ESET Mail Security

Guía para el usuario

Haga clic aquí para mostrar la versión de ayuda de este documento

Digital Security
Progress. Protected.

Copyright ©2024 de ESET, spol. s r.o.

ESET Mail Security ha sido desarrollado por ESET, spol. s r.o.

Para obtener más información, visite https://www.eset.com.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de la aplicación sin previo aviso.

Soporte técnico: https://support.eset.com

REV. 26/03/2024

1 Información general ... 1
1.1 Características principales ... 1
1.2 Novedades ... 3
1.3 Flujo de correos ... 4
1.4 ESET Mail Security Características y roles de Exchange Server ... 5
1.5 Roles de Exchange Server ... 6
1.6 Módulos de protección ... 6
1.7 Seguridad multicapa ... 7
1.7 Protección de la base de datos de correo electrónico ... 8
1.7 Protección del transporte de correo electrónico ... 8
1.7 Exploración de la base de datos del buzón de correo a petición ... 9
1.7 La exploración de base de datos del buzón de Microsoft 365 ... 10
2 Requisitos del sistema ... 11
3 Preparar para la instalación ... 12
3.1 Pasos para la instalación de ESET Mail Security ... 14
3.1 Exportar configuración o eliminar instalación ... 17
3.1 Actualización de módulos iniciales ... 18
3.2 Instalación silenciosa/sin supervisión ... 19
3.2 Instalación de la línea de comandos ... 20
3.3 Activación de producto ... 23
3.3 La activación se completó correctamente ... 25
3.3 Cuenta de ESET HUB ... 25
3.3 Falla en la activación ... 25
3.3 Licencia ... 26
3.4 Actualizando a la versión más reciente. ... 26
3.4 Actualización mediante ESET PROTECT ... 27
3.4 Actualización mediante el clúster de ESET ... 28
3.5 Instalación en un entorno de clúster ... 31
3.6 Terminal Server ... 31
3.7 Multiservidor/entorno DAG ... 31
4 Primeros pasos ... 32
4.1 Tareas posteriores a la instalación ... 32
4.2 Administrado a través de ESET PROTECT ... 33
4.3 Supervisión ... 34
4.3 Actualización de Windows disponible ... 36
4.3 Aislamiento de red ... 36
5 Uso de ESET Mail Security ... 38
5.1 Exploración ... 38
5.1 Ventana de exploración y registro de exploración ... 40
5.2 Archivos de registro ... 43
5.2 Filtrado de registros ... 46
5.3 Actualización ... 48
5.4 Cuarentena de correo ... 50
5.5 Configuración ... 53
5.5 Servidor ... 54
5.5 Equipo ... 56
5.5 Red ... 57
5.5 Asistente para la resolución de problemas de red ... 58
5.5 Web y correo electrónico ... 59
5.5 Herramientas - Registro de diagnósticos ... 59

5.5 Importar y exportar una configuración ... 60
5.6 Herramientas ... 61
5.6 Procesos activos ... 62
5.6 Estadísticas de la protección ... 64
5.6 Clúster ... 66
5.6 Asistente del clúster - Seleccionar nodos ... 68
5.6 Asistente del clúster - Configuración del clúster ... 69
5.6 Asistente del clúster - Configuración de instalación de clúster ... 70
5.6 Asistente del clúster - Verificación de nodos ... 70
5.6 Asistente del clúster - Instalación de nodos ... 72
5.6 Shell de ESET ... 74
5.6 Uso ... 76
5.6 Comandos ... 81
5.6 Accesos directos de teclado ... 84
5.6 Archivos por lotes/ Cifrado ... 85
5.6 ESET LiveGuard Advanced ... 86
5.6 ESET SysInspector ... 87
5.6 ESET SysRescue Live ... 88
5.6 Tareas programadas ... 89
5.6 Tareas programadas: Agregar tarea ... 90
5.6 Tipo de tarea ... 93
5.6 Ejecución de la tarea ... 94
5.6 Cuando se cumpla la condición ... 94
5.6 Ejecutar aplicación ... 95
5.6 Pasar por alto tarea ... 95
5.6 Informe de protección del servidor de correo electrónico ... 95
5.6 Resumen general de tareas programadas ... 96
5.6 Enviar muestras para su análisis ... 96
5.6 Archivo sospechoso ... 97
5.6 Sitio sospechoso ... 98
5.6 Archivo falso positivo ... 98
5.6 Sitio falso positivo ... 99
5.6 Otro ... 99
5.6 Cuarentena ... 99
5.7 Asistente de exploración del buzón de Microsoft 365 ... 101
5.7 Registrar explorador ESET Mail Security ... 102
5.7 Eliminar el registro del explorador ESET Mail Security ... 105
6 Configuración de protección para servidores ... 107
6.1 Configuración de la prioridad del agente ... 108
6.2 Antivirus y antispyware ... 109
6.3 Protección antispam ... 110
6.3 Filtro y verificación ... 111
6.3 Configuración avanzada de antispam ... 114
6.3 Configuración de la lista gris ... 118
6.3 SPF y DKIM ... 119
6.3 Protección contra retrodispersión ... 121
6.3 Protección contra la suplantación de identidad del remitente ... 122
6.4 Protección antiphishing ... 124
6.5 Reglas ... 125
6.5 Condición de regla ... 128
6.5 Acción de regla ... 134

6.5 Ejemplos de reglas 137
6.6 Protección del transporte de correo electrónico 139
6.6 Configuración avanzada de transporte de correo 142
6.7 Protección de la base de datos de correo electrónico 143
6.7 Exploración en segundo plano 145
6.8 Exploración de la base de datos del buzón de correo a petición 146
6.8 Exploración de la base de datos del buzón 148
6.8 Exploración del buzón de Microsoft 365 150
6.8 Elementos adicionales del buzón de correo 151
6.8 Servidor proxy 152
6.8 Detalles de la cuenta de la exploración de la base de datos 152
6.9 Tipos de cuarentena de correo 154
6.9 Cuarentena local 155
6.9 Almacenamiento de archivos 156
6.9 Interfaz Web 156
6.9 Enviar informes de cuarentena de correo - tarea programada 162
6.9 Interfaz web de la Cuarentena de correos del usuario 163
6.9 Buzón de correo de cuarentena y cuarentena de MS Exchange 165
6.9 Configuración de la administración de cuarentena 166
6.9 Servidor proxy 167
6.9 Detalles de la cuenta del administrador de la cuarentena 167
6.10 Firma DKIM 168
6.11 Prueba Antivirus 170
6.12 Prueba antispam 170
6.13 Prueba anti-phishing 170
7 Configuración general 170
7.1 Computer 171
7.1 Detección de aprendizaje automático 173
7.1 Exclusiones 177
7.1 Exclusiones de rendimiento 178
7.1 Exclusiones de detección 179
7.1 Crear asistente de exclusión 181
7.1 Opciones avanzadas 181
7.1 Exclusiones automáticas 181
7.1 Detección de una infiltración 183
7.1 Protección del sistema de archivos en tiempo real 184
7.1 ThreatSense parámetros 185
7.1 Parámetros ThreatSense adicionales 189
7.1 Extensiones de archivos que no se analizarán 190
7.1 Exclusiones de procesos 190
7.1 Protección basada en la nube 191
7.1 Filtro de exclusión 193
7.1 Exploración de malware 194
7.1 Administrador de perfiles 194
7.1 Objetos de perfil 195
7.1 Objetos para explorar 197
7.1 Exploración en estado inactivo 199
7.1 Exploración en el inicio 199
7.1 Verificación de archivos de inicio automática 200
7.1 Medios extraíbles 201
7.1 Protección de documentos 202

7.1 Exploración Hyper-V 202
7.1 HIPS 205
7.1 Configuraciones de reglas HIPS 207
7.1 Configuración avanzada de HIPS 210
7.2 Actualizar configuración 210
7.2 Revertir actualización 214
7.2 Tarea programada - actualización 215
7.2 Actualizar reflejo 215
7.3 Protección de la red 217
7.3 Redes conocidas 217
7.3 Agregar red 218
7.3 Zonas 220
7.4 Protección contra ataques en la red 221
7.4 Excepciones de IDS 222
7.4 Sospecha de amenaza bloqueada 223
7.4 Lista negra temporal de direcciones IP 223
7.4 Protección contra ataques por fuerza bruta 224
7.4 Reglas de protección contra ataques por fuerza bruta 224
7.4 Exclusiones de protección contra ataques por fuerza bruta 224
7.5 Web y correo electrónico 225
7.5 Filtrado de protocolos 225
7.5 Clientes de Internet y correo electrónico 226
7.5 SSL/TLS 226
7.5 Lista de certificados conocidos 228
7.5 Comunicación cifrada SSL 228
7.5 Protección del cliente de correo electrónico 229
7.5 Protocolos de correo electrónico 231
7.5 Etiquetas de correo electrónico 231
7.5 Barra de herramientas de Microsoft Outlook 232
7.5 Barra de herramientas de Outlook Express y Windows Mail 232
7.5 Cuadro de diálogo de confirmación 233
7.5 Exploración reiterada de los mensajes 233
7.5 Protección del acceso a la Web 233
7.5 Administración de direcciones URL 234
7.5 Creación de una nueva lista 235
7.5 Protección web Anti-Phishing 237
7.6 Control de dispositivos 238
7.6 Reglas del dispositivo 238
7.6 Grupos de dispositivos 241
7.7 Configuración de herramientas 242
7.7 Intervalos de tiempo 243
7.7 Actualización de Microsoft Windows 243
7.7 Explorador de la línea de comandos 244
7.7 ESET CMD 246
7.7 ESET RMM 247
7.7 Licencia 249
7.7 Proveedor WMI 249
7.7 Datos proporcionados 249
7.7 Acceso a los datos proporcionados 259
7.7 Destinos de las exploraciones de la consola de administración de ESET 260
7.7 Modo de anulación 260

7.7 Archivos de registro 263
7.7 Asignación de eventos en Syslog 266
7.7 Servidor proxy 268
7.7 Modo de presentación 269
7.7 Diagnósticos 269
7.7 Soporte técnico 270
7.7 Clúster 271
7.8 Interfaz de usuario 272
7.8 Configuración del acceso 273
7.8 Shell de ESET 274
7.8 Deshabilitación de la interfaz gráfica del usuario en Terminal Server 275
7.8 Ícono en el área de notificación de Windows 275
7.9 Notificaciones 276
7.9 Estados de la aplicación 276
7.9 Mensajes y estados deshabilitados 277
7.9 Notificaciones en el escritorio 277
7.9 Personalización 278
7.9 Notificaciones en el escritorio 279
7.9 Alertas interactivas 279
7.9 Reenvío 280
7.10 Revertir a la configuración predeterminada 282
7.11 Ayuda y soporte 283
7.11 Enviar una solicitud de soporte 284
7.11 Acerca de ESET Mail Security 284
7.12 Glosario 284
8 Acuerdo de licencia de usuario final 285
9 Política de privacidad 292

Información general

ESET Mail Security para Microsoft Exchange Server es una solución integrada que protege los servidores de correo y los buzones de correo de usuarios frente a diversos tipos de contenido malicioso. Incluye archivos adjuntos de correo electrónico infectados por gusanos o troyanos, documentos que contienen scripts dañinos, phishing, spam, falsificación de remitentes y suplantación de correo electrónico.

ESET Mail Security ofrece cuatro tipos de protección: Antivirus, Antispam, Antiphishing y Reglas. ESET Mail Security filtra contenido malicioso en las bases de datos del buzón de coreo así como también en la capa de transporte de correo antes de que llegue al buzón de correo del destinatario.

ESET Mail Security es compatible con la versión 2010 de Microsoft Exchange Server y versiones posteriores, además de Microsoft Exchange Server en un entorno de clúster. Los roles específicos (buzón de correo, concentradores, perimetral) también son compatibles.

A la vez que proporciona protección para Microsoft Exchange Server, ESET Mail Security también incluye funciones para asegurar la protección del servidor en sí mismo (protección del sistema de archivos en tiempo real, protección de red, protección de acceso a la Web y protección del cliente de correo electrónico).

En redes más grandes, es posible administrar ESET Mail Security en forma remota con la ayuda de ESET PROTECT. También, ESET Mail Security le permite usarlo con herramientas de monitorización y administración remota (RMM) de terceros.

Características principales

La siguiente tabla contiene una lista de funciones disponibles en ESET Mail Security.

Producto de 64 bits nativo	Agrega mayor desempeño y estabilidad a los componentes de productos nativos.
Anti-Malware	Una defensa innovadora y galardonada contra el malware. Esta tecnología de punta previene ataques y elimina todos los tipos de amenazas, incluidos los virus, ransomware, rootkits, gusanos y spyware con un análisis impulsado por la nube para mejores tasas de detección. Con una pequeña huella, es ligero en los recursos del sistema y no compromete su rendimiento. Utiliza un modelo de seguridad por capas. Cada capa, o fase, tiene un número de tecnologías núcleo. La fase de Pre-ejecución tiene tecnologías como el explorador UEFI, la Protección contra ataques en la red, Reputación y Caché, producto Sandbox, Detecciones DNA. Las tecnologías en la fase de Ejecución son el bloqueador de exploits, la protección ransomware, la exploración de Memoria avanzada y el explorador en script (AMSI), y la fase de Post-ejecución usa la protección contra botnets, el sistema de protección contra el malware en la nube y Sandboxing. Este conjunto completo de tecnologías núcleo proporciona un nivel de protección inigualable.

Antispam	El Antispam es un componente esencial para cualquier servidor de correo. ESET Mail Security usa un motor antispam de avanzada que previene intentos de spam y phishing con tasas muy altas de captura. ESET Mail Security ha ganado consecutivamente la evaluación de filtro de spam por Virus Bulletin, una autoridad examinadora de seguridad líder, y ha recibido la certificación VBSpam+ por varios años. El motor antispam ha alcanzado un resultado de una tasa de captura de spam del 99,99% con cero falsos positivos, lo que lo convierte en la tecnología líder de la industria en la protección contra el spam. ESET Mail Security La protección antispam incorpora múltiples tecnologías (tales como RBL, DNSBL, huellas digitales, verificación de reputación, análisis de contenido, Reglas, creación manual de listas blancas y negras, Protección contra retrodispersión y validación de mensaje mediante SPF and DKIM) para maximizar la detección. ESET Mail Security El antispam se basa en la nube y la mayoría de las bases de datos en la nube están ubicadas en los centros de datos de ESET. Los servicios antispam en la nube permiten actualizaciones rápidas de datos que proporcionan un tiempo de reacción más rápido en caso de aparición de un nuevo spam.
Protección antiphishing	Característica que evita que los usuarios accedan a páginas web conocidas por phishing. Mensajes de correo electrónico que pudieran contener enlaces que conducen a páginas web con phishing, ESET Mail Security usa un analizador que busca en el cuerpo del mensaje y asunto de los mensajes de correo electrónico entrantes para identificar dichos vínculos (URL). Los vínculos se comparan contra la base de datos de phishing.
Reglas	Las reglas permiten que los administrador filtren correos electrónicos no deseados y archivos adjuntos basado en la política de la compañía. Los archivos adjuntos como los ejecutables, archivos multimedia, archivos protegidos con contraseña, etc. Se pueden realizar diferentes acciones con los mensajes de correo electrónico filtrados y sus archivos adjuntos, como cuarentena, eliminación, envío de notificaciones o registro de eventos.
Exportar a servidor syslog (Arcsight)	Permite que los contenidos del Registro de protección del servidor de correo se dupliquen en el servidor syslog en Formato de Evento Común (CEF) para su uso con soluciones de gestión de registros, como Micro Focus ArcSight. Los eventos pueden suministrarse a través de SmartConnector a ArcSight, o bien, exportarse a archivos. De esta manera, se ofrece una manera práctica de monitorear y administrar los eventos de seguridad en forma centralizada. Puede beneficiarse a partir de esta función en particular si cuenta con una infraestructura compleja compuesta por una gran cantidad de Microsoft Exchange Servers con la solución ESET Mail Security.
Exploración del buzón de Microsoft 365	Para los negocios que utilizan un entorno híbrido de Excange, aporta la capacidad de explorar buzones de correo en la nube.
ESET LiveGuard Advanced	Servicio basado en nube ESET. Cuando ESET Mail Security evalúa que un mensaje de correo electrónico es sospechoso, se pone temporalmente en ESET LiveGuard Advanced cuarentena. Un mensaje de correo electrónico sospecho se envía automáticamente a ESET LiveGuard Advanced servidor para un análisis por los motores de detección de malware avanzados. ESET Mail Security luego recibe un resulto del análisis y el mensaje de correo electrónico sospechoso se trata según el resultado.
Administrador de la cuarentena de correo con interfaz web	El administrador puede inspeccionar objetos en cuarentena y decidir si los eliminará o los liberará. Esta función ofrece una herramienta de administración fácil de usar. La interfaz web de cuarentena permite una administración remota del contenido. Es posible elegir sus administrador y/o acceso delegado. Además, los usuarios pueden ver y administrar su propio spam después de iniciar sesión en la interfaz de la Web de cuarentena de correo, con acceso a los mensajes solamente.
Informes de la cuarentena del correo	Los informes de cuarentena son correos electrónicos enviados a usuarios o administradores seleccionados para proporcionar información sobre los mensajes de correo electrónico en cuarentena. También les permite administrar de manera remota el contenido en cuarentena.

Exploración de la base de datos del buzón de correo a petición	La exploración de la base de datos del buzón de correo a petición otorga a los administradores una opción para explorar buzones de correo seleccionados manualmente, o programar la exploración fuera del horario de operación. El explorador de la base de datos del buzón de correo a petición utiliza el API de EWS (Exchange Web Services) para conectarse a Microsoft Exchange Server mediante HTTP/HTTPS. También, el explorador realiza un proceso de exploración paralela para mejorar el rendimiento.
Clúster de ESET	El Clúster de ESET permite la administración de servidores múltiples desde una sola ubicación. Similar a ESET File Security para Microsoft Windows Server, la unión de servidores a nodos facilita la administración debido a su capacidad para distribuir una configuración en todos los nodos miembros del clúster. El Clúster de ESET también se puede utilizar para sincronizar las bases de datos de la creación de listas grises y los contenidos de la cuarentena de correo local.
Exclusiones de procesos	Excluye procesos específicos de la exploración en el acceso del Anti-Malware. La exploración en el acceso del Anti-Malware puede generar conflictos en ciertas situaciones, por ejemplo, durante un proceso de copia de seguridad o migraciones en vivo de máquinas virtuales. Las exclusiones de procesos ayudan a minimizar el riesgo de conflictos potenciales y a mejorar el rendimiento de aplicaciones excluidas, lo que a su vez tiene un efecto positivo sobre el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso/aplicación es una exclusión de su archivo ejecutable (.exe).
eShell (Shell de ESET)	eShell 2.0 ahora está disponible en ESET Mail Security. eShell es una interfaz de línea de comandos que ofrece a los usuarios y administradores avanzados opciones más exhaustivas para administrar los productos de servidor de ESET.
ESET PROTECT	Mejor integración con ESET PROTECT incluida la posibilidad de programar varias tareas. Para más información sobre ESET PROTECT, visite Ayuda en línea.
Instalación basada en componentes	La instalación se puede personalizar para que contenga únicamente partes seleccionadas del producto.
Protección contra la suplantación de identidad del remitente	Una nueva función que brinda protección frente a una práctica habitual de falsificar información de remitentes de un correo electrónico llamado suplantación de remitente. Es improbable que el destinatario del correo electrónico distinga un remitente válido de uno falsificado, ya que el correo electrónico suele aparecer como si se hubiera enviado desde una fuente legítima. En Configuración avanzada puede activar y configurar la Protección contra la suplantación de remitente o crear reglas personalizadas.
Firma DKIM	ESET Mail Security ofrece una función de firma DKIM para mejorar la seguridad de los mensajes de correo electrónico salientes. Seleccione el certificado del cliente y especifique qué encabezados de correo electrónico están firmados con la firma DKIM. Puede configurar la firma DKIM para cada dominio por separado para varios dominios.

