizar una prueba.

El propósito es asegurarse de que el software está instalado correctamente y puede detectar virus y spam en correos electrónicos.

Procedimientos

- *Prueba del componente antivirus en la página 22*
Adjunte el archivo de prueba antivirus EICAR a un mensaje de correo electrónico y envíe el mensaje mediante Microsoft Exchange Server en el que instaló MSME.
- *Prueba del componente antispam en la página 22*
Ejecute el correo electrónico de prueba general para correo masivo no solicitado (GTUBE) para probar el software McAfee Anti-Spam.
- *Pruebe la instalación mediante McAfee Virtual Technician en la página 22*
McAfee Virtual Technician comprueba automáticamente si se han producido desviaciones normales desde la instalación del producto.

Componentes y servicios instalados

MSME instala diversos componentes en Microsoft Exchange Server.

Para tener acceso a un componente de MSME, haga clic en **Iniciar** | **Programas** | **McAfee** | **Security for Microsoft Exchange** y haga clic en el componente:

- **McAfee Anti-Spam for McAfee Security for Microsoft Exchange:** detecta contenidos de spam y phishing.
- **Control de acceso:** permite o deniega el acceso a la interfaz de usuario de MSME a usuarios o grupos específicos.
- **Configuración del producto:** inicia la versión independiente de MSME o se inicia por medio de una interfaz web.
- **Editor de Sitelist:** especifica la ubicación desde la que se descargan las actualizaciones automáticas (archivos DAT y motores de análisis inclusive).
- **Configuración de replicación de clúster:** replica la base de datos de cuarentena, las configuraciones de directivas y las actualizaciones de productos; solo para Microsoft Exchange Server 2010, 2013 y 2016 (Actualización acumulativa 2). Esto depende de que la configuración de replicación de un **Grupo de disponibilidad de la base de datos** (DAG), sea reconocida por una instalación de MSME.

Servicios disponibles

- **Servicio McAfee Agent, Servicios comunes de McAfee Agent y Servicio de compatibilidad con versiones anteriores de McAfee Agent:** son un requisito previo para instalar y utilizar McAfee ePO. Para obtener más detalles sobre este servicio, véase la documentación del producto correspondiente a McAfee ePO.
- **McAfee Security for Microsoft Exchange:** protege Microsoft Exchange Server versiones 2010, 2013 y 2016 (Actualización acumulativa 2) contra virus, contenido no deseado, programas potencialmente no deseados y tipos de archivos o mensajes prohibidos.
- **Actualizador de reglas antispam de McAfee:** necesario para actualizar las reglas antispam.

Prueba del componente antivirus

Adjunte el archivo de prueba antivirus EICAR a un mensaje de correo electrónico y envíe el mensaje mediante Microsoft Exchange Server en el que instaló MSME.

El archivo de prueba antivirus estándar EICAR fue creado por un conjunto de proveedores de antivirus de todo el mundo. Es un estándar para comprobar las instalaciones antivirus.



Este archivo no es un virus. Asegúrese de eliminar el archivo cuando haya terminado de probar la instalación, a fin de no alarmar a los usuarios.