Novedades

Nuevas funciones y mejoras en ESET Mail Security:

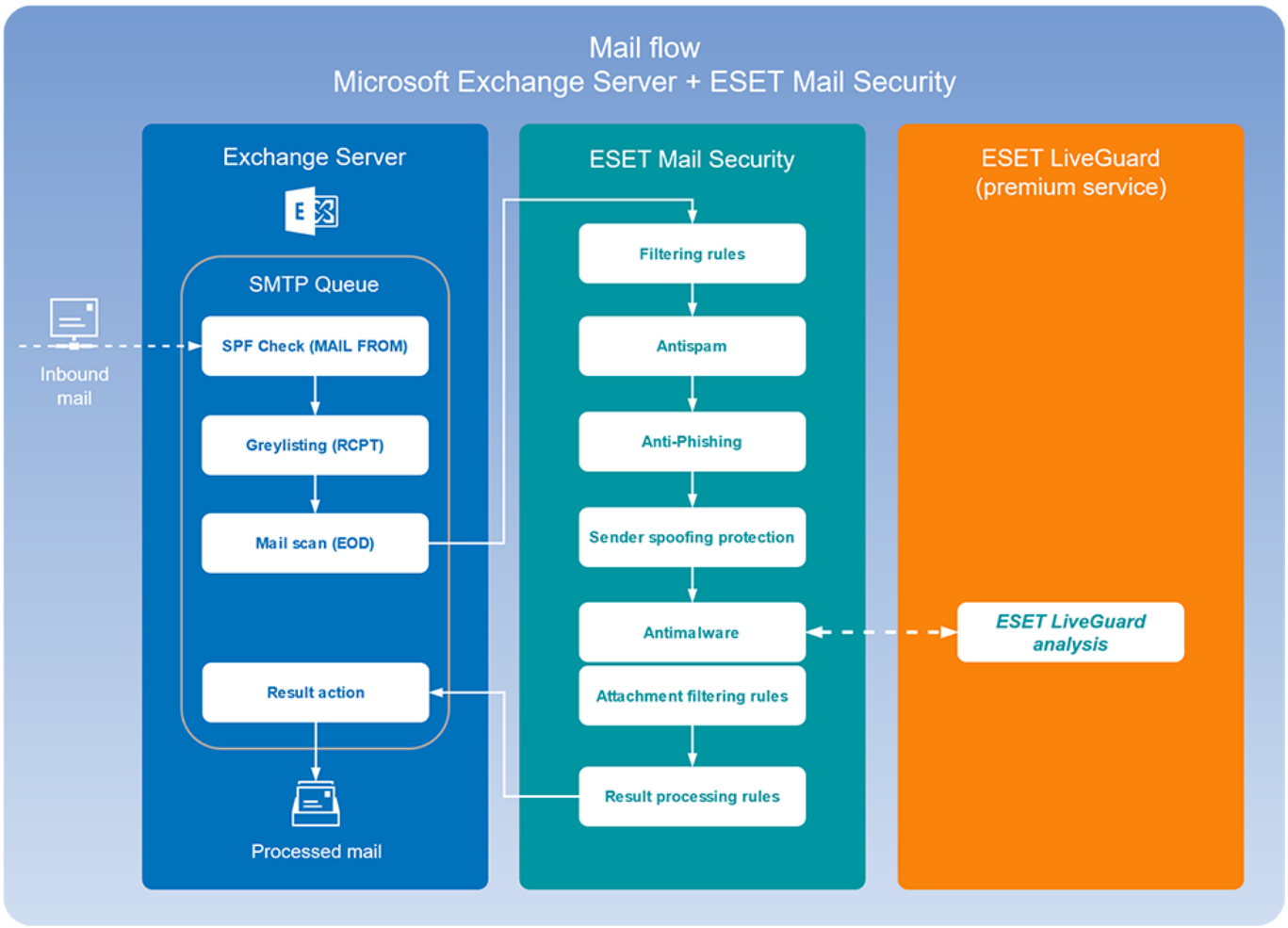
- Producto de 64 bits nativo
- Exploración del buzón de Office 365
- Protección Anti-Phishing para correo
- Protección contra retrodispersión
- Informes del administrador de cuarentena de correos
- Informe de protección del servidor de correo electrónico

- ESET Cluster ahora disponible en Cuarentena de correos
- Sincronización de cuarentena de correos local a través del Clúster de ESET
- Registro de Protección SMTP
- ESET LiveGuard Advanced
- ESET Inspect soporte
- ESET RMM
- Exportar a servidor syslog (Arcsight)
- Aislamiento de red
- Detección de aprendizaje automático
- Registros de auditorías
- microactualizaciones de componentes del programa
- Protección contra la suplantación de identidad del remitente
- Firma DKIM
- Exploración del buzón de Microsoft 365

Consulte los registros de cambios detallados para ESET Mail Security.

Flujo de correos

En el siguiente diagrama, se muestra el flujo de correos en Microsoft Exchange Server y ESET Mail Security. Para obtener más información sobre el uso de ESET LiveGuard Advanced con ESET Mail Security, consulte la Ayuda en línea de ESET LiveGuard Advanced.



ESET Mail Security Características y roles de Exchange Server

En la siguiente tabla, puede identificar qué características están disponibles para cada versión compatible de Microsoft Exchange Server y sus roles. El asistente de instalación de ESET Mail Security comprueba el entorno durante la instalación y, una vez instalado, ESET Mail Security mostrará las características según la versión detectada de Exchange Server y sus roles.

Versión y roles de Exchange Server	Protección antispam	Protección antiphishing	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Protección de la base de datos de correo electrónico
Microsoft Exchange Server 2010 (múltiples funciones)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2010 (casilla de correo)	?	✓	✓	?	✓	✓

Versión y roles de Exchange Server	Protección antispam	Protección antiphishing	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Protección de la base de datos de correo electrónico
Microsoft Exchange Server 2013 (múltiples funciones)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2013 (casilla de correo)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2016 (casilla de correo)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2019 (casilla de correo)	✓	✓	✓	✓	✓	?

Roles de Exchange Server

Rol de Edge y rol de Hub

Tanto los servidores Transporte Edge como Transporte Hub tienen las características antispam deshabilitadas de manera predeterminada. Esta es la configuración deseada en una organización de Exchange con el servidor Transporte Edge. Recomendamos que el servidor Transporte Edge tenga activado el antispam ESET Mail Security configurado para filtrar los mensajes antes de que se distribuyan a la organización Exchange.

El rol de Edge es la ubicación preferida para la exploración antispam ya que permite a ESET Mail Security rechazar el spam durante la primera etapa del proceso sin sobrecargar innecesariamente los niveles de red. Con esta configuración, ESET Mail Security filtra los mensajes entrantes en el servidor Transporte Edge, para que puedan moverse con seguridad al servidor Transporte Hub sin necesidad de un filtro adicional.

Supongamos que su organización no usa un servidor Transporte Edge y solo tiene un servidor Transporte Hub. En ese caso, se recomienda habilitar las características antispam en el servidor Transporte Hub que recibe mensajes entrantes de Internet a través de SMTP.

> i Debido a las restricciones técnicas de Microsoft Exchange Server 2010 y versiones posteriores, ESET Mail Security no soporta la implementación de Microsoft Exchange Server con el rol de Client Access Server (CAS) únicamente (por sí solo, Servidor de Acceso de Cliente)

Módulos de protección

La funcionalidad del núcleo de ESET Mail Security incluye los siguientes módulos de protección:

- Antivirus

La protección antivirus es una de las funciones básicas del producto ESET Mail Security. La protección antivirus defiende el sistema ante ataques malintencionados mediante el control de archivos, correos electrónicos y comunicaciones por Internet. Si se detecta una amenaza con código malicioso, el módulo antivirus la puede eliminar al bloquearla y luego desinfectarla, eliminándola o enviándola a Cuarentena.

Antispam

La protección antispam incorpora múltiples tecnologías (tales como RBL, DNSBL, huellas digitales, verificación de reputación, análisis de contenido, reglas, creación manual de listas blancas y negras, etc.) para maximizar la detección de amenazas provenientes del correo electrónico.
ESET Mail Security El antispam se basa en la nube y la mayoría de las bases de datos en la nube se ubican en los centros de datos de ESET. Los servicios antispam en la nube permiten actualizaciones rápidas de datos que proporcionan un tiempo de reacción más veloz en caso de aparición de un nuevo spam. También permite eliminar datos incorrectos o falsos de las listas negras de ESET. La comunicación con los servicios antispam en la nube se realiza a través de un protocolo propietario en el puerto 53535, siempre que sea posible. Si no es posible comunicarse a través del protocolo de ESET, se utilizan en su lugar los servicios de DNS (puerto 53). Sin embargo, el uso de DNS no es tan efectivo porque requiere que se envíen varias solicitudes durante el proceso de clasificación de correo no deseado de un solo mensaje de correo electrónico.

> Recomendamos que abra el puerto 53535 de TCP/UDP para las direcciones IP enumeradas en este artículo de base de conocimiento. Este puerto es utilizado por ESET Mail Security para enviar solicitudes.

Por lo general, no se envían mensajes de correo electrónico ni de sus partes durante el proceso de clasificación de spam. Sin embargo, supongamos que ESET LiveGrid® está habilitado y ha permitido explícitamente que las muestras se envíen para su análisis. En ese caso, solo se pueden enviar mensajes marcados como spam (o probablemente spam) para ayudar con el análisis exhaustivo y la mejora de la base de datos en la nube.
Si desea denunciar la clasificación de falsos positivos o falsos negativos de spam, consulte nuestro artículo de base de conocimiento para más información.
Además, ESET Mail Security también podrá utilizar el método de Listas grises (deshabilitado de manera predeterminada) para el filtrado de spam.

Anti-Phishing

ESET Mail Security incluye protección anti-phishing que evita que los usuarios accedan a páginas web conocidas por phishing. Mensajes de correo electrónico que pudieran contener enlaces que conducen a páginas web con phishing, ESET Mail Security usa un analizador que busca en el cuerpo del mensaje y asunto de los mensajes de correo electrónico entrantes para identificar dichos vínculos (URL). Los vínculos se comparan contra la base de datos de phishing y se evalúan las reglas con condición cuerpo del mensaje.

Reglas

La disponibilidad de reglas para la protección de la base de datos del buzón de correo electrónico, Exploración de la base de datos del correo electrónico a petición, Exploración y Protección del transporte de correo electrónico en su sistema varía según la versión de Microsoft Exchange Server que tenga instalada con ESET Mail Security.
Las Reglas le permiten definir manualmente las condiciones de filtrado de correo electrónico y las acciones que se deben realizar con los mensajes de correo electrónico filtrados. Existen diferentes conjuntos de condiciones y acciones. Puede crear reglas individuales que también se pueden combinar entre sí. Si una regla usa varias condiciones, las condiciones se vincularán usando el operador lógico AND. En consecuencia, la regla se ejecutará únicamente cuando se cumplan todas sus condiciones. Si se crean varias reglas, se aplicará el operador lógico OR, lo que significa que el programa ejecutará la primera regla para la cual se cumplan las condiciones.
La primera técnica que se usa en la secuencia de exploración es la creación de listas grises si está habilitada. Los procedimientos subsiguientes siempre ejecutarán estas técnicas: protección basada en las reglas definidas por el usuario, luego, la exploración antivirus y, finalmente, una exploración antispam.

Seguridad multicapa

ESET Mail Security proporciona una protección compleja en diferentes niveles:

- Protección de la base de datos de correo electrónico
- Protección del transporte de correo electrónico
- Exploración de la base de datos del buzón de correo a petición
- La exploración de base de datos del buzón de Microsoft 365

> Para una visión completa, vea matriz de ESET Mail Security características y las versiones de Microsoft Exchange Server y sus roles.

Protección de la base de datos del buzón de correo electrónico

Microsoft Exchange Server activa el proceso de exploración del buzón de correo y lo controla. Los correos electrónicos en el almacén de Microsoft Exchange Server se exploran constantemente. Dependiendo de la versión de Microsoft Exchange Server, la versión de la interfaz VSAPI y la configuración definida por el usuario, el proceso de exploración puede activarse en cualquiera de las siguientes situaciones:

- Cuando el usuario accede al correo electrónico, por ejemplo, en un cliente de correo electrónico (el correo electrónico siempre se analiza con el motor de detección más reciente).
- En segundo plano, cuando el uso de Microsoft Exchange Server es bajo.
- En forma proactiva (basándose en el algoritmo interno de Microsoft Exchange Server).

> La protección de la base de datos del buzón de correo electrónico no está disponible para Microsoft Exchange Server 2013, 2016 y 2019.

La protección de la base de datos del buzón de correo electrónico está disponible para los siguientes sistemas:

Versión y roles de Exchange Server	Protección antispam	Protección antiphishing	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Protección de la base de datos de correo electrónico
Microsoft Exchange Server 2010 (casilla de correo)	⍰	✓	✓	⍰	✓	✓
Microsoft Exchange Server 2010 (múltiples funciones)	✓	✓	✓	✓	✓	✓

Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya el rol de Casilla de correo o Respaldo).

Protección del transporte de correo electrónico

El filtrado en el nivel del servidor SMTP se asegura mediante el uso de un complemento especial. En Microsoft Exchange Server 2010, the plugin is registered as a transport agent on the Edge or the Hub roles of the Microsoft

Exchange Server.el plugin está registrado como un agente de transporte en los roles Edge o Hub de Microsoft Exchange Server.

El filtrado en el nivel del servidor SMTP por un agente de transporte ofrece protección antivirus, antispam y mediante reglas definidas por el usuario. A diferencia del filtrado de VSAPI, el filtrado en el nivel del servidor SMTP se realiza antes de que el correo electrónico explorado llegue al buzón de correo de Microsoft Exchange Server.

Anteriormente se denominaba filtrado de mensajes a nivel del servidor SMTP. Esta protección es proporcionada por el agente de transporte y solo está disponible para Microsoft Exchange Server 2010 o más reciente ejecutado en rol de servidor Transporte Edge o servidor Transporte Hub. Este tipo de exploración puede realizarse en una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados).

La protección del transporte de correo electrónico está disponible para los siguientes sistemas:

Versión y roles de Exchange Server	Protección antispam	Protección antiphishing	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Protección de la base de datos de correo electrónico
Microsoft Exchange Server 2010 (múltiples funciones)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2013 (múltiples funciones)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	⍰	⍰
Microsoft Exchange Server 2013 (casilla de correo)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	⍰	⍰
Microsoft Exchange Server 2016 (casilla de correo)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	⍰	⍰
Microsoft Exchange Server 2019 (casilla de correo)	✓	✓	✓	✓	✓	⍰

Exploración de la base de datos del buzón de correo a petición

Le permite ejecutar o programar una exploración de la base de datos del buzón de correo de Exchange. Esta característica solo está disponible para Microsoft Exchange Server 2010 o más reciente que funcione en el rol de Servidor de la casilla de correo o Transporte Hub. Esto también se aplica a una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor mencionados).

La exploración de base de datos del buzón de correo bajo demanda está disponible para los siguientes sistemas:

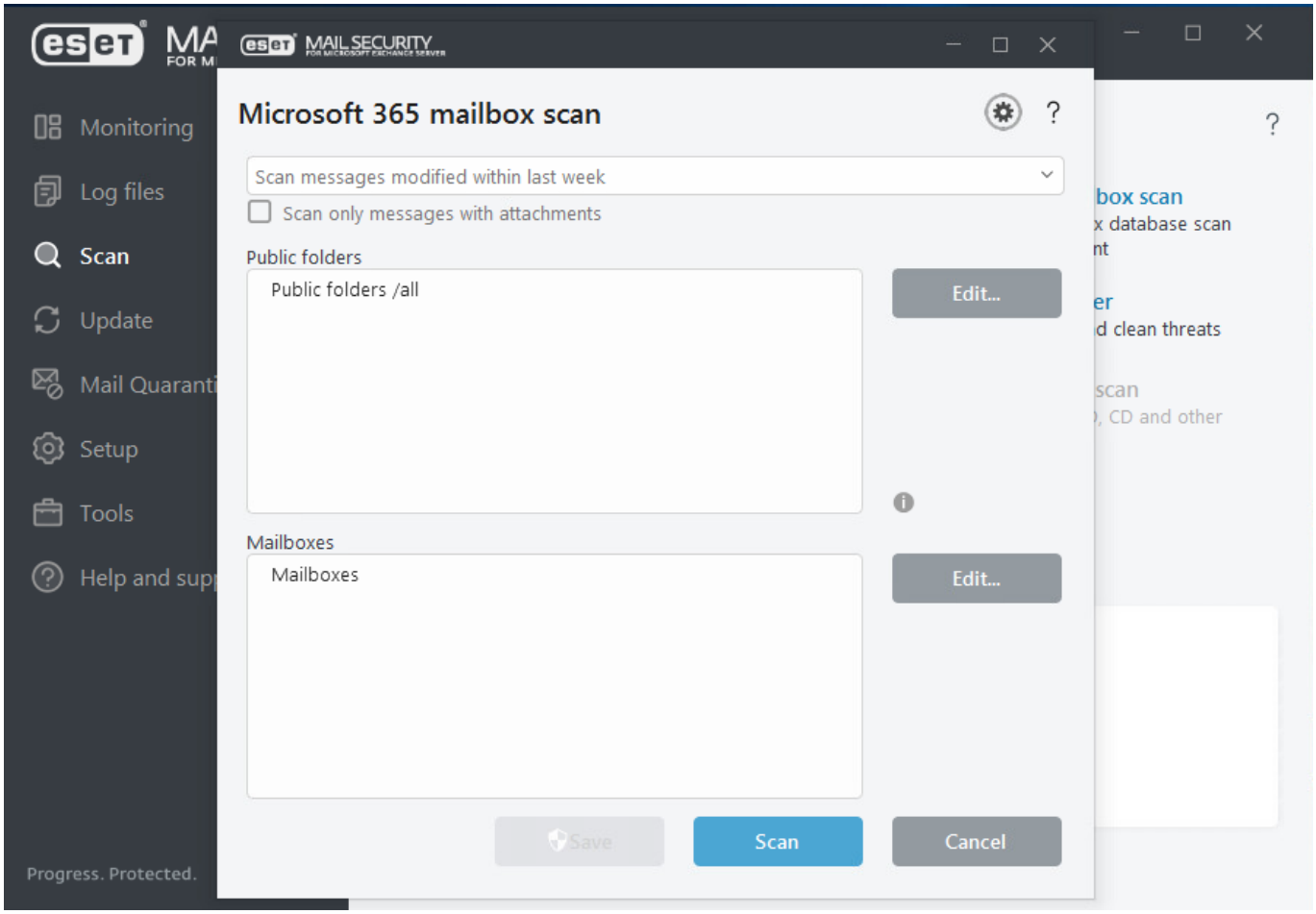
Versión y roles de Exchange Server	Protección antispam	Protección antiphishing	Reglas	Protección del transporte de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Protección de la base de datos de correo electrónico
Microsoft Exchange Server 2010 (múltiples funciones)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2010 (casilla de correo)	⍰	✓	✓	⍰	✓	✓
Microsoft Exchange Server 2013 (múltiples funciones)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2013 (casilla de correo)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2016 (casilla de correo)	✓	✓	✓	✓	✓	⍰
Microsoft Exchange Server 2019 (casilla de correo)	✓	✓	✓	✓	✓	⍰

La exploración de base de datos del buzón de Microsoft 365

ESET Mail Security provee funcionalidad de exploración para ambientes híbridos de Microsoft 365. Está disponible y visible en ESET Mail Security solo si tiene un ambiente híbrido de Exchange (in situ y nube). Ambas posibilidades de enrutamiento son compatibles, a través de **Exchange Online** u organización **in situ**. Para obtener más información, consulte Enrutamiento de transporte en implementaciones híbridas de Exchange.

Para activar esta función, registre el explorador ESET Mail Security.

Puede explorar las casillas de correo electrónico de Microsoft 365 y las carpetas públicas de la misma manera que lo haría con la exploración de la base de datos del buzón de correo electrónico a petición.



Ejecutar una exploración completa de la base de datos de correo electrónico en entornos grandes puede provocar cargas de sistema no deseadas. Para evitar este problema, ejecute un análisis en bases de datos o buzones de correo específicos. Para minimizar aún más el impacto del sistema, debe usar un filtro de tiempo en la parte superior de la ventana. Por ejemplo, en lugar de usar **Explorar todos los mensajes**, puede seleccionar **Explorar los mensajes modificados en la última semana**.

Le recomendamos configurar Microsoft 365. Presione la tecla **F5** y haga clic en **Servidor** > **exploración de base de datos del buzón de correo a petición**. Además, consulte los detalles de la cuenta de exploración de base de datos.

Para ver la actividad de exploración del buzón de correo de Office 365, consulte **Archivos de registro** > **Exploración de base de datos del buzón de correo**.

Requisitos del sistema

Sistemas operativos compatibles:

- Microsoft Windows Server 2022 (Server Core y Desktop Experience)
- Microsoft Windows Server 2019 (Server Core y Desktop Experience)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

La compatibilidad con Azure Code Signing debe estar instalada en todos los sistemas operativos Windows para instalar o actualizar los productos ESET lanzados después de julio de 2023. Más información.

Versiones compatibles de Microsoft Exchange Server:

- Microsoft Exchange Server 2019 hasta CU13
- Microsoft Exchange Server 2016 hasta CU23
- Microsoft Exchange Server 2013 hasta CU23 (CU1 y CU4 no son compatibles)
- Microsoft Exchange Server 2010 SP1, SP2, SP3 hasta RU32

El rol de servidor de acceso de cliente (CAS) independiente no es compatible, consulte Roles de Exchange Server para obtener más información.
Se recomienda hacer referencia a las características de ESET Mail Security y los roles de Exchange Server para identificar las funciones que están disponibles para cada versión compatible de Microsoft Exchange Server y sus roles.

Requisitos mínimos de hardware:

Componente	Requisito
Procesador	Intel o AMD x64 de núcleo único
Memoria	256 MB de memoria libre
Disco rígido	700 MB de espacio libre en el disco
Resolución de pantalla	800 x 600 píxeles o superior

ESET Mail Security tiene los mismos requisitos de hardware recomendados que se aplican a Microsoft Exchange Server. Consulte los siguientes artículos técnicos de Microsoft para obtener más información:

Microsoft Exchange Server 2010

Microsoft Exchange Server 2013

Microsoft Exchange Server 2016

Recomendamos firmemente instalar el último Service Pack de su sistema operativo Microsoft Server y la aplicación antes de instalar el producto de seguridad de ESET. Recomendamos instalar las actualizaciones y las correcciones de problemas de Windows más recientes en cuanto estén disponibles.

Preparar para la instalación

Recomendamos seguir estos pocos pasos en la preparación de la instalación del producto:

- Luego de adquirir ESET Mail Security, descargue el paquete de instalación .msi desde el sitio web de ESET.
- Asegúrese de que el servidor en el que instalará ESET Mail Security cumpla con los requisitos del sistema.
- Inicie sesión en el servidor con una Cuenta de administrador.
- Si va a realizar una actualización desde una instalación existente de ESET Mail Security, le recomendamos

hacer una copia de respaldo de la configuración actual mediante la característica Exportar la configuración

• Elimine/desinstale el software antivirus de terceros de su sistema, Para ver una lista de software antivirus de terceros, si corresponde. Le recomendamos usar ESET AV Remover . Para ver una lista de software antivirus de terceros que se pueden eliminar con la herramienta ESET AV Remover, consulte este artículo de base de conocimiento.

• Si está ESET Mail Security instalando en Windows Server 2016, Microsoft recomienda que desinstale las características de Windows Defender (Microsoft Defender Antivirus) y rescindir de la inscripción ATP de Windows Defender para evitar problemas causados por la instalación de múltiples productos antivirus en una máquina.

• Si está instalando ESET Mail Security en Windows Server 2019 o Windows Server 2022, Microsoft recomienda deshabilitar Microsoft Defender Antivirus manualmente para evitar problemas causados por la instalación de múltiples productos antivirus en una máquina.

> Si las **funciones de Windows Defender** están presentes en su Windows Server 2016, 2019 o 2022 durante la instalación de ESET Mail Security, ESET Mail Security desactiva estas funciones para evitar colisiones de la protección en tiempo real entre varios productos antivirus. Además, ESET Mail Security desactiva las características de Windows Defender con cada inicio y reinicio del sistema.
> Hay una excepción: si realiza una instalación de componentes sin el componente de **Protección del sistema de archivos en tiempo real**, las características de Windows Defender en Windows Server 2016 no se desactivarán.

• Para una visión completa, vea matriz de ESET Mail Security características y las versiones de Microsoft Exchange Server y sus roles.

• Para verificar la cantidad de buzones de correo, ejecute la herramienta de recuento de buzones de correo, consulte nuestro artículo de la base de conocimientos para obtener más información. Después de instalar ESET Mail Security, se mostrará el recuento de buzones de correo actual en la parte inferior de la ventana Supervisión.

El instalador ESET Mail Security puede ejecutarse de dos maneras:

• Ventana del programa principal: la instalación recomendada es con el Asistente de instalación.

• Instalación silenciosa/desatendida – Además de poder usara el asistente de instalación, puede elegir instalar ESET Mail Security en forma silenciosa a través de una línea de comando.

• Actualizando a la versión más reciente. – Si usa una versión de ESET Mail Security anterior, puede elegir un método de actualización adecuado.

Luego de que haya instalado o actualizado correctamente su ESET Mail Security, deberá hacer lo siguiente:

Activación de producto

Los escenarios de activación disponibles en la ventana de activación pueden variar según el país y los medios de distribución.

Tareas posteriores a la instalación

Consulte la lista de tareas recomendadas que puede realizar después de una instalación exitosa de ESET Mail Security.

Ajustar las configuraciones generales

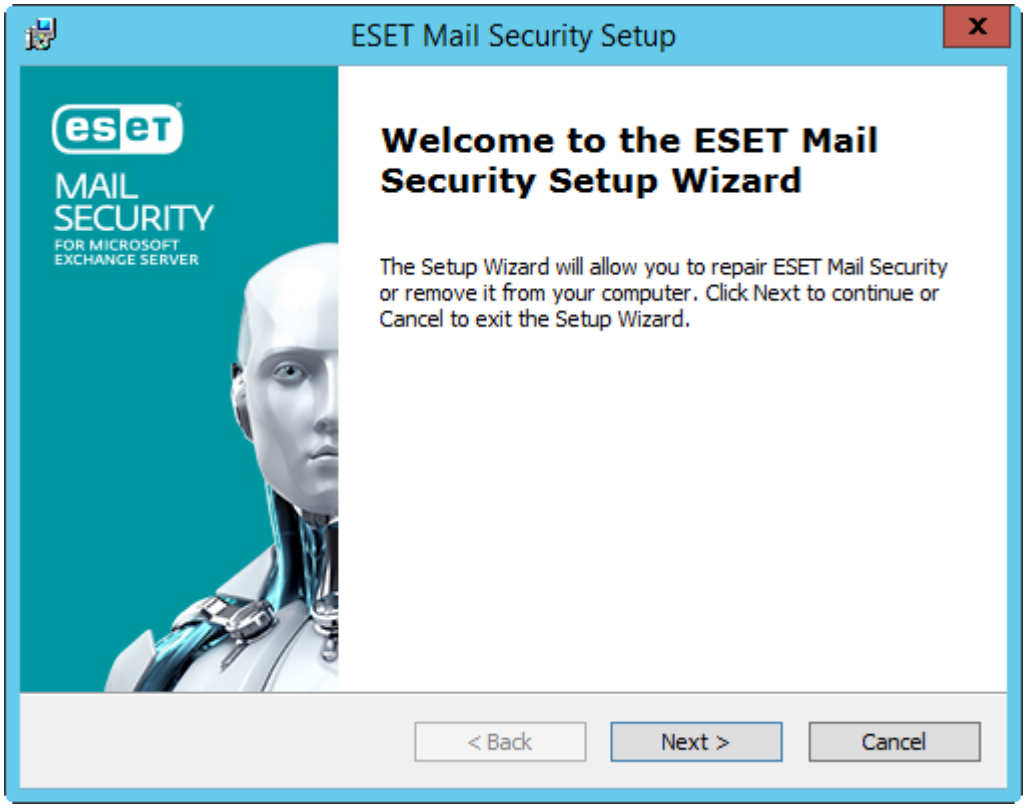
Puede ajustar ESET Mail Security si modifica la configuración avanzada de cada característica.

Pasos para la instalación de ESET Mail Security

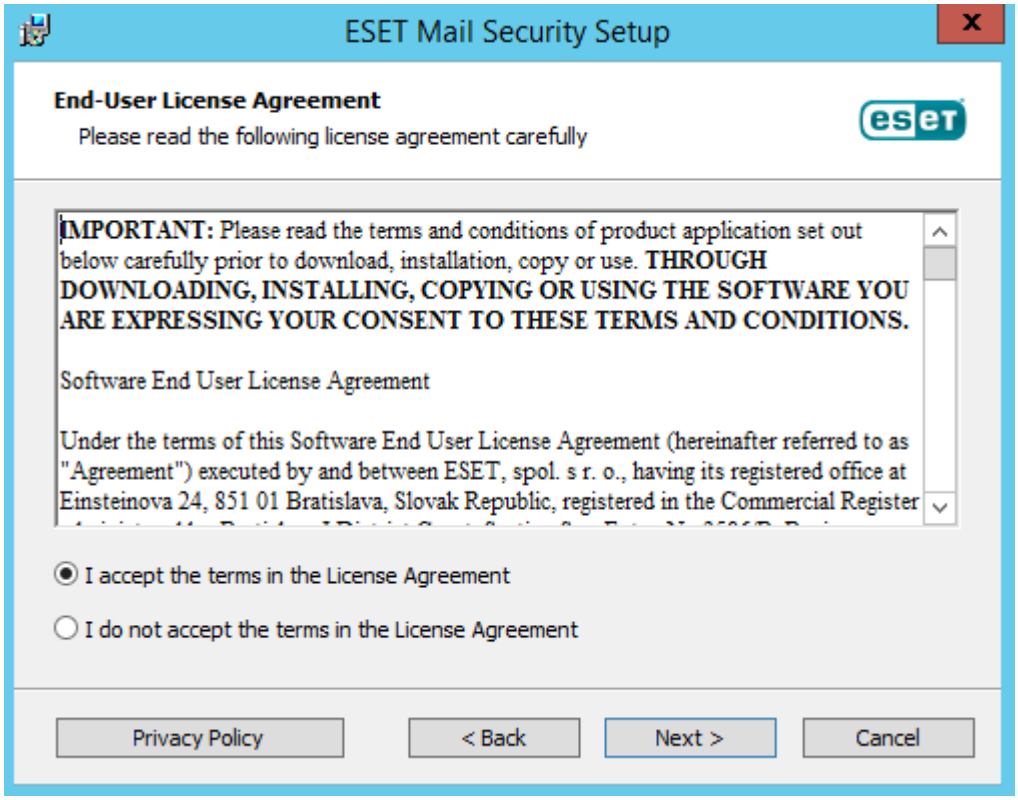
Este es un asistente de instalación típica de ventana principal del programa. Haga doble clic en el paquete .msi y siga los pasos para instalar ESET Mail Security:

1. Haga clic en **Siguiente** para continuar o en **Cancelar** para salir de la instalación.

2. El asistente de instalación permite ejecutar un lenguaje especificado como **Ubicación inicial** de la configuración **Región** > **Ubicación** de su sistema operativo (o **Ubicación actual** de una configuración **Región e idioma** > **Ubicación** en los sistemas anteriores). Utilice el menú desplegable para seleccionar el **Idioma del producto** en que se instalará su ESET Mail Security. El idioma seleccionado para ESET Mail Security es independiente del lenguaje que ve en el asistente de instalación.



3. Haga clic en **Siguiente** y se mostrará el Acuerdo de licencia para el usuario final. Luego de confirmar la aceptación del Acuerdo de licencia para el usuario final y de la Política de privacidad, haga clic en **Siguiente**.



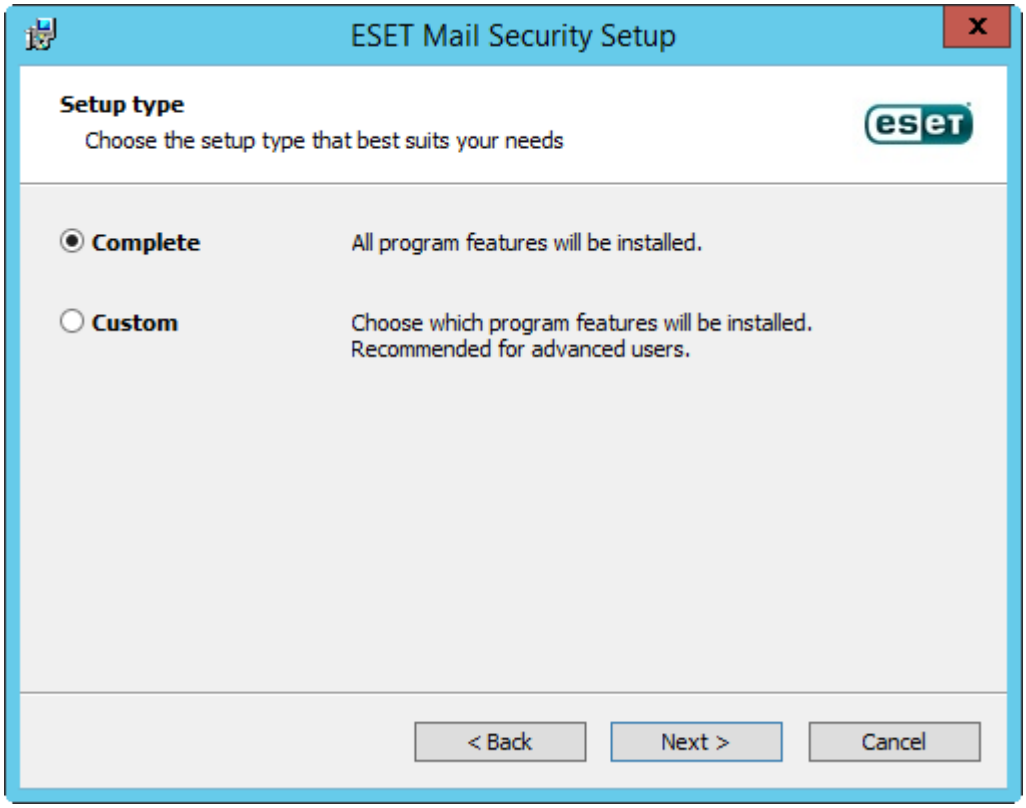
4. Elija uno de los tipos de instalación disponibles (la disponibilidad depende de su sistema operativo):

Completa

Instala todas las funciones de ESET Mail Security.

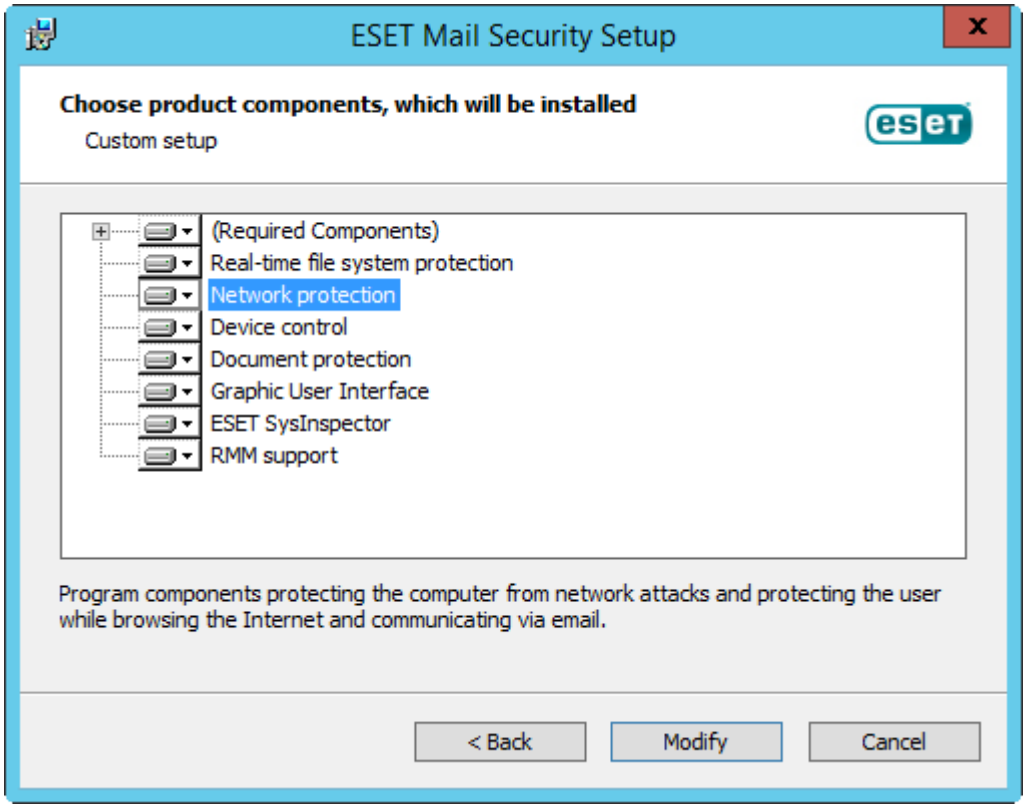
> El instalador solo incluye los módulos esenciales. El resto de los módulos se descargarán durante la actualización del módulo inicial tras la activación del producto.

> En caso de que planee utilizar cuarentena local para los mensajes de correo electrónico y no desea que los archivos de mensaje en cuarentena se almacenen en su unidad C:, cambie la ruta de la **carpeta de datos** con su unidad y ubicación preferidas. Sin embargo, tenga en cuenta que todos los archivos de datos de ESET Mail Security se almacenarán en esta ubicación.



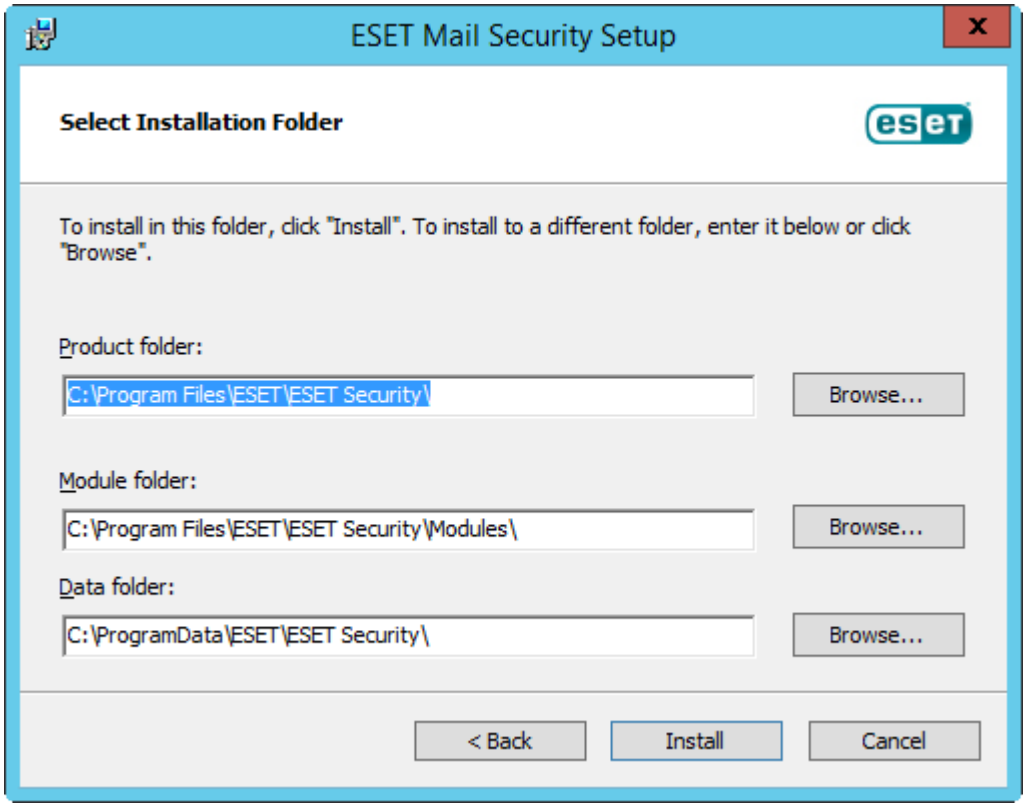
Personalizada

Le permite elegir que características de ESET Mail Security se instalarán en su sistema. Aparecerá una lista de módulos y características del producto antes de comenzar la instalación. Es útil cuando se quiere personalizar ESET Mail Security solamente con los componentes que necesita.



5. Se le pedirá que seleccione la ubicación en la que desea instalar ESET Mail Security. En forma predeterminada, el programa se instala en *C:\Program Files\ESET\ESET Mail Security*. Haga clic en **Examinar**

para cambiar esta ubicación (no se recomienda).