Procedimiento

- 1 Abra un editor de texto, copie el siguiente código y guarde el archivo con el nombre `EICAR.COM`:

```
X5O!P%@AP[4\PZX54(P^7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

El tamaño del archivo es 68 o 70 bytes.

- 2 Envíe un correo electrónico por medio de Microsoft Exchange Server con el archivo de prueba EICAR adjunto.



Cuando MSME examine el mensaje de correo electrónico, informará haber detectado el archivo de prueba EICAR. Sin embargo, no podrá limpiarlo ni repararlo porque es un archivo de prueba.

- 3 MSME reemplaza el archivo de prueba EICAR con un mensaje de alerta.

Prueba del componente antispam

Ejecute el correo electrónico de prueba general para correo masivo no solicitado (GTUBE) para probar el software McAfee Anti-Spam.

El mensaje de prueba debe enviarse desde una cuenta de correo electrónico externa (un dominio diferente).

Procedimiento

- 1 Genere un mensaje de correo electrónico.
- 2 Copie el siguiente código en el texto del cuerpo:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Asegúrese de copiarlo sin espacios adicionales ni saltos de línea.

- 3 Envíe este mensaje desde una dirección externa de correo electrónico a un buzón de correo del servidor donde se haya instalado MSME con el complemento McAfee Anti-Spam. McAfee Anti-Spam analiza el mensaje, lo identifica como correo basura y actúa en consecuencia.



La prueba GTUBE omite las listas negras y blancas. Para obtener más información sobre el archivo de prueba GTUBE, visite <http://spamassassin.apache.org/>.

Pruebe la instalación mediante McAfee Virtual Technician

McAfee Virtual Technician comprueba automáticamente si se han producido desviaciones normales desde la instalación del producto.

Ejecute McAfee Virtual Technician para probar si MSME se ha instalado correctamente.

Para descargar McAfee Virtual Technician visite: <http://mvt.mcafee.com/mvt/index.asp>.

2

Reparación de la instalación

Permite reparar errores de instalación en el programa. Esta opción repara archivos dañados o que falten, accesos directos y entradas del registro.



También puede reparar la instalación de MSME desde **Panel de control | Programas y características | Desinstalar un programa** mediante un clic en **Desinstalar/Cambiar**. Al reparar la instalación la configuración vuelve a sus valores predeterminados.

Procedimiento

- 1 En la carpeta que contiene los archivos de instalación, haga doble clic en `setup_x64.exe`.
- 2 Haga clic en **Siguiente**. Aparece la pantalla **Mantenimiento del programa**.
- 3 En la pantalla **Mantenimiento del programa**, seleccione **Reparar** y haga clic en **Siguiente**. Aparece la pantalla **Listo para reparar el programa**.
- 4 Haga clic en **Instalar** para finalizar la reparación. Aparece el cuadro de diálogo **Finalizado el Asistente InstallShield**.
- 5 Haga clic en **Finalizar** para salir.

3

Desinstalación del software

Elimine o desinstale MSME de Exchange Server.



También es posible eliminar MSME desde la consola de **Panel de control | Programas y características | Desinstalar un programa**. Con este método, la base de datos de cuarentena se conserva de manera predeterminada.

Procedimiento

- 1 En la carpeta que contiene los archivos de instalación, haga doble clic en `setup_x64.exe`.
Aparece la pantalla **Bienvenido**.
- 2 Haga clic en **Siguiente**.
Aparece la pantalla **Mantenimiento del programa**.
- 3 Seleccione **Eliminar** y haga clic en **Siguiente**.
Aparece la pantalla **Mantener configuración**.
- 4 Seleccione **Conservar base de datos de cuarentena** para conservar la base de datos de cuarentena y haga clic en **Siguiente**.
Aparece la pantalla **Eliminar el programa**.
- 5 Haga clic en **Eliminar** para desinstalar MSME de Exchange Server.
Aparece la pantalla **Finalizado el Asistente InstallShield**.
- 6 Haga clic en **Finalizar** para salir.

A

Preguntas frecuentes

A continuación, se presentan respuestas a las preguntas frecuentes sobre la instalación de MSME.

¿Cómo se realiza la instalación silenciosa?

Ejecute el archivo `Silent.bat` del paquete de descarga. Para obtener información sobre la personalización, consulte *Cómo realizar una instalación silenciosa*.

¿Puedo instalar McAfee Security for Microsoft Exchange 8.6 con una cuenta que no sea de administrador de dominio?

Sí, se puede instalar. Para obtener más información, consulte el artículo de la base de conocimiento de McAfee [KB82190](#).

¿Cuál es la versión admitida de ePolicy Orchestrator?

McAfee ePolicy Orchestrator 5.1.x, 5.3.x y 5.9.x.

¿Cuál es la versión admitida de McAfee Agent?

McAfee Agent 5.0.5 compilación 658.

¿En qué puerto funciona la replicación de configuración de MSME?

Este servicio no funciona en los puertos, pero supervisa las carpetas configuradas por el administrador que usa la interfaz de usuario de replicación.

¿Debo tener en cuenta algo especial a la hora de ampliar a MSME 8.6 desde MSME 8.0 Parche 2 o 8.5 Parche 1 en el entorno de DAG?

No hay que tener nada en cuenta. Siga los pasos de la instalación autónoma.

Índice

A

- acceder
 - Editor de Sitelist [18](#)
- antispam, componente [22](#)
- antivirus, componente [22](#)
- archivo de prueba EICAR [22](#)
- archivos de configuración [21](#)

C

- componentes adicionales [21](#)
- componentes instalados [21](#)
- configuración
 - rápida [15](#)
- configuración de proxy
 - configuración de Sitelist [20](#)
- configuración de repositorio
 - configuración de Sitelist [19](#)
- configuración rápida [15](#)
- configurar
 - configuración de proxy de Sitelist [20](#)
 - configuración de repositorio de Sitelist [19](#)
 - control de acceso [17](#)
- contenido del paquete [7](#)
- contenido, paquete [7](#)
- control de acceso
 - configuración [17](#)

D

- desinstalar [25](#)

E

- Editor de Sitelist
 - acceso [18](#)
 - configuración de proxy [18](#)
 - repositorio [18](#)
- eliminar [25](#)
- Exchange Server
 - funciones admitidas [7](#)

F

- funciones compatibles
 - Exchange Server [7](#)

G

- GTUBE, archivo de prueba [22](#)

I

- instalación
 - uso del asistente [8](#)
- instalación silenciosa [11](#)
- instalación, prueba [22](#)
- instalar
 - P+F [27](#)
 - reparación [23](#)

M

- McAfee Virtual Technician [22](#)

P

- P+F
 - instalar [27](#)
- preinstalación [5](#)

R

- reparar
 - instalación [23](#)
- requisitos
 - sistema [6](#)

S

- servicios [21](#)
- sistema
 - requisitos [6](#)
- software
 - ampliación [14](#)
 - desinstalar el [25](#)
 - eliminar el [25](#)