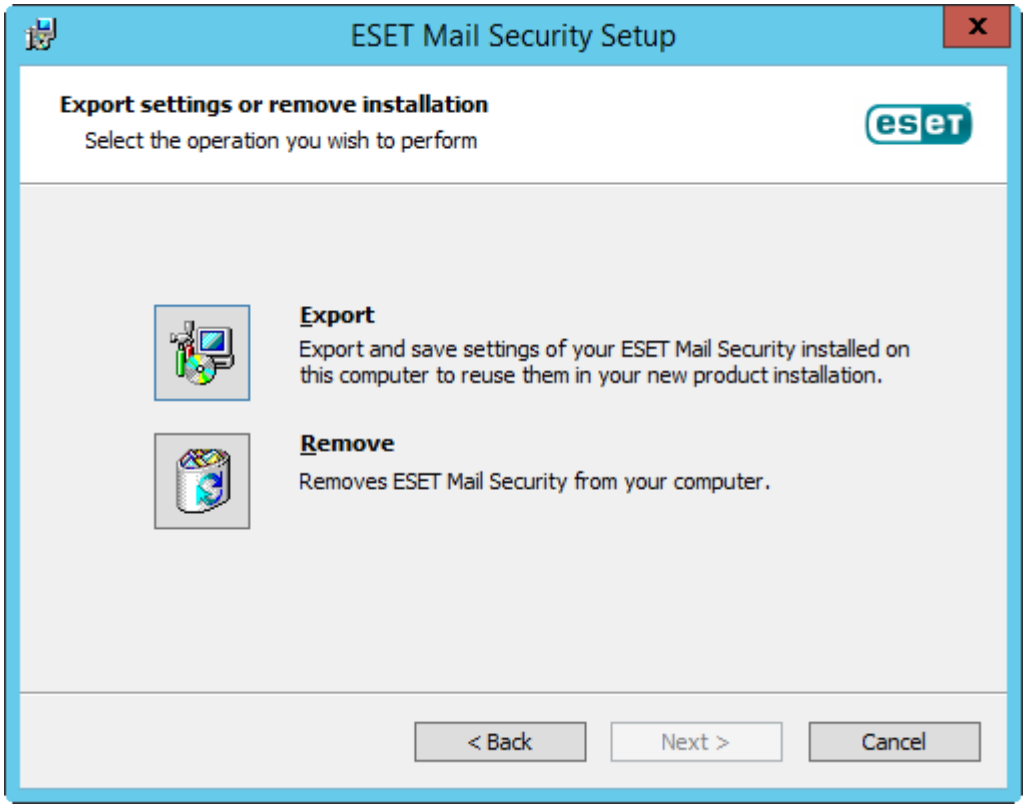


6. Haga clic en **Instalar** para comenzar la instalación. Tras la instalación, se le pedirá que active ESET Mail Security.

Exportar configuración o eliminar instalación

Puede exportar y guardar la configuración o quitar la instalación. Para hacerlo, ejecute el paquete de instalador *.msi* que usó durante la instalación inicial, o vaya a **Programas y características** (accesible desde el Panel de control de Windows), haga clic con el botón secundario en ESET Mail Security y seleccione **Cambiar**.

Puede **exportar** su configuración de ESET Mail Security o **quitar** (desinstalar) ESET Mail Security por completo.



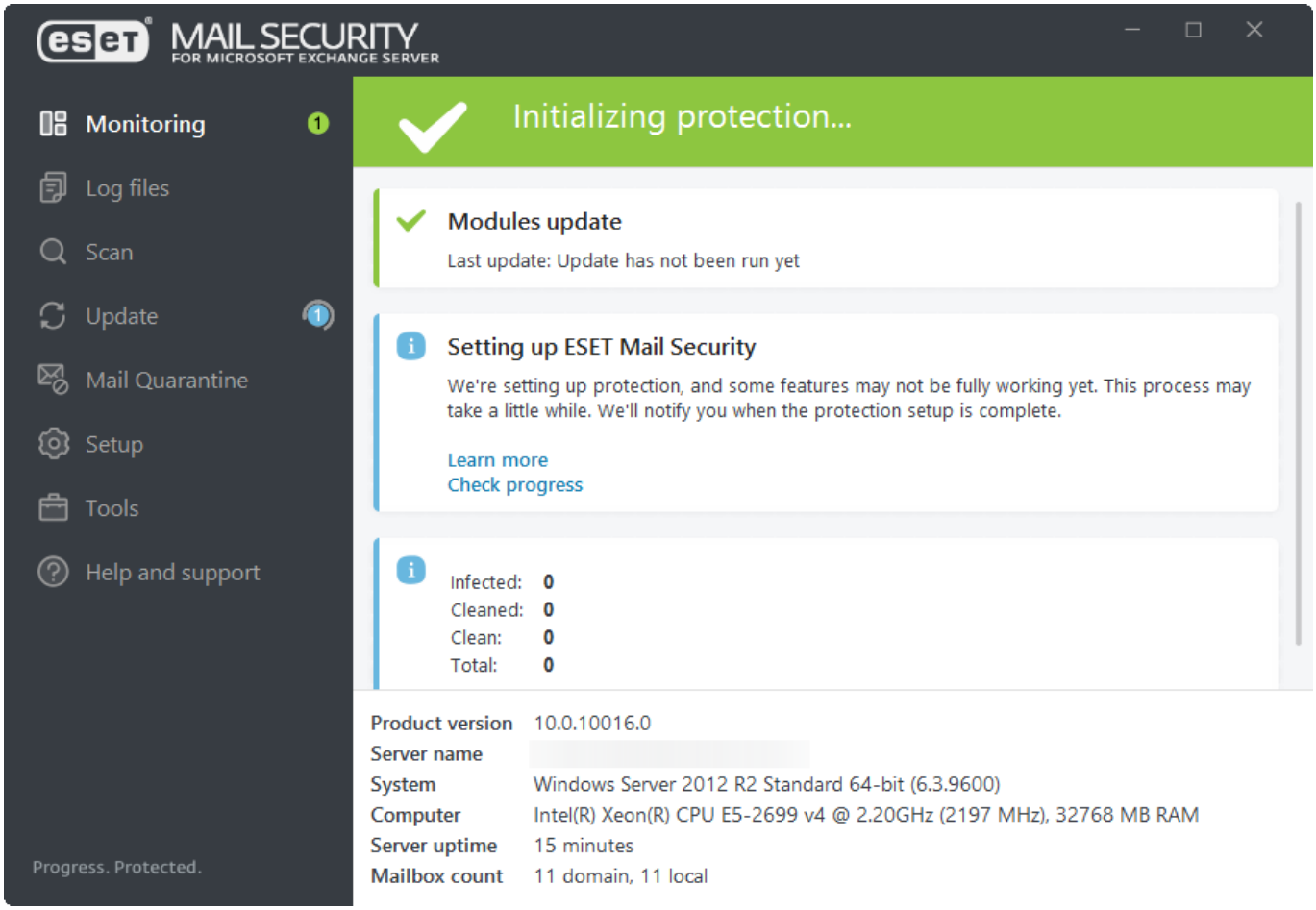
Actualización de módulos iniciales

Para reducir el tráfico de red relacionado con el tamaño del instalador y ahorrar recursos, el instalador solo contiene módulos esenciales. El resto de los módulos se descargarán durante la actualización inicial del módulo tras la activación del producto. La principal ventaja es un instalador de menor tamaño, y que ESET Mail Security descarga solo los módulos de la aplicación más recientes cuando activa el producto.

El instalador de módulos mínimo contiene los siguientes módulos:

- Loaders
- Soporte de Anti-Stealth
- Comunicación directa a la nube
- Soporte de traducción
- Configuración
- SSL

Tras la activación del producto, verá el estado **Iniciando protección** que le informa sobre las características que se inician.



Si tiene problemas para descargar los módulos (por ejemplo, sin conexión de red, firewall o configuración de proxy), se muestra el estado de aplicación de alerta **Se requiere atención**.
Haga clic en **Actualizar** > **Buscar actualizaciones** en la ventana principal del programa para iniciar el proceso de actualización de nuevo.
Tras varios intentos sin éxito, se muestra un estado rojo de la aplicación **Error en la configuración de la protección**. Si no puede actualizar los módulos, descargue el instalador completo de ESET Mail Security *.msi*.

Si su servidor no tiene conexión a Internet y necesita actualizaciones, use los siguientes métodos para descargar archivos de módulos de actualización de servidores de actualización de ESET:

- Actualización desde el mirror
- Usar la herramienta Mirror

Instalación silenciosa/sin supervisión

Ejecute el siguiente comando para completar la instalación a través de la línea de comandos: `msiexec /i <packagename> /qn /l*xv msi.log`

Utilice el Visor de eventos de Windows para comprobar el **Registro de aplicaciones** (busque registros en la fuente: MsiInstaller) para asegurarse de que la instalación sea correcta o revisar cualquier problema de instalación.

Instalación completa en un sistema de 64 bits:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Una vez finalizada la instalación, se inicia la interfaz gráfica de usuario (GUI) de ESET y se muestra el ícono del área de notificación de Windows en el área de notificación de Windows.

Instalación del producto en un **idioma específico** (por ejemplo, alemán):
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Consulte los **Parámetros de idioma** en el tema Instalación de la línea de comandos para obtener más información y ver la lista de códigos de idioma.

Al especificar los valores para los parámetros de `REINSTALL`, debe incluir el resto de las características que no utiliza como valores de los parámetros `ADDLOCAL` o `REMOVE`. Para que la instalación de la línea de comandos se ejecute correctamente, es necesario es necesario que incluya todas las funciones como valores de los parámetros`REINSTALL`, `ADDLOCAL` y `REMOVE`. Es posible que no pueda agregar o quitar características correctamente si no utiliza el parámetro `REINSTALL`.
Consulte la sección Instalación de la línea de comandos si desea obtener la lista completa de las características.

Instalación completa (desinstalación) de un sistema de 64 bits:
```
msiexec /x emsx_nt64.msi /qn /l*xv msi.log
```

Su servidor se reiniciará automáticamente tras una desinstalación correcta.

Instalación de la línea de comandos

La siguiente configuración está diseñada para usarse **solo con el nivel reducido**, básico y **sin nivel** de la interfaz de usuario. Vea la documentación de la versión `msiexec` utilizada para los conmutadores de línea de comando apropiados.

Parámetros admitidos:

APPDIR=<path>

- ruta : ruta de directorio válida
- Directorio de instalación de aplicación
- Por ejemplo: `emsx_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- ruta : ruta de directorio válida
- Directorio de instalación de los datos de la aplicación

MODULEDIR=<path>

- ruta : ruta de directorio válida

- Directorio de instalación del módulo

ADDLOCAL=<list>

- Instalación de componente: lista de características no obligatorias que se instalarán en forma local.
- Uso con paquetes *.msi*: `emsx_nt64.msi /qn ADDLOCAL=<list>`
- Para obtener más información sobre la propiedad `ADDLOCAL`, consulte https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- La lista `ADDLOCAL` es una lista separada por comas con todas las características que se instalarán.
- Al seleccionar una característica que se instalará, se debe incluir explícitamente la ruta completa (todas las funciones principales) en la lista.

REMOVE=<list>

- Instalación de componentes - característica principal que no quiere instalar a nivel local.
- Uso con paquetes .msi: `emsx_nt64.msi /qn REMOVE=<list>`
- Para obtener más información sobre la propiedad `REMOVE`, consulte https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove
- La lista `REMOVE` es una lista separada por comas con todas las funciones principales que se instalarán (o eliminarán en caso de que sea una instalación existente).
- Resulta suficiente especificar la función principal únicamente. No es necesario incluir de manera explícita todas las funciones secundarias en la lista.

ADDEXCLUDE=<list>

- La lista `ADDEXCLUDE` es una lista separada por comas con todos los nombres de funciones que no se deben instalar.
- Al seleccionar una característica que no debe instalarse, la ruta completa (es decir, todos sus subccaracterísticas) y las características invisibles relacionadas deben incluirse explícitamente en la lista.
- Por ejemplo: `emsx_nt64.msi /qn ADDEXCLUDE=<list>`

> ℹ `ADDEXCLUDE` no se puede usar con `ADDLOCAL`.

Presencia de característica

- **Obligatoria** : la característica siempre está instalada.
- **Opcional**: La característica puede ser deseleccionada para la instalación.
- **Invisible**: función lógica obligatoria para que otras características funcionen correctamente.

Lista de ESET Mail Security características:

Los nombres de todas las características distinguen entre mayúsculas y minúsculas, por ejemplo `RealtimeProtection` no es igual a `REALTIMEPROTECTION`.

Nombre de característica	Presencia de característica
SERVER	Obligatoria
RealtimeProtection	Obligatoria
MAILSERVER	Obligatoria
WMIProvider	Obligatoria
HIPS	Obligatoria
Updater	Obligatoria
eShell	Obligatoria
UpdateMirror	Obligatoria
DeviceControl	Opcional
DocumentProtection	Opcional
WebAndEmail	Opcional
ProtocolFiltering	Invisible
NetworkProtection	Opcional
IdsAndBotnetProtection	Opcional
Rmm	Opcional
WebAccessProtection	Opcional
EmailClientProtection	Opcional
MailPlugins	Invisible
Cluster	Opcional
_Base	
eula	
ShellExt	Opcional
_FeaturesCore	
GraphicUserInterface	Opcional
SysInspector	Opcional
SysRescue	Opcional
EnterpriseInspector	Opcional

Si desea eliminar cualquiera de las siguientes características, deberá eliminar todo el grupo, para lo cual deberá especificar cada una de las funciones que pertenecen al grupo. De lo contrario, la característica no se eliminará. Aquí se muestran dos grupos (cada línea representa un grupo):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailP
lugins,EmailClientProtection
```

Excluya la sección **NetworkProtection** (incluidas las características secundarias) de la instalación mediante el uso del parámetro `REMOVE`.
Especifique únicamente la característica principal:
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

Alternativamente, puede usar el parámetro `ADDEXCLUDE`, pero también debe especificar todas las características secundarias:
```
msiexec /i emsx_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^
ProtocolFiltering,MailPlugins,EmailClientProtection
```

Si desea que su ESET Mail Security se configure automáticamente después de la instalación, puede especificar los parámetros de configuración básicos en el comando de instalación.

Instalar ESET Mail Security y deshabilitar ESET LiveGrid®:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log CFG_LIVEGRID_ENABLED=0
```

Lista de todas las propiedades de configuración:

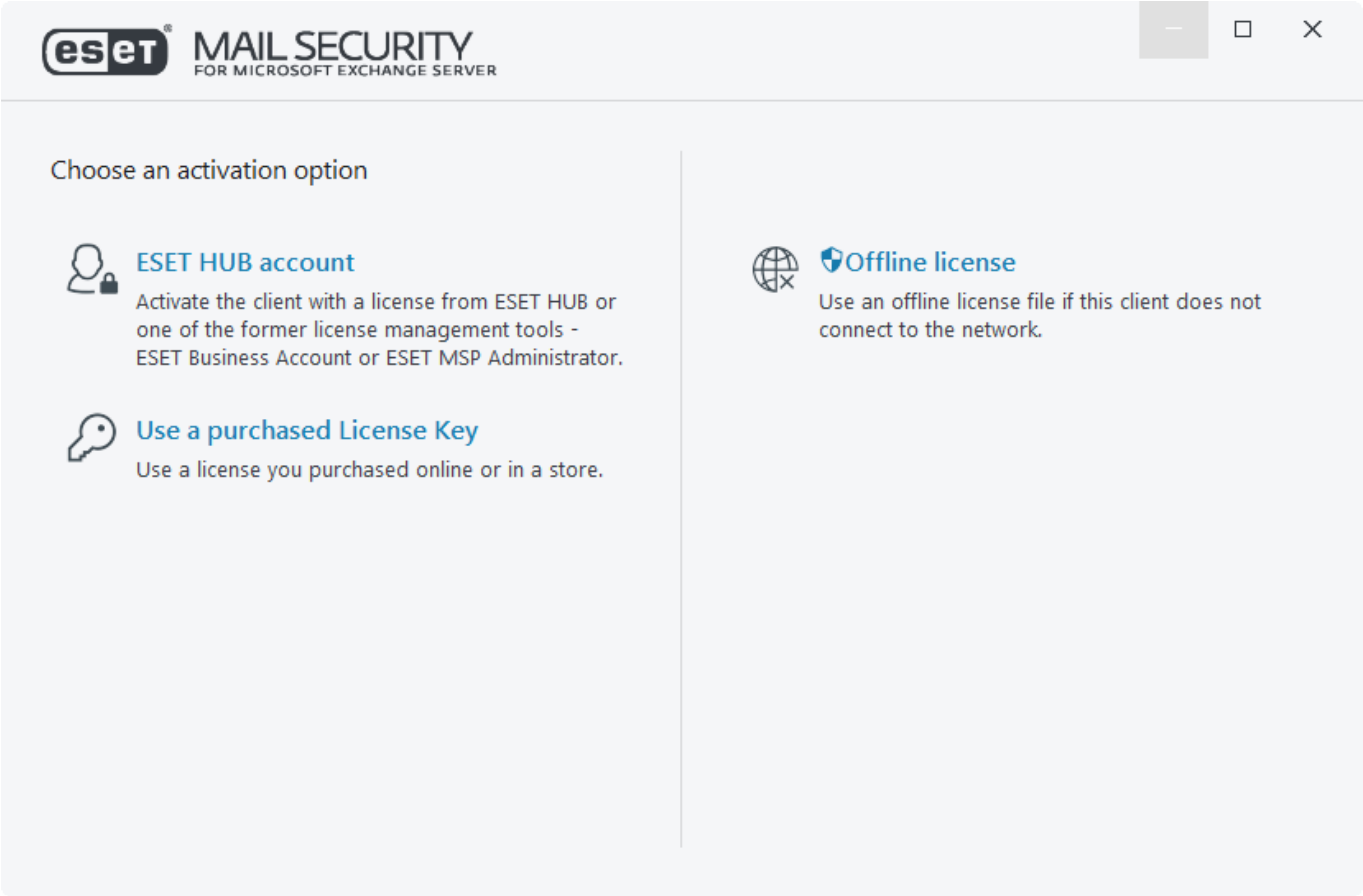
Cambiar	Valor
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0: Deshabilitado, 1: Habilitado
`CFG_LIVEGRID_ENABLED=1/0`	0: Deshabilitado, 1: Habilitado
`FIRSTSCAN_ENABLE=1/0`	0: Deshabilitar, 1: Habilitar
`CFG_PROXY_ENABLED=0/1`	0: Deshabilitado, 1: Habilitado
`CFG_PROXY_ADDRESS=<ip>`	Dirección IP de proxy
`CFG_PROXY_PORT=<port>`	Número de puerto de proxy
`CFG_PROXY_USERNAME=<user>`	Nombre de usuario para la autenticación
`CFG_PROXY_PASSWORD=<pass>`	Contraseña para la autenticación

Parámetros del idioma: Idioma del producto (debe especificar ambos parámetros)

Cambiar	Valor
`PRODUCT_LANG=`	LCID Decimal (Id. de configuración regional), por ejemplo 1033 para English - United States, consulte la lista de códigos de idiomas.
`PRODUCT_LANG_CODE=`	La cadena LCID (Nombre de referencia cultural) en minúscula, por ejemplo en-us para English - United States, consulte la lista de códigos de idiomas.

Activación de producto

Cuando la instalación se complete, se le solicitará que active el producto.



Puede usar cualquiera de los siguientes métodos para activar ESET Mail Security:

Una clave de licencia que compró

Escriba o copie y pegue su clave de licencia emitida por ESET en el campo **Clave de licencia** y haga clic en **Continuar**. Escriba la clave de licencia tal como está, incluidos los guiones. Si copia y pega la licencia, asegúrese de no seleccionar accidentalmente ningún espacio adicional alrededor del texto.

Cuenta de ESET HUB

Debe crear una cuenta de ESET HUB. ESET HUB es una puerta de enlace central a la plataforma de seguridad unificada ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Cree una nueva cuenta si no tiene una cuenta registrada en ESET Hub.

Archivo de Licencia sin conexión

Es un archivo generado automáticamente que se transfiere al producto de ESET. Su licencia sin conexión se genera desde el portal de licencias y se usa en los entornos donde la aplicación no puede conectarse con la autoridad otorgante.

Haga clic en **Activar más tarde** con ESET PROTECT si su equipo es miembro de una red administrada y su administrador realizará la activación remota a través de ESET PROTECT. También puede usar esta opción para activar un cliente más adelante.

Seleccione **Ayuda y soporte** > **Cambiar la licencia** en la ventana principal del programa para administrar la información de su licencia en cualquier momento. Verá la ID de la licencia pública usada para identificar su producto y licencia. El nombre de usuario bajo el cual su equipo está registrado se almacena en la sección Acerca de que puede visualizar al hacer clic con el botón derecho en el icono de la Área de notificación de Windows.

Tras activar correctamente ESET Mail Security, se abrirá la ventana principal del programa y se mostrará el estado actual en la página Supervisión. Deberá prestar atención al principio; por ejemplo, se le preguntará si desea ser parte de ESET LiveGrid®.

La ventana principal también mostrará notificaciones acerca de otros elementos, como actualizaciones de sistema (Windows Updates) o actualizaciones del motor de detección. Una vez resuelto todo lo que requiere atención, el estado de supervisión cambiará a color verde y mostrará el estado **Está protegido**.

También puede activar su producto desde el menú principal en **Ayuda y soporte** > **Activar el producto** o estado de **Seguimiento** > **El producto no está activado**.

> ESET PROTECT puede activar equipos de clientes de manera silenciosa usando licencias que el administrador pone a disposición.

La activación se completó correctamente

ESET Mail Security ya está activado. A partir de este momento, ESET Mail Security recibirá actualizaciones regularmente para identificar las últimas amenazas y mantener su equipo seguro.

Haga clic en **Listo** para finalizar con la activación del producto.

Cuenta de ESET HUB

ESET HUB es una puerta de enlace central a la plataforma de seguridad unificada ESET PROTECT. Proporciona administración centralizada de identidades, suscripciones y usuarios para todos los módulos de la plataforma ESET. Active ESET Mail Security con herramientas de administración de licencias, ESET Business Account o ESET MSP Administrator. Cree una nueva cuenta si no tiene una cuenta registrada en ESET Hub.

Falla en la activación

Si la activación de ESET Mail Security no se realizó correctamente, las siguientes situaciones son posibles:

- La clave de licencia ya está en uso
- Clave de licencia no válida: error en el formulario de activación del producto
- Debe corregir la información no válida o proporcionar la faltante
- Error al comunicarse con la base de datos de activación: inténtelo de nuevo en 15 minutos
- La conexión con los servidores de activación de ESET no está disponible o está desactivada

Asegúrese de haber ingresado la **Clave de licencia** correcta o de haber adjuntado una **Licencia sin conexión** e intente activar de nuevo.

Si no puede realizar la activación, consulte el asistente para la resolución de problemas de activación.

Licencia

Se le pedirá que seleccione una licencia de ESET Mail Security asociada a su cuenta. Haga clic en **Continuar** para seguir adelante con la activación.

Actualizar a la versión más reciente

Las versiones nuevas de ESET Mail Security se emiten para brindar mejoras del programa o para resolver problemas que no se pueden solucionar mediante la actualización automática de los módulos del programa.

Métodos de actualización:

- **Desinstalar / Instalar** - Remover la versión anterior antes de instalar la nueva versión. Descargar la última versión de ESET Mail Security Exportar la configuración de su configuración existenteESET Mail Security en caso de que desee conservar dicha configuración. Desinstalar ESET Mail Security y reiniciar el servidor. Realizar una nueva instalación con el instalador que ha descargado. Importar la configuración para cargar su configuración. Le recomendamos este procedimiento si tiene un único servidor en ejecución ESET Mail Security.

- **En sitio** - Un método actualizado sin remover la versión existente e instalar la nueva ESET Mail Security por encima.

Es necesario que no tenga **actualizaciones pendientes de Windows** en su servidor, así como ningún **reinicio pendiente** debido a las actualizaciones de Windows o por otro motivo. Si intenta una actualización en sitio con Actualizaciones de Windows o reinicio pendientes, la versión existente de ESET Mail Security puede no ser eliminada correctamente. También experimentará problemas si luego decide eliminar la versión anterior de ESET Mail Security de forma manual.

Será necesario reiniciar el servidor durante la actualización de ESET Mail Security.

- Remoto: para usar en entornos de redes grandes gestionados por ESET PROTECT. Este es básicamente un método de actualización limpio, pero realizado de forma remota. Es útil si tiene varios servidores ejecutando ESET Mail Security.

- Asistente de clúster de ESET: también puede usarse como método de actualización. Recomendamos usar este método para dos o más servidores con ESET Mail Security. Este es básicamente un método de actualización en sitio, pero realizado mediante el Clúster de ESET. Una vez finalizada la actualización, puede continuar usando el clúster de ESET y aprovechar sus funciones.

Las siguientes configuraciones se conservan de las versiones anteriores de ESET Mail Security:

- Configuración general de ESET Mail Security.

Configuración de la protección antispam:

- Todas las configuraciones que sean idénticas en las versiones anteriores, las configuraciones nuevas

utilizarán los valores predeterminados.

- Entradas en las listas blancas y negras.

> Una vez que haya actualizado ESET Mail Security, le recomendamos revisar todas las configuraciones para asegurarse de que estén correctamente configuradas y según sus necesidades.

Actualización mediante ESET PROTECT

ESET PROTECT le permite actualizar varios servidores que ejecuten una versión ESET Mail Security anterior. Este método tiene la ventaja de actualizar muchos servidores simultáneamente y garantizar que cada uno ESET Mail Security se configure de forma idéntica (si se desea).

El procedimiento incluye las siguientes fases:

- **Actualice el primer servidor** manualmente mediante la instalación de la versión ESET Mail Security más reciente sobre la versión existente para conservar su configuración, incluidas las reglas y varias listas blancas/negras. Esta fase se realiza a nivel local en el servidor que ejecuta ESET Mail Security.

- **Solicite la configuración** del recientemente configurado ESET Mail Security a la versión 7.x y convierta a la política en ESET PROTECT. La política se aplicará más tarde a todos los servidores actualizados. Esta fase y las fases siguientes a continuación se llevan a cabo de manera remota con ESET PROTECT.

- **Ejecute la tarea de desinstalación de software** en todos los servidores que ejecutan la versión ESET Mail Security anterior.

- **Ejecute la tarea Instalación del software** en todos los servidores en los que desee la versión ESET Mail Security más reciente.

- **Asigne la política de configuración** a todos los servidores que ejecutan la versión ESET Mail Security más reciente.

Siga las instrucciones indicadas a continuación para actualizar a través de ESET PROTECT

1. Inicie sesión en uno de los servidores que ejecuta ESET Mail Security y actualícelo mediante la descarga e instalación de la última versión respecto de la existente. Siga los pasos de instalación regulares. Durante ESET Mail Security la instalación se conservan sus configuraciones originales.

2. Abra la ESET PROTECTConsola Web de , elija un equipo cliente dentro de los grupos estáticos o dinámicos y haga clic en **Mostrar detalles**.

3. Seleccione la pestaña Configuración y haga clic en el botón **Solicitar configuración** para recopilar las configuraciones de su producto administrado. Tenga en cuenta que este proceso toma un tiempo. Cuando aparezca en la lista la configuración más reciente, haga clic en **Producto de seguridad** y elija **Configuración abierta**.

4. Haga clic en el botón **Convertir en política** para crear una política de configuración. Ingrese el **Nombre** de una nueva política y haga clic en **Finalizar**.

5. Seleccione **Tareas de clientes** y elija la tarea Desinstalación de software. Al crear la tarea de desinstalación, le recomendamos reiniciar el servidor después de la desinstalación; para ello, seleccione la casilla de

verificación **Reiniciar automáticamente cuando fuera necesario**. Una vez creada la tarea, agregue todos los equipos de destino que desee para la desinstalación.

6. Asegúrese de que ESET Mail Security se desinstale de todos los destinos.

7. Cree la tarea Instalación de software para instalar la versión ESET Mail Security más reciente de en todos los destinos deseados.

8. **Asigne la política de configuración** a todos los servidores que ejecutan ESET Mail Security, idealmente en un grupo.

Actualización mediante el clúster de ESET

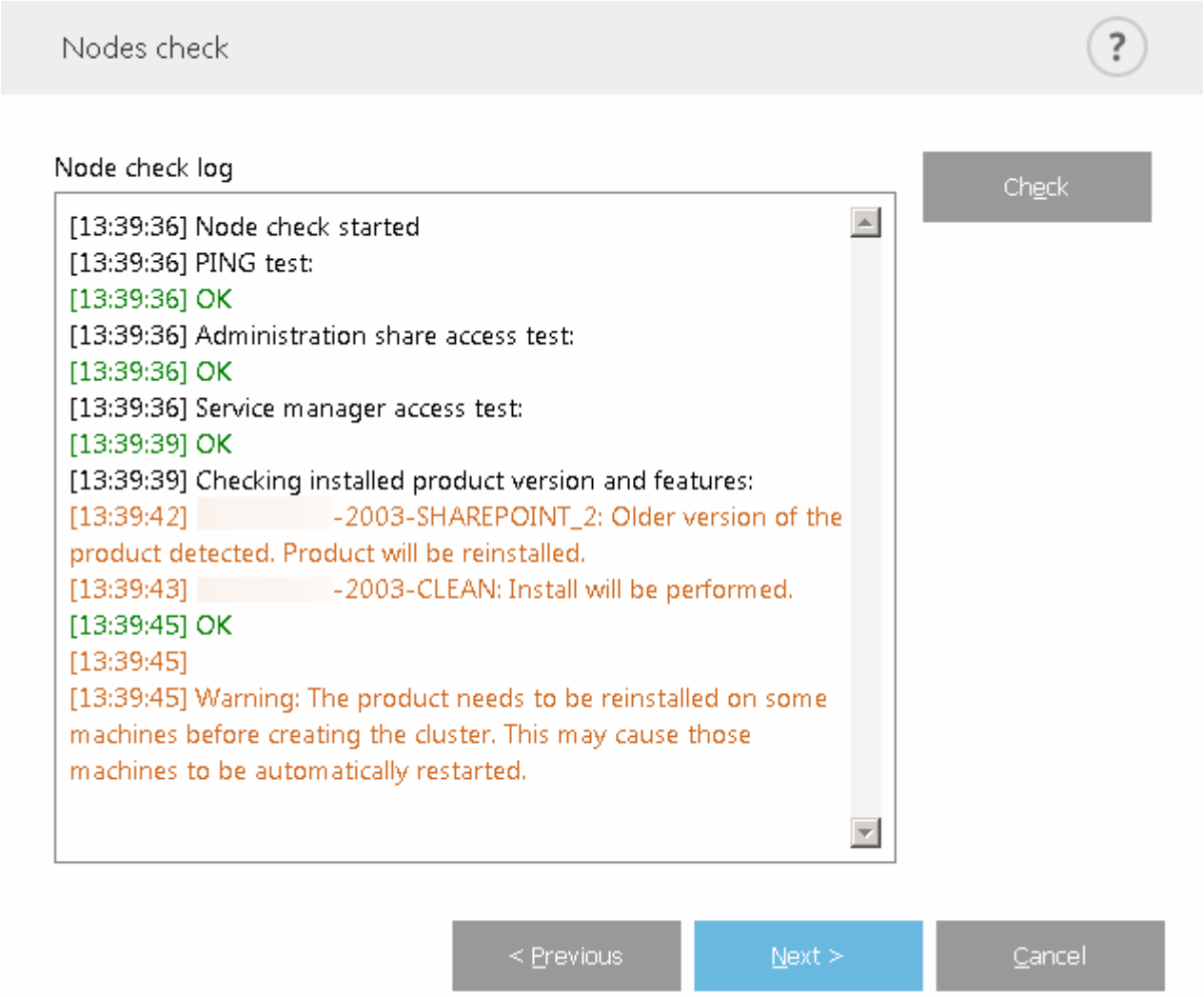
La creación de un clúster de ESET le permite actualizar varios servidores con versiones anteriores de ESET Mail Security. Recomendamos usar el método de clúster de ESET si tiene 2 o más servidores con ESET Mail Security en su entorno. Otro beneficio de este método de actualización es que puede continuar usando el Clúster de ESET para que la configuración de ESET Mail Security se sincronice en todos los nodos de los miembros.

Siga los siguientes pasos para actualizar con este método:

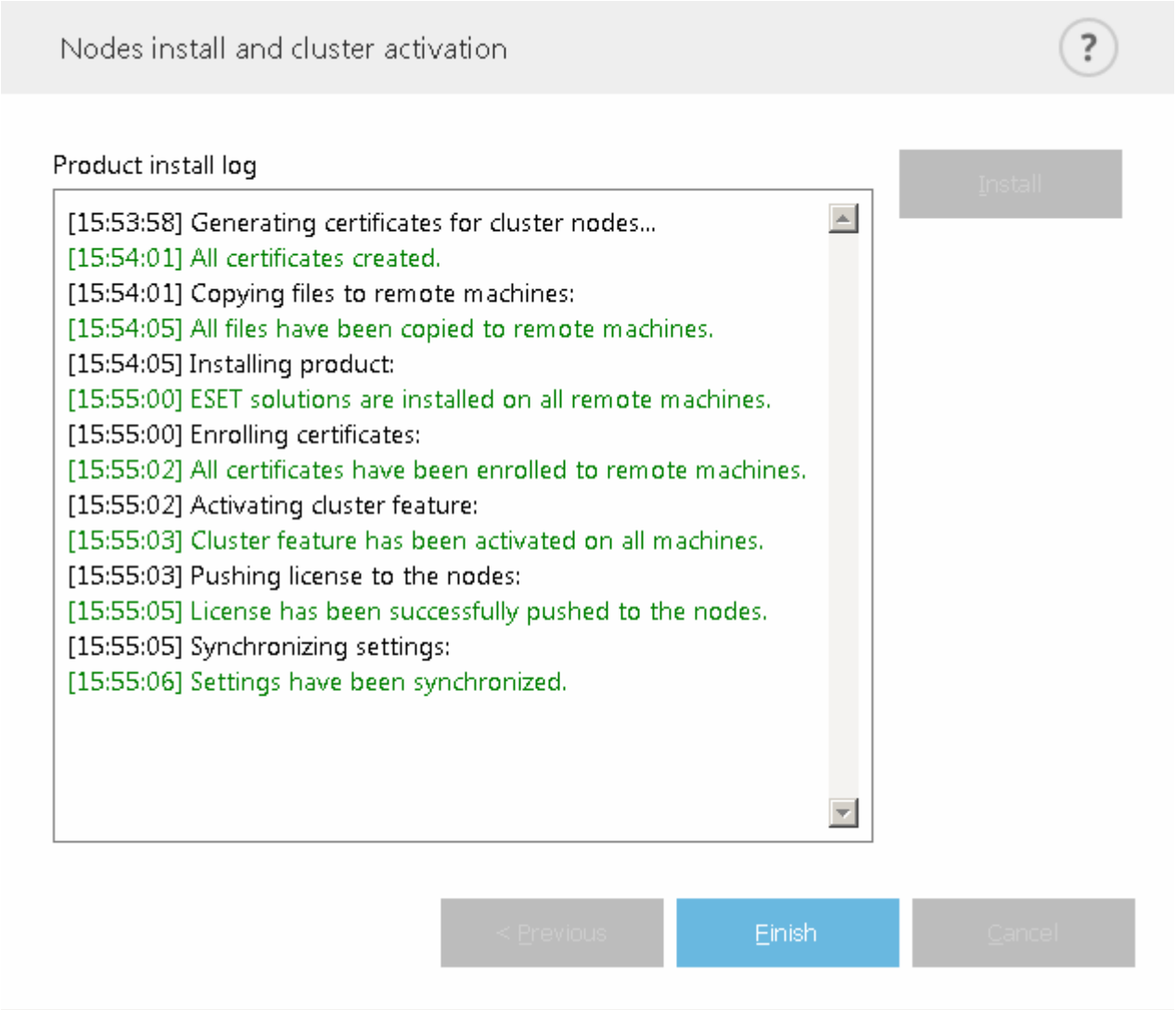
1. Inicie sesión en uno de los servidores que ejecuta ESET Mail Security y actualícelo mediante la descarga e instalación de la última versión respecto de la existente. Siga los pasos de instalación regular. La configuración original de su ESET Mail Security anterior se preservará durante la instalación.

2. Ejecute el asistente del clúster de ESET y agregue los nodos del clúster (servidores en los que quiere actualizar ESET Mail Security). Si se requiere, puede agregar otros servidores que aún no ejecutan ESET Mail Security (se llevará a cabo una instalación en ellos). Le recomendamos dejar la configuración predeterminada al especificar el nombre del clúster y el tipo de instalación (asegúrese de tener marcada la opción Enviar licencia a nodos sin un producto activado).

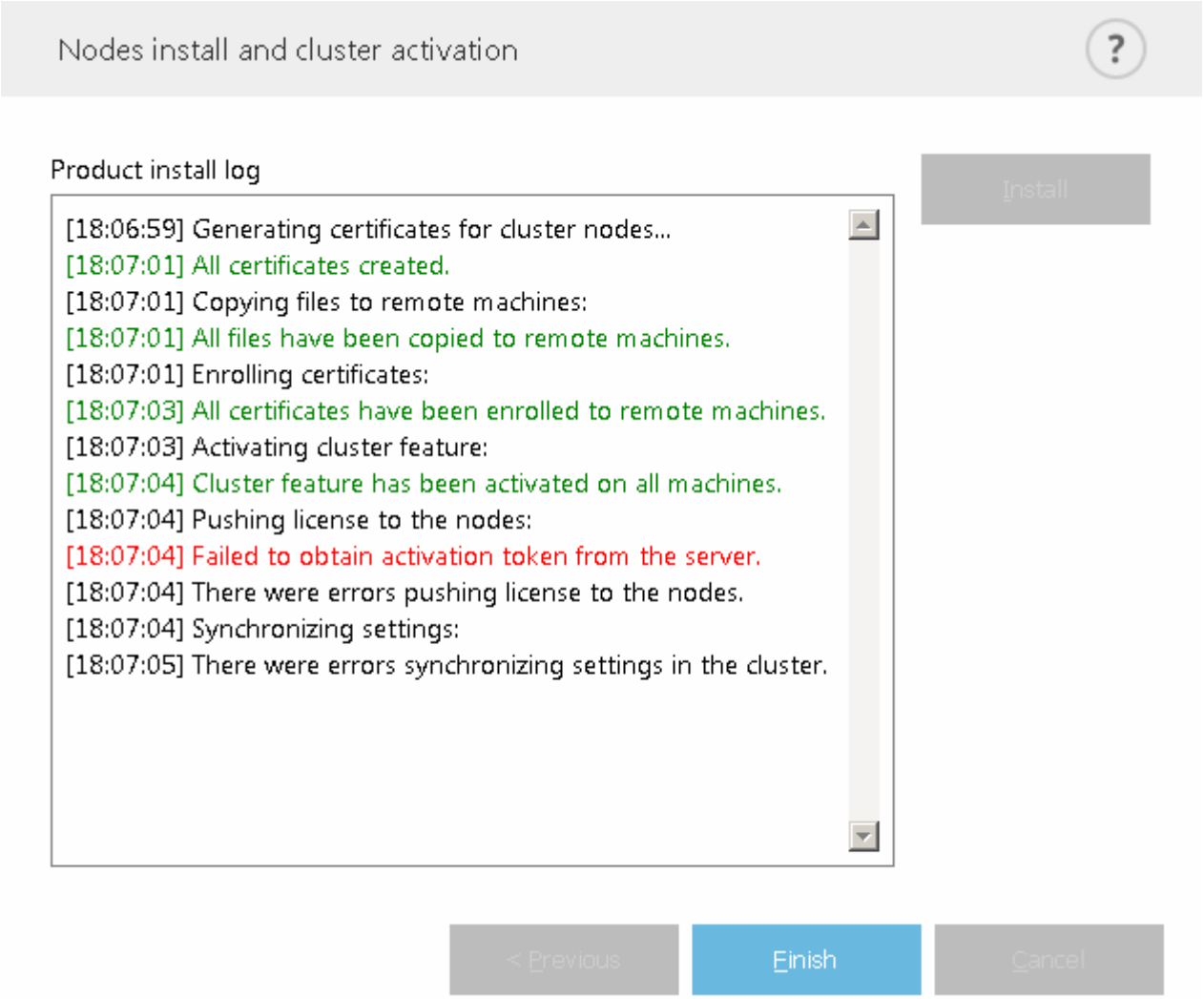
3. Revise la pantalla Registro de verificación de nodos. Enumera los servidores con versiones anteriores del producto y el producto se reinstalará. ESET Mail Security también se instalará en todo servicio agregado donde no se encuentre instalado.



4. La pantalla **Instalación de nodos y activación del clúster** mostrará el progreso de la instalación. Cuando se complete correctamente la instalación, debería finalizar con resultados similares a estos:



Si su red o DNS no está configurada correctamente, podrá recibir un mensaje de error que diga **Error al obtener el token de activación del servidor**. Intente ejecutar nuevamente el asistente del clúster de ESET. Destruirá el clúster y generará uno nuevo (sin reinstalar el producto) y esta vez la activación debe finalizar correctamente. Si el problema persiste, verifique su configuración de DNS y red.



Instalación en un entorno de clúster

Puede implementar ESET Mail Security en un entorno de clúster (por ejemplo un clúster de conmutación por error). Le recomendamos instalar ESET Mail Security en un nodo activo y luego redistribuir la instalación en nodos pasivos usando la función Clúster de ESET de ESET Mail Security. Además de la instalación, el clúster de ESET actuará como replicación de la configuración de ESET Mail Security para garantizar la consistencia entre los nodos de clúster necesarios para el funcionamiento correcto.

Terminal Server

Si está instalando ESET Mail Security en un Servidor Windows que funciona como Terminal Server, quizás deba deshabilitar la IGU de ESET Mail Security para evitar que se ejecute cada vez que ingresa un usuario. Para ver los pasos específicos para deshabilitarla, consulte el capítulo Deshabilitación de la interfaz gráfica del usuario en Terminal Server.

Multiservidor/entorno DAG

ESET Mail Security es compatible con entornos multiservidor. Si su estructura está compuesta por múltiples servidores, por ejemplo, grupo de disponibilidad de bases de datos (DAG), puede instalar ESET Mail Security en

cada uno de los roles de Exchange Server con buzón de correo.

La manera más sencilla es instalar ESET Mail Security en todos los servidores haciendo uso de ESET Cluster. También, le recomendamos habilitar la opción Use ESET Cluster para almacenar todos los mensajes en cuarentena en un nodo en la configuración Cuarentena de correo. Si planea usar la creación de listas grises, habilite la opción Sincronizar las bases de datos de creación de listas grises en el clúster de ESET.

Primeros pasos

Los siguientes temas lo ayudarán a empezar ESET Mail Security.

Supervisión

Esta es una descripción rápida del ESET Mail Securityestado actual, en la que puede ver fácilmente si algún problema requiere su atención.

Administrado a través de ESET PROTECT

Puede usar ESET PROTECT para administrar de forma remota ESET Mail Security. La siguiente parte debería ayudarlo a empezar con ESET Mail Security.

Tareas posteriores a la instalación

Tiene como finalidad ayudarle con la configuración inicial.

Tareas posteriores a la instalación

Las siguientes son tares recomendadas que cubren la configuración inicial de ESET Mail Security.

Tema	Descripción
Activación del producto	Asegúrese de que ESET Mail Security está activado. Puede realizar la activación de varias maneras diferentes.
Actualización	Después de activar el producto, la actualización del módulo se ejecuta automáticamente. Verifique el estado de la actualización para ver su la actualización fue exitosa.
Administrador de la cuarentena de correo	Conozca al administrador de cuarentena de correo, al que se puede acceder desde la ventana principal del programa. Esta función le permite administrar mensajes en cuarentena tales como spam, archivos adjuntos infectados con malware, mensajes de phishing y mensajes filtrados por reglas. Podrá ver los detalles de cada mensaje y actuar (liberar o eliminar).
Interfaz web de la cuarentena de correos	La interfaz web de la Cuarentena de correo es un administrador alternativo de la Cuarentena de correo que le permite administrar remotamente los elementos en cuarentena. La interfaz web de cuarentena de correo también permite a los usuarios (destinatarios de correo electrónico) administrar sus mensajes en cuarentena. Se puede notificar a los usuarios acerca del contenido en cuarentena con los informes de cuarentena de correo enviados por correo electrónico. Le recomendamos configurar los informes.
Informes de la cuarentena del correo	Crear una tarea programada para enviar informes de cuarentena de correo a usted mismo y a usuarios seleccionados para permitirles liberar (entregar) determinados tipos de mensajes falsos positivos y manejar el contenido en cuarentena mediante la interfaz de la Web de cuarentena de correo (visor en línea). Los usuarios pueden acceder a la interfaz web si hacen clic en el enlace provisto en los informes de cuarentena de correo y si inician sesión con las credenciales de dominio.

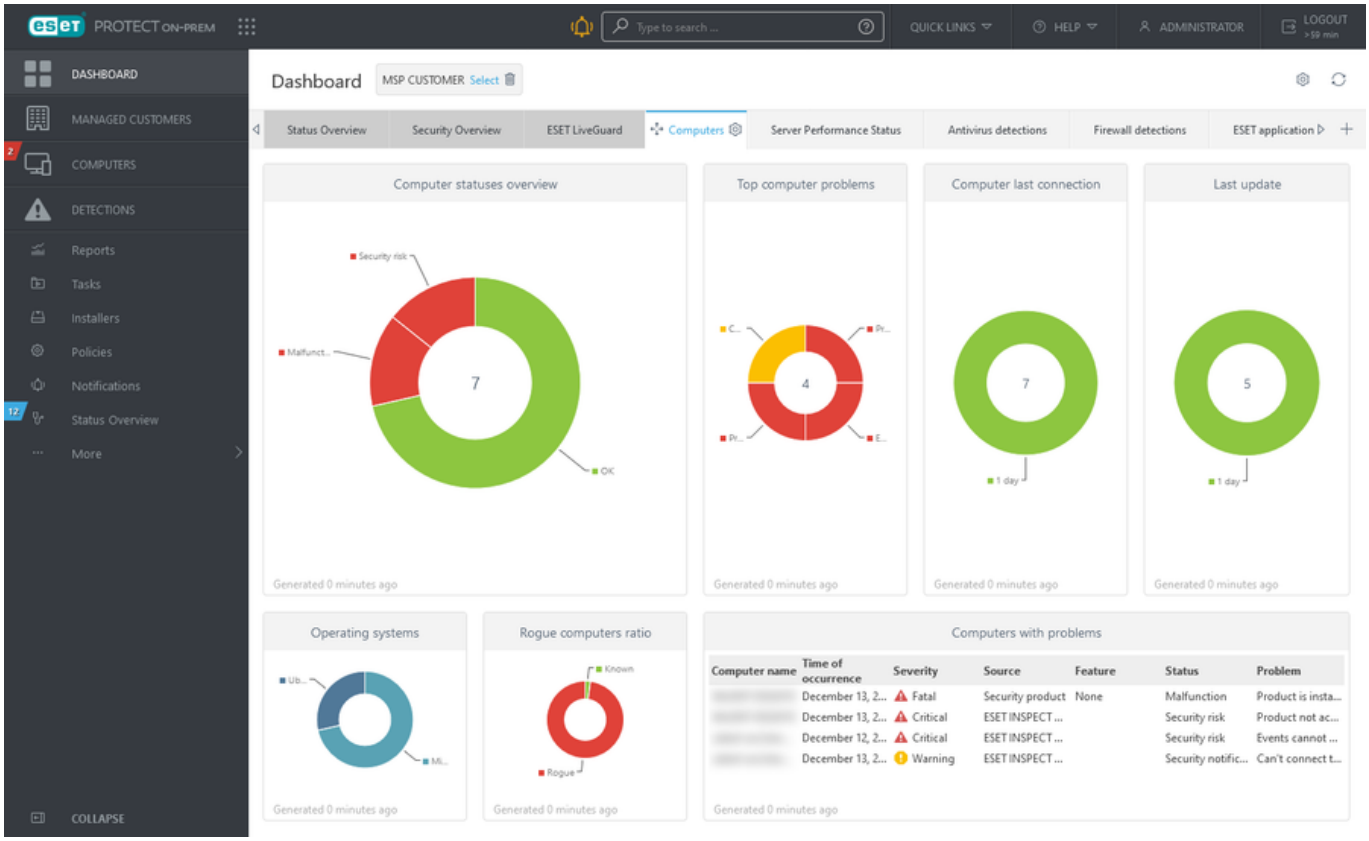
Tema	Descripción
Antispam - Filtro y verificación	El antispam es una funcionalidad basada en la nube sofisticada que evita que los usuarios (destinatarios de correo electrónico) reciban spam. Le recomendamos utilizar el filtrado y la verificación y agregar sus direcciones IP locales a la lista de IP ignorada. Las direcciones IP dentro de la infraestructura de red serán ignoradas durante la clasificación. Puede configurar y administrar el resto de las listas aprobadas, bloqueadas e ignoradas para personalizar el filtrado y la verificación. También puede habilitar las listas grises si decide usar esta función.
Reglas	Una función poderosa le permite filtrar mensajes de correo electrónico basados en condiciones y acciones definidas. Utilice reglas predefinidas (modifíquelas si fuera necesario) para crear reglas nuevas y personalizadas que se adapten a sus necesidades. Las reglas se pueden configurar para todas las capas de protección (Protección de transporte de correo, Protección de base de datos de buzón o Exploración de la base de datos del buzón de correo a petición).
Prueba Antivirus	Verifique que la protección antivirus funciona correctamente.
Prueba antispam	Verifique que la protección antispam funciona correctamente.
Prueba anti-phishing	Verifique que la protección anti-phishing funcione correctamente.

Administrado a través de ESET PROTECT

ESET PROTECT es una aplicación que le permite administrar los productos de ESET en un entorno en red desde una ubicación central. El sistema de administración de tareas ESET PROTECT le permite instalar soluciones de seguridad ESET en equipos remotos y responder rápidamente a nuevos problemas y amenazas.

El sistema de administración de tareas de ESET PROTECT le permite instalar las soluciones de seguridad de ESET en equipos remotos y responder rápidamente a los nuevos problemas y las nuevas amenazas.

Las soluciones de seguridad ESET son compatibles con redes que incluyen varios tipos de plataformas. Su red puede incluir una combinación de los sistemas operativos actuales de Microsoft, basados en Linux, macOS y móviles.



Para más información sobre , visite ESET PROTECTAyuda en línea.

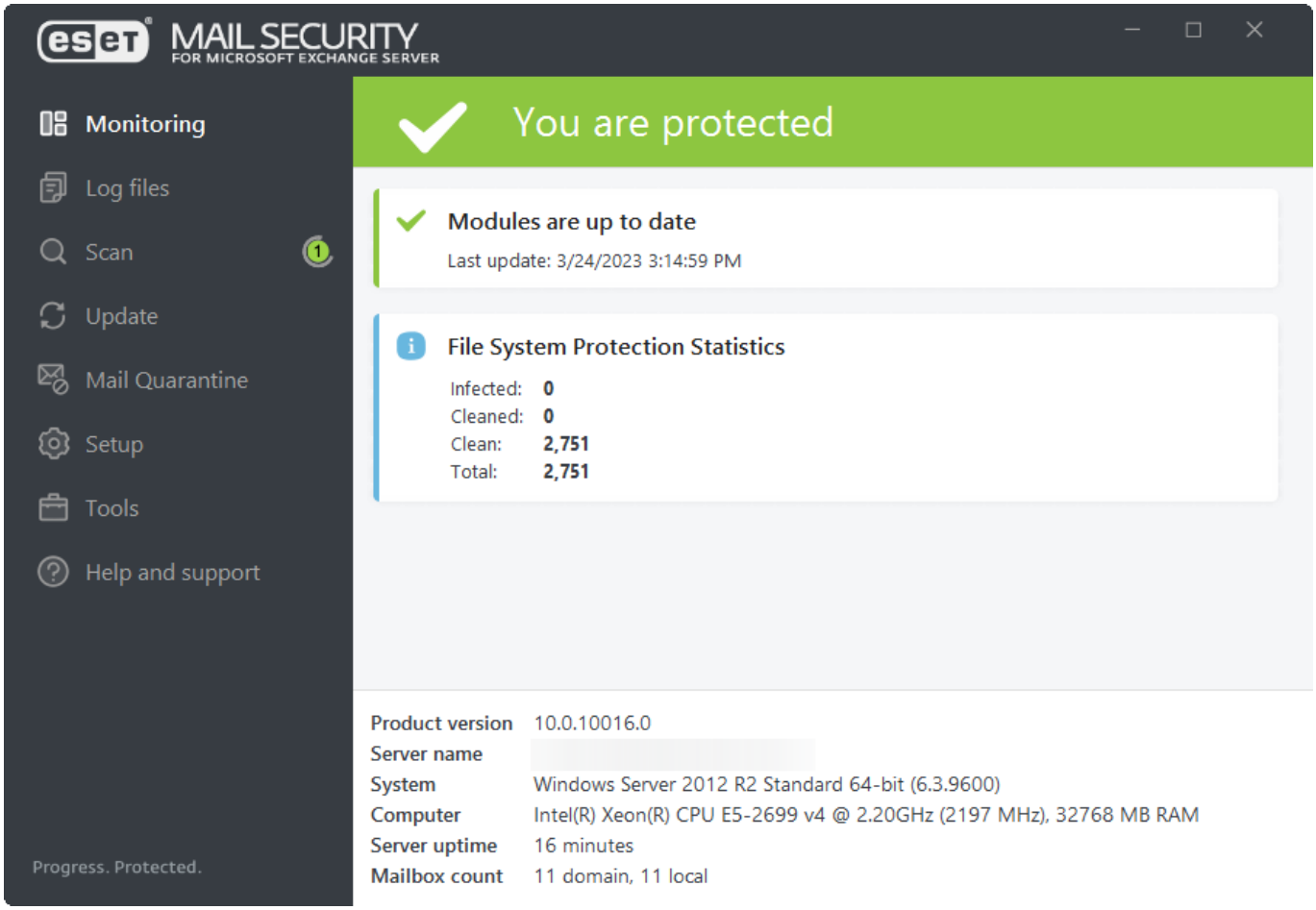
Supervisión

El estado de protección que se muestra en la sección **Monitoreo** le informa acerca del nivel de protección actual de su computadora. Se mostrará un resumen de estado del funcionamiento de los módulos de ESET Mail Security en la ventana principal.

El estado verde de **Usted está protegido** indica que la protección máxima está garantizada.

El ícono rojo indica que existen problemas críticos; la protección máxima de su computadora no está garantizada. Los detalles del mensaje de error deberían ofrecer una mejor comprensión del estado actual. Si no puede solucionar un problema, busque la Base de conocimientos de ESET. Si sigue necesitando asistencia, puede Enviar una solicitud de soporte. El servicio de atención al cliente de ESET responderá rápidamente a sus preguntas y lo ayudará a encontrar una resolución. Para obtener una lista completa de estados, abra las **notificaciones de Configuración avanzada** (**F5**) > > estados de aplicación y haga clic en **Editar**.

El ícono naranja indica que su producto ESET requiere atención para un problema que no es crítico.



Se asigna una marca de verificación verde a los módulos que funcionan adecuadamente. Se asigna un signo de exclamación rojo o una notificación naranja a los módulos que no son completamente funcionales. Se muestra la información adicional sobre el módulo en el sector superior de la ventana. También se muestra la solución sugerida para reparar el módulo.

Para cambiar el estado de un módulo individual, haga clic en Configuración en el menú principal y luego en el módulo deseado.

La página de Control también contiene información sobre su sistema, incluyendo:

- Versión del producto: número de versión de ESET Mail Security.
- Nombre del servidor - nombre del host del equipo o FQDN.
- Sistema: detalles del sistema operativo.
- Equipo: detalles del hardware.
- Tiempo de actividad total del servidor: muestra cuánto tiempo ha estado en actividad en sistema, básicamente es lo opuesto a tiempo de inactividad.

Total del buzón de correo

ESET Mail Security detecta la cantidad de buzones de entrada y muestra el contador de acuerdo a la detección:

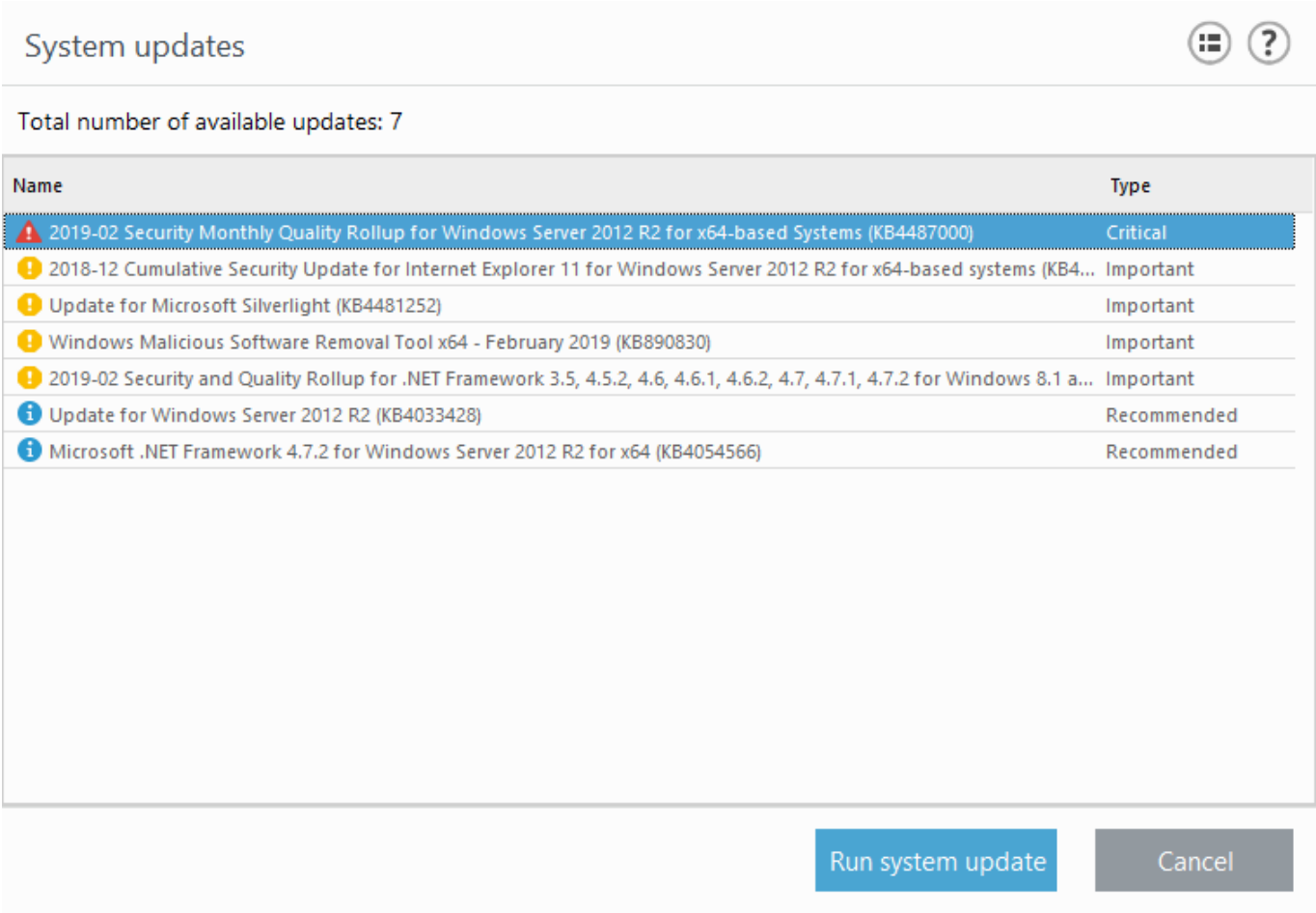
- **Dominio**: contador de todos los buzones de entrada en un dominio en particular al que pertenece Exchange Server. Este recuento también se aplica a un entorno DAG y su número total de buzones.

- **Local**: refleja el número de buzones de Exchange Server con ESET Mail Security instalado. Si el servidor pertenece a un DAG, este número es el número de buzones almacenados en Exchange Server local a partir del recuento total de dominios.

Si no puede solucionar el problema mediante las sugerencias recomendadas, haga clic en **Ayuda y soporte** para acceder a los archivos de ayuda o buscar en la base de conocimiento de ESET . Si sigue necesitando asistencia, puede Enviar una solicitud de soporte. El servicio de atención al cliente de ESET responderá rápidamente a sus preguntas y lo ayudará a encontrar una resolución.

Actualización de Windows disponible

La ventana de actualizaciones del sistema muestra la lista de actualizaciones disponibles que ya están preparadas para su descarga e instalación. El nivel de prioridad de la actualización aparece junto al nombre de la actualización. Haga un clic con el botón secundario en cualquier línea de actualización y luego haga clic en **Más información** para abrir una ventana con información adicional:



Haga clic en **Ejecutar la actualización del sistema** para abrir **Actualización de Windows** y seguir adelante con las actualizaciones del sistema.

Aislamiento de red

ESET Mail Security le proporciona una opción de aislamiento de red para bloquear la conexión de red del servidor. En algunos escenarios extremos, puede que quiera aislar un servidor de la red como medida preventiva. Por ejemplo, si descubre que el servidor se infectó con un malware o que la máquina se expuso de alguna otra

manera.

Al activar el aislamiento de red, todo el tráfico de red queda bloqueado, excepto lo siguiente:

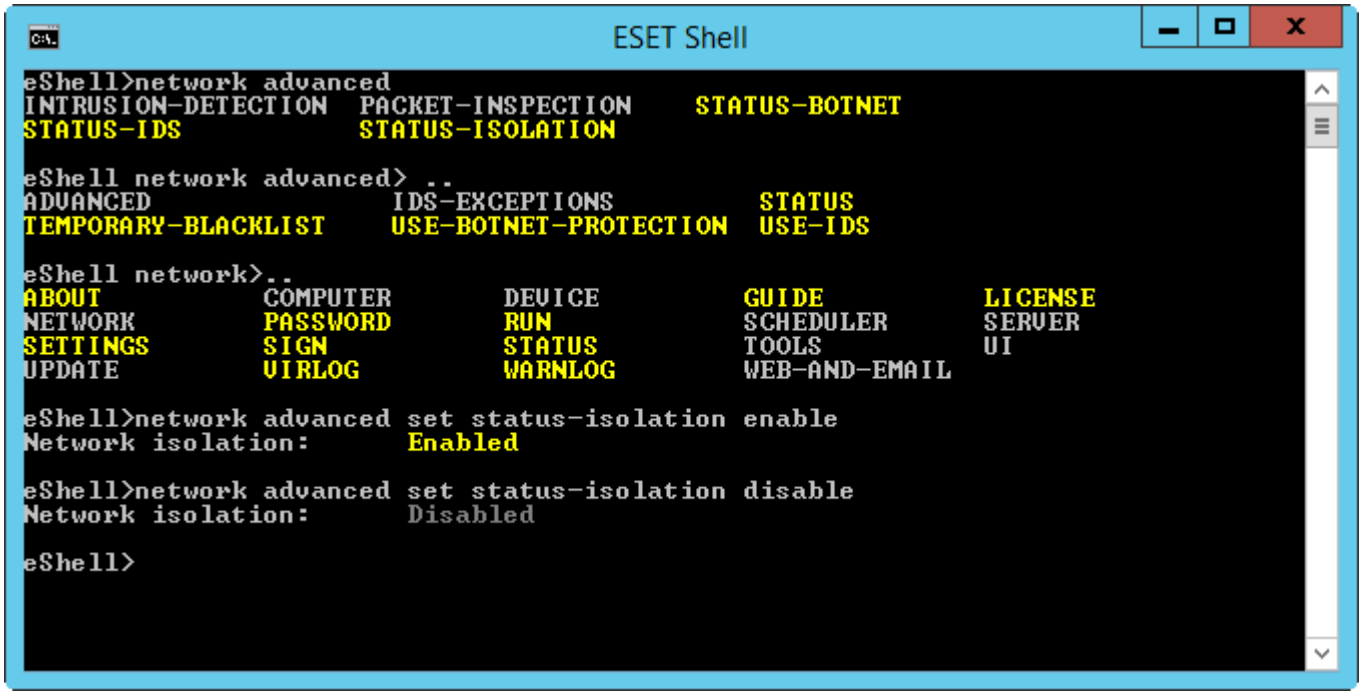
- La conectividad al controlador de dominio permanece
- ESET Mail Security aún se puede comunicar
- Si está presente, ESET Management Agent y ESET Inspect Connector pueden comunicarse por la red

Activar y desactivar el aislamiento de red mediante el comando eShell o la tarea del cliente ESET PROTECT.

eShell

En modo interactivo:

- Activar aislamiento de la red: `network advanced set status-isolation enable`
- Desactivar aislamiento de la red: `network advanced set status-isolation disable`



Como alternativa, puede crear y ejecutar un archivo por lotes con el modo Batch/Script.

ESET PROTECT

- Activar aislamiento de la red por tarea del cliente.
- Desactivar aislamiento de red por tarea del cliente.

Cuando el aislamiento de red está activado, el estado de ESET Mail Security cambia al color rojo con el mensaje **Acceso a la red bloqueado**.

Uso de ESET Mail Security

Esta sección contiene una descripción detallada de la interfaz de usuario del programa, y tiene por objeto explicar el uso de su ESET Mail Security.

La interfaz de usuario le permite acceder de manera rápida a las características más usadas:

- Supervisión
- Archivos de registro
- Exploración
- Actualización
- Cuarentena de correo
- Configuración
- Herramientas

Exploración

El módulo de exploración a petición es una parte importante de ESET Mail Security. Se usa para realizar la exploración de los archivos y las carpetas del equipo. Para garantizar la seguridad de su red, es esencial que las exploraciones del equipo no se ejecuten solo cuando existen sospechas de una infección, sino en forma habitual como parte de una medida de seguridad de rutina.

Recomendamos que realice exploraciones profundas de manera regular (por ejemplo, una vez al mes) en su sistema para detectar los virus que no haya detectado la Protección del sistema de archivos en tiempo real. Esto puede ocurrir si se introduce una amenaza cuando la Protección del sistema de archivos en tiempo real se deshabilitó, si el motor de detección era obsoleto o si el archivo no se detectó como virus cuando se guardó en el disco.

Seleccione exploraciones a petición disponibles para ESET Mail Security:

Exploración de la base de datos del buzón

Le permite ejecutar exploraciones de la base de datos a petición. Puede elegir Carpetas públicas, servidores de correo y buzón de correo para la exploración. Además, puede usar las Tareas programadas para ejecutar el explorador de la base de datos en un horario específico o en un evento.

> Si ejecuta Microsoft Exchange Server 2007, 2010, 2013 o 2016 puede elegir entre la Protección de la base de datos de correo electrónico y la Exploración de la base de datos a petición, solamente un tipo de protección puede estar activo a la vez. Si decide utilizar la Exploración de la base de datos a petición, deberá deshabilitar la integración de la Protección de la base de datos de correo electrónico en la Configuración avanzada del Servidor. De lo contrario, la Exploración de la base de datos a petición no estará disponible.

Exploración del buzón de Microsoft 365

Le permite explorar buzones de correo remotos en entornos híbridos de Microsoft 365.

Exploración de almacenamiento

Explora todas las carpetas compartidas dentro del servidor local. Si Exploración de almacenamiento no se encuentra disponible, significa que no hay carpetas compartidas en su servidor.

Explore el equipo

Permite iniciar rápidamente una exploración del equipo y desinfectar los archivos infectados sin necesidad de la intervención del usuario. La ventaja de la Exploración es su facilidad de uso y que no requiere una configuración detallada de la exploración. La exploración verifica todos los archivos en los discos locales y desinfecta o elimina en forma automática las infiltraciones detectadas. El nivel de desinfección está establecido automáticamente en el valor predeterminado. Para obtener información más detallada sobre los tipos de desinfección, consulte Desinfección.

> i Se recomienda ejecutar una exploración del equipo al menos una vez al mes. La exploración se puede configurar como una tarea programada.

Exploración personalizada

La exploración personalizada es una solución ideal si desea especificar los parámetros de exploración, tales como los objetos para explorar y los métodos de exploración. La ventaja de la exploración personalizada es la capacidad de configurar los parámetros detalladamente. Es posible guardar las configuraciones en perfiles de exploración definidos por el usuario, lo que resulta útil si la exploración se efectúa reiteradamente con el uso de los mismos parámetros.

Exploración de medios extraíbles

Es similar a la exploración inteligente: inicia rápidamente una exploración de los medios extraíbles (como CD/DVD/USB) que estén conectados al equipo. Puede ser útil cuando conecta al equipo una unidad flash USB y desea explorar sus contenidos en busca de malware y otras amenazas potenciales. Este tipo de exploración también puede iniciarse al hacer clic en Exploración personalizada, luego seleccionar Medios extraíbles del menú desplegable de Objetos para explorar y, por último, hacer clic en Explorar.

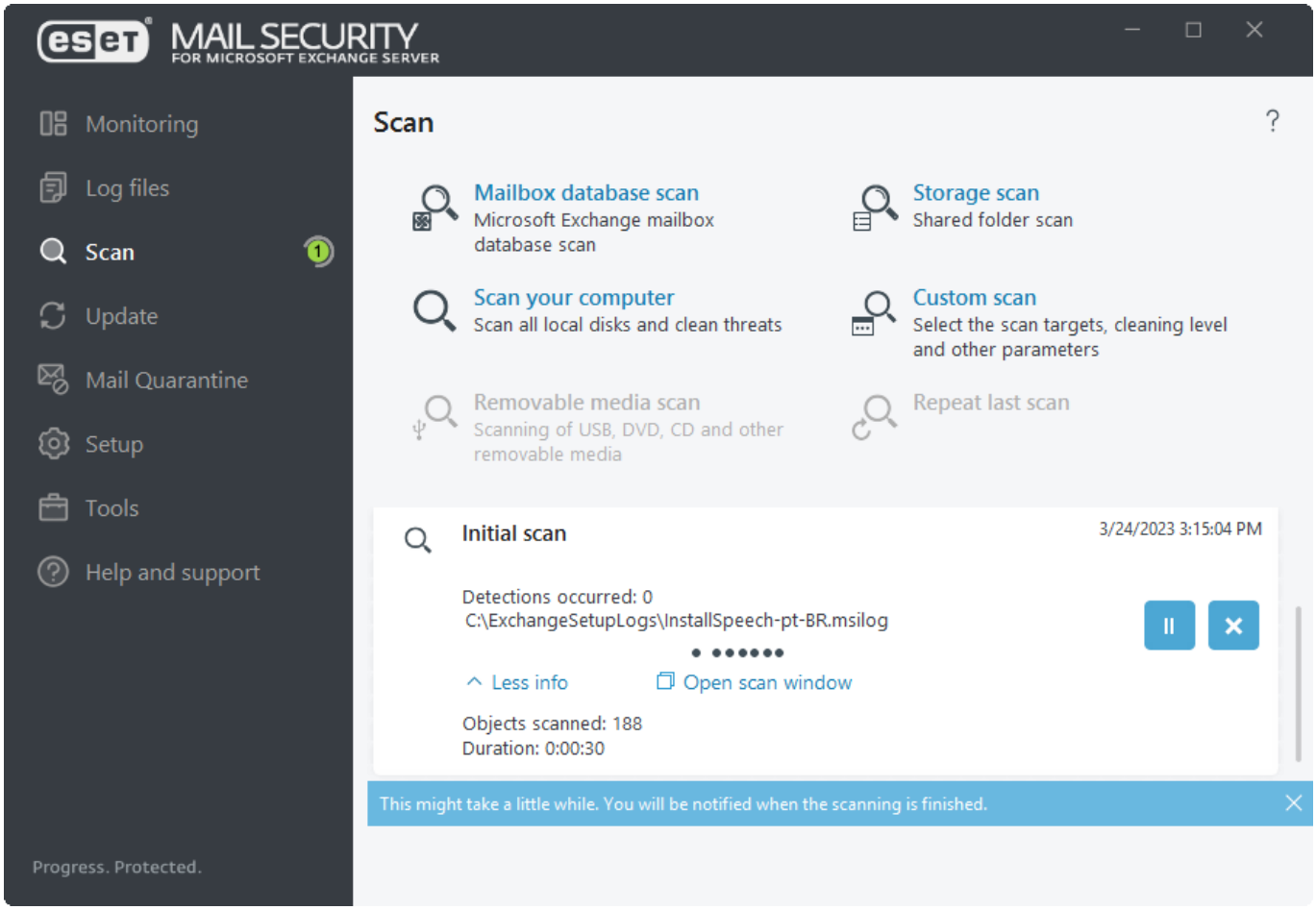
Exploración Hyper-V

Esta opción únicamente estará visible en el menú si el administrador de Hyper-V está instalado en el servidor que ejecuta ESET Mail Security. La exploración de Hyper-V permite explorar los discos de las máquinas virtuales (VM) en Microsoft Hyper-V Server sin la necesidad de tener instalado un “agente” en la VM en cuestión.

Repetir última exploración

Repite la última operación de exploración utilizando exactamente la misma configuración.

> i repita la última función de exploración no estará disponible si la Exploración de la base de datos a petición está presente.



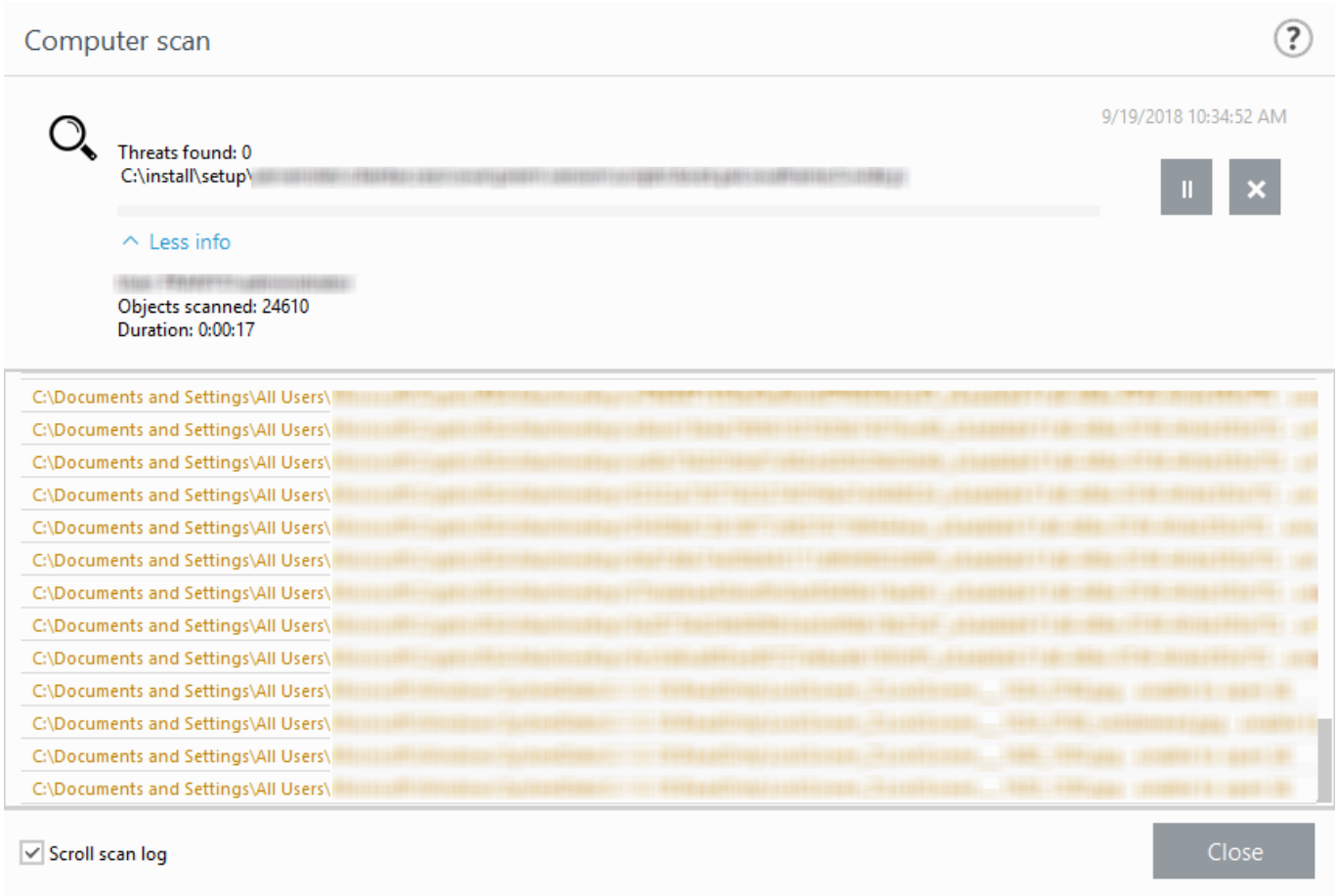
Puede utilizar las opciones y muestra más información sobre los estados de exploración:

Arrastrar y soltar archivos	También puede arrastrar y soltar archivos en la ventana de exploración de ESET Mail Security. Estos archivos se analizarán por virus de inmediato.
Descartar / Descartar todo	Descarta los mensajes.
Estados de exploraciones	Muestra el estado de la exploración inicial. Esta exploración finalizó o ha sido interrumpida por el usuario.
Mostrar registro	Muestra más información detallada.
Obtener más información	Durante la exploración puede ver detalles como el Usuario que ejecutó la exploración, la cantidad de Objetos explorados y la **Duración** de la exploración. Si se está ejecutando una Exploración de la base de datos a petición, muestra al usuario quién ejecutó la exploración, no la Cuenta de exploración de la base de datos real que se está usando para conectar a EWS (Servicios web de Exchange) durante el proceso de exploración.
Abrir ventanas de exploración	La ventana de progreso de la exploración muestra el estado actual de la exploración junto con información sobre la cantidad detectada de archivos con códigos maliciosos.

Ventana de exploración y registro de exploración

La ventana de exploración muestra los objetos explorados actualmente, como su ubicación, el número de amenazas encontradas (si las hubiera), la cantidad de objetos explorados y la duración de la exploración. La parte inferior de la ventana es un registro de exploración que muestra el número de versión del motor de detección, la fecha y la hora en que se inició la exploración y la selección del objetivo.

Cuando la exploración esté en marcha, puede hacer clic en **Pausar** si desea interrumpirla temporalmente. La opción **Reanudar** está disponible cuando el proceso de exploración está en pausa.

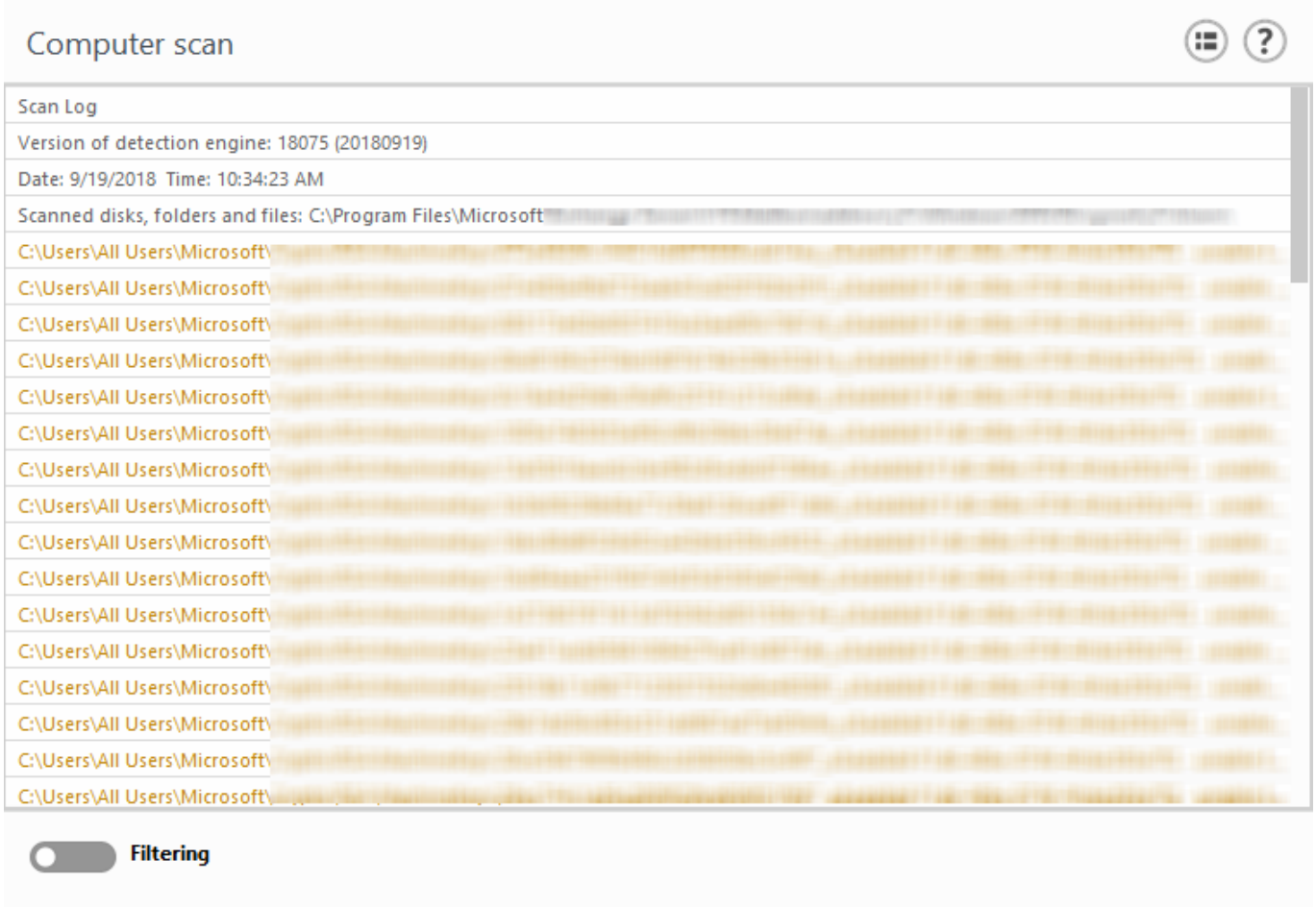


Desplazarse por el registro de exploración

Deje esta opción habilitada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana Archivos de registro.

> Es común que algunos archivos, como los archivos protegidos por contraseña o los que usa el sistema de manera exclusiva (habitualmente, archivos *pagefile.sys* y ciertos archivos de registro), no se puedan explorar.

Una vez finalizada la exploración, verá el registro de exploración con toda la información importante en relación con la exploración concreta.



Haga clic en el icono de cambio **Filtrado** para abrir la ventana Filtrado de registros en la que puede definir criterios de filtrado o búsqueda. Para ver el menú contextual, haga clic con el botón secundario en una entrada específica del registro:

Acción	Uso	Acceso directo	Ver también
Filtrar los mismos registros	Activa la filtración de registros. Se muestran solo los registros del mismo tipo que el registro seleccionado.	Ctrl + Shift + F	
Filtrar...	Tras hacer clic en esta opción, la ventana Filtrado de registros le permitirá definir los criterios de filtrado para entradas de registros específicas.		Filtrado de registros
Habilitar filtro	Activa las configuraciones de los filtros. La primera vez que active el filtrado, debe definir la configuración.		
Deshabilitar el filtro	Desactiva los filtros (al igual que el hacer clic en el interruptor en la parte inferior).		
Copiar	Copia la información de los registros seleccionados/resaltados al portapapeles.	Ctrl + C	
Copiar todo	Copia la información de todos los registros en la ventana.		
Exportar...	Exporta la información de los registros seleccionados/resaltado a un archivo .xml.		
Exportar todo...	Exporta toda la información de la ventana a un archivo XML.		

Archivos de registro

Los archivos de registro contienen información sobre los sucesos importantes del programa que se llevaron a cabo, proporcionan una visión general de los resultados de la exploración, las amenazas detectadas, etc. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. La emisión de registros se mantiene activa en segundo plano sin necesidad de la interacción del usuario. La información se registra de acuerdo con el nivel de detalle actualmente configurado. Es posible ver los mensajes de texto y los registros directamente desde el entorno de ESET Mail Security o exportarlos para su visualización en otra parte.

Seleccione el tipo de registro apropiado desde el menú desplegable. Se encuentran disponibles los siguientes registros:

Detecciones

El registro de amenazas ofrece información detallada sobre las infiltraciones detectadas por los módulos de ESET Mail Security. Esta información incluye la hora de la detección, el nombre de la infiltración, la ubicación, la acción realizada y el nombre del usuario registrado cuando se detectó la infiltración.

Haga doble clic en la entrada de cualquier registro para mostrar sus detalles en una ventana separada. De ser necesario, puede crear una exclusión de detección. Haga clic con el botón secundario del mouse en un registro (detección) y, luego, en **Crear exclusión**. Se abrirá el asistente de exclusión con criterios previamente definidos. Si hay un nombre de detección junto a un archivo excluido, significa que el archivo se excluye únicamente para la detección específica. Si dicho archivo se infecta más adelante con otro malware, se detectará.

Eventos

Todas las acciones importantes que ESET Mail Security lleva a cabo se registran en el registro de sucesos. El registro de sucesos contiene información sobre los sucesos y errores que se produjeron en el programa. Se diseñó para ayudar a los administradores de sistemas y a los usuarios a resolver problemas. Con frecuencia, la información aquí incluida puede ayudarlo a encontrar una solución a un problema que ocurra en el programa.

Exploración del equipo

Todos los resultados de la exploración se muestran en esta ventana. Cada línea corresponde a un control individual de un equipo. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración respectiva.

Archivos bloqueados

Contiene registros de archivos que fueron bloqueados y a los que no se podía acceder. El protocolo muestra la causa y el módulo fuente que bloqueó el archivo, así como la aplicación y el usuario que ejecutó el archivo.

Enviar archivos

Contiene registros de protección basada en la nube de archivos ESET LiveGuard Advanced y ESET LiveGrid®.

Registros de auditoría

Contiene registros de cambios en la configuración o en el estado de protección, y crea instantáneas para referencia futura. Haga clic con el botón secundario en cualquier registro del tipo Cambios de configuración y seleccione Mostrar cambios del menú de contexto para mostrar información detallada sobre el cambio realizado.

Si quiere ir a la configuración anterior, seleccione Restablecer. También puede usar la opción Quitar todo para eliminar registros de archivo. Si quiere desactivar el registro de Auditoría, vaya a Configuración avanzada > Herramientas > Archivos de registro > Registro de auditoría.

HIPS

Contiene historiales de las reglas específicas que se marcan para su inclusión en el registro. El protocolo muestra la aplicación que desencadenó la operación, el resultado (si la regla se permitió o prohibió) y el nombre de la regla creada.

Protección de la red

Contiene registros de archivos que fueron bloqueados por la Protección contra botnets e IDS (Protección contra ataques en la red).

Sitios Web filtrados

Lista de sitios web que fueron bloqueados por la protección de acceso a la weby la protección de correos electrónicos anti-phishing. Estos registros muestran la hora, la URL, el usuario y la aplicación que abrió una conexión con el sitio web en particular.

Control de dispositivos

Contiene registros de medios o dispositivos extraíbles que se conectaron al equipo. Solo los dispositivos con una Regla de control del dispositivo se registrarán en el archivo de registro. Si la regla no coincide con un dispositivo conectado, se creará una entrada del registro para un dispositivo conectado. Aquí también puede ver detalles tales como el tipo de dispositivo, número de serie, nombre del proveedor y tamaño del medio (si está disponible).

Protección del servidor de correo

Todos los mensajes detectados por ESET Mail Security como infiltración o como spam se registran aquí. Estos registros son aplicables a los siguientes tipos de protección: Antispam, Antiphishing, Protección contra la suplantación de remitente, Reglas y Antimalware.

Al hacer doble clic sobre un elemento, se abrirá una ventana emergente con información Adicional acerca del mensaje de correo electrónico detectado, como la dirección IP, dominio HELO, ID del mensaje, tipo de exploración que muestra la capa de protección que se detectó. Además, puede visualizar el resultado de la exploración del protección contra malware, Anti-Phishing y exploración antispam y los motivos de la detección o si se activó un Regla.

> i No todos los mensajes procesados quedan registrados en un registro de protección del servidor de correo. Sin embargo, todos los mensajes que en realidad fueron modificados (archivo adjunto eliminado, cadena personalizada agregada a un encabezado de mensaje, etc.) se escriben en el registro.

Exploración de la base de datos del buzón

Contiene la versión del motor de detección, la fecha, la ubicación explorada, la cantidad de objetos escaneados, la cantidad de amenazas encontradas, la cantidad de aciertos de la regla y el tiempo de compleción.

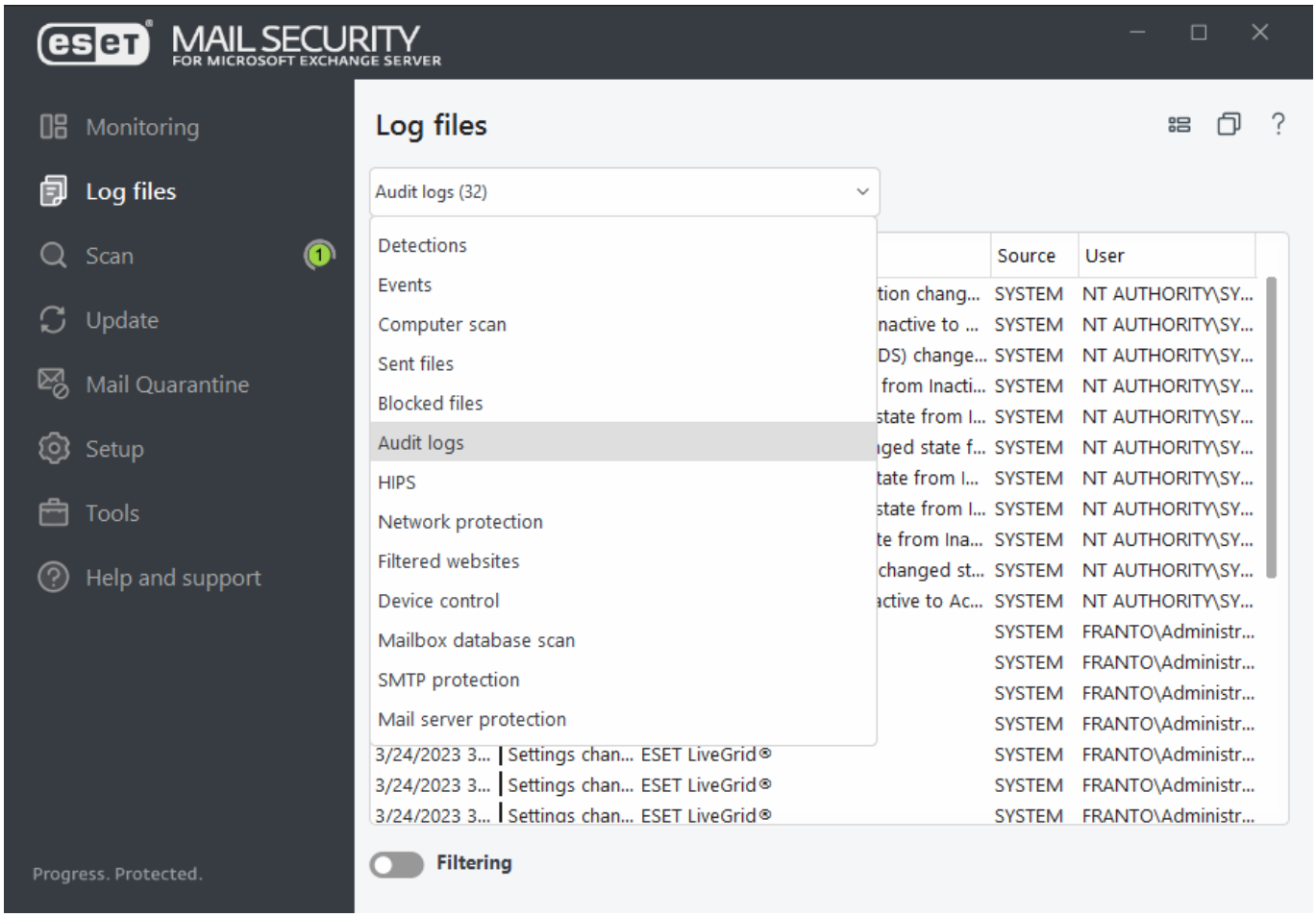
Protección SMTP

Todos los mensajes que se han evaluado utilizando el método de creación lista gris. Aquí también se muestran SPF y Backscatter. Cada registro contiene el dominio HELO, la dirección IP del remitente y del destinatario, los

estados de Acciones (rechazados, rechazados (no verificados) y mensajes entrantes verificados). Hay una nueva acción para agregar el subdominio a la lista blanca de listas grises. Vea la tabla de abajo.

Exploración de Hyper-V

Contiene una lista de los resultados del análisis Hyper-V. Haga doble clic en cualquier entrada para visualizar los detalles de la exploración respectiva.



El menú de contexto (clic con el botón secundario) le permite escoger una acción con un registro seleccionado:

Acción	Uso	Acceso directo	Ver también
Mostrar	Muestra información más detallada acerca del registro seleccionado en una ventana nueva (igual que hacer doble clic).		
Filtrar los mismos registros	Activa la filtración de registros. Se muestran solo los registros del mismo tipo que el registro seleccionado.	Ctrl + Shift + F	
Filtrar...	Tras hacer clic en esta opción, la ventana Filtrado de registros le permitirá definir los criterios de filtrado para entradas de registros específicas.		Filtrado de registros
Habilitar filtro	Activa las configuraciones de los filtros. La primera vez que active el filtrado, debe definir la configuración.		
Deshabilitar el filtro	Desactiva los filtros (al igual que el hacer clic en el interruptor en la parte inferior).		
Copiar	Copia la información de los registros seleccionados/resaltados al portapapeles.	Ctrl + C	
Copiar todo	Copia la información de todos los registros en la ventana.		

Acción	Uso	Acceso directo	Ver también
Eliminar	Elimina los registros seleccionados/resaltados. Esta acción requiere contar con privilegios de administrador.	Quitar	
Eliminar todo	Elimina todos los registros en la ventana. Esta acción requiere privilegios de administrador.		
Exportar...	Exporta la información de los registros seleccionados/resaltado a un archivo .xml.		
Exportar todo...	Exporta toda la información de la ventana a un archivo XML.		
Buscar...	Abre la ventana Buscar en los registros y le permite definir los criterios de búsqueda. Puede utilizar la función Buscar para localizar un registro específico incluso mientras el filtrado está activado.	Ctrl + F	Búsqueda en el registro
Encontrar siguiente	Busca la siguiente concordancia de los criterios de búsqueda definidos.	F3	
Encontrar anterior	Encuentra la ocurrencia anterior.	Shift + F3	
Crear exclusión	Para excluir objetos de la limpieza mediante el uso del nombre, la ruta o el hash de detección.		Crear exclusión

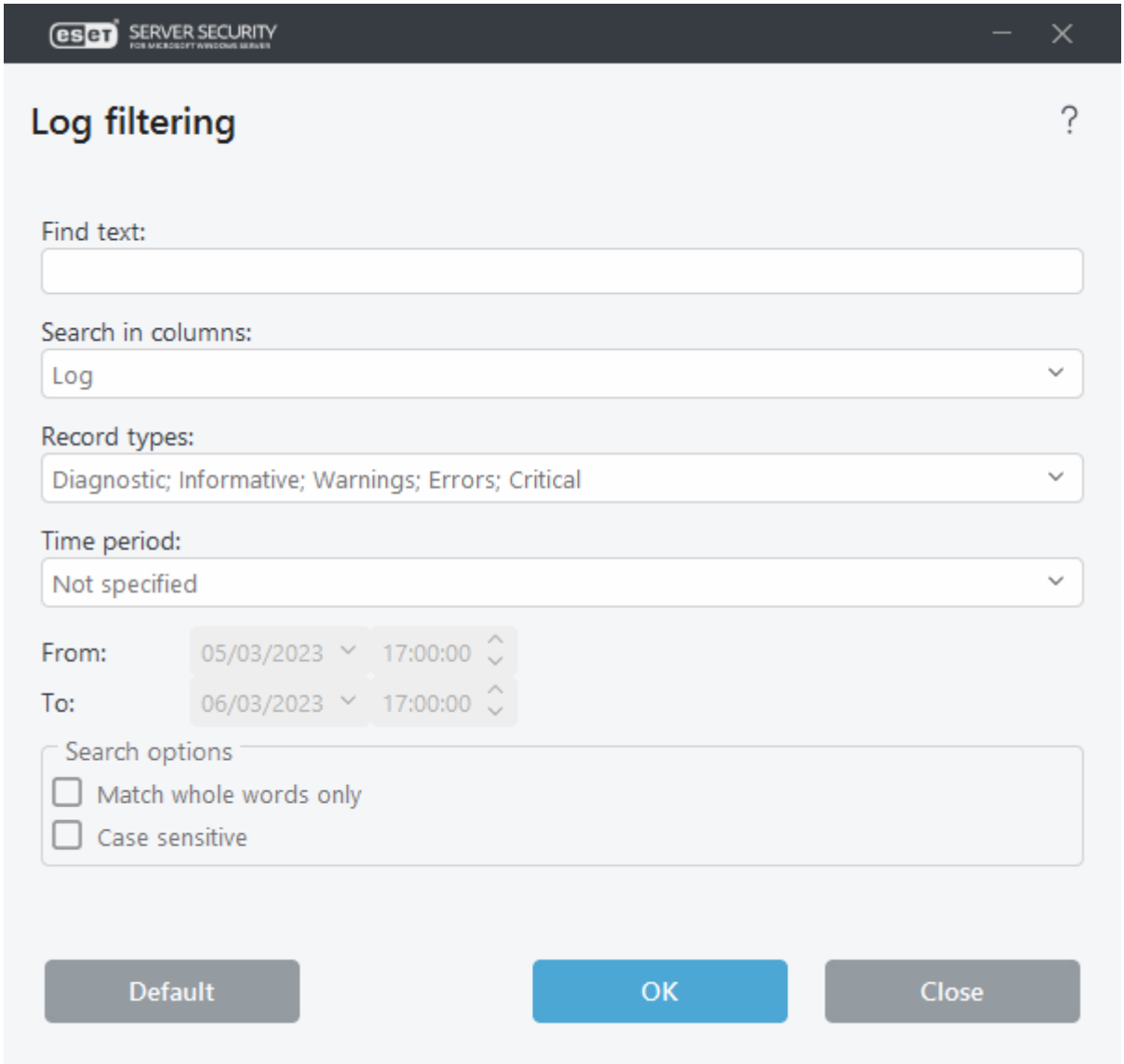
Agregar dirección IP a la lista gris o blanca.	Agrega la dirección IP del remitente a la lista blanca de IP. Puede encontrar la lista blanca de IP en la sección Listas grises y SPF de Filtrado y verificación. Esto aplica a los elementos registrados en las listas grises o SPF.
Agregar dominio a la lista gris y la lista blanca de SPF	Agrega el dominio del remitente a la lista blanca Dominio a IP. Solo se agrega el dominio y se ignora el subdominio. Por ejemplo, si la dirección del remitente es sub.domain.com, solo se agrega domain.com a la lista blanca. Puede encontrar la lista blanca Dominio a IP en la sección Listas grises y SPF de Filtrado y verificación. Esto aplica a los elementos registrados por las Listas grises.
Agregar subdominio a la lista grises y lista blanca SPF	Agrega el dominio del remitente a la lista blanca Dominio a IP. Se agrega el dominio completo, incluido el subdominio (por ejemplo, sub.domain.com). Esto aporta mayor flexibilidad al filtrado, en caso de ser necesario. Puede encontrar la lista blanca Dominio a IP en la sección Listas grises y SPF de Filtrado y verificación. Esto aplica a los elementos registrados por las Listas grises.

Filtrado de registros

La característica de filtrado de registros puede ayudarlo a encontrar la información que está buscando, en especial cuando hay muchos registros. Le permite limitar los registros de archivos, por ejemplo, si busca una clase específica de evento, estado o período de tiempo.

Puede filtrar registros de registro indicando ciertas opciones de búsqueda, sólo se mostrarán en la ventana Archivos de registro los registros que sean relevantes (de acuerdo con esas opciones de búsqueda).

Escriba la palabra clave que está buscando en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para precisar su búsqueda. Elija uno o más registros del menú desplegable **Tipos de historial de registros**. Defina el **Período de tiempo** desde el que desea que se muestren los resultados. También puede utilizar otras opciones de búsqueda, como **Hacer coincidir palabras enteras** o **Coincidir mayúsculas y minúsculas**.



Buscar el texto

Escriba una cadena (una palabra o parte de una palabra). Solo se mostrarán los historiales que contengan la cadena de texto especificada. Se omitirán otros historiales.

Buscar en columnas:

Seleccione qué columnas se tendrán en cuenta durante la búsqueda. Se pueden seleccionar una o más columnas para usar en la búsqueda.

Tipos de historiales

Elija un tipo de historial de registro o varios desde el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo**: registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias**: registra los errores críticos y los mensajes de advertencia.

- **Errores**: se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico**: registra solo los errores críticos.

Período

Defina el período a partir del cual desea que se muestren los resultados.

- No especificado (predeterminado): no busca en el período especificado, ya que busca en el registro completo.
- Último día
- Última semana
- Último mes
- Período de tiempo: puede especificar el período exacto (Desde: y Hasta:) para filtrar solo aquellos historiales del período específico.

Solo coincidir palabras completas

Use esta casilla de verificación si desea buscar palabras completas para obtener resultados más precisos.

Coincidir mayúsculas y minúsculas

Habilite esta opción si es importante que utilice mayúsculas o minúsculas al filtrar. Al configurar las opciones de filtrado/búsqueda, haga clic en **OK** para mostrar los registros de registro filtrados o en **Buscar** para iniciar la búsqueda.

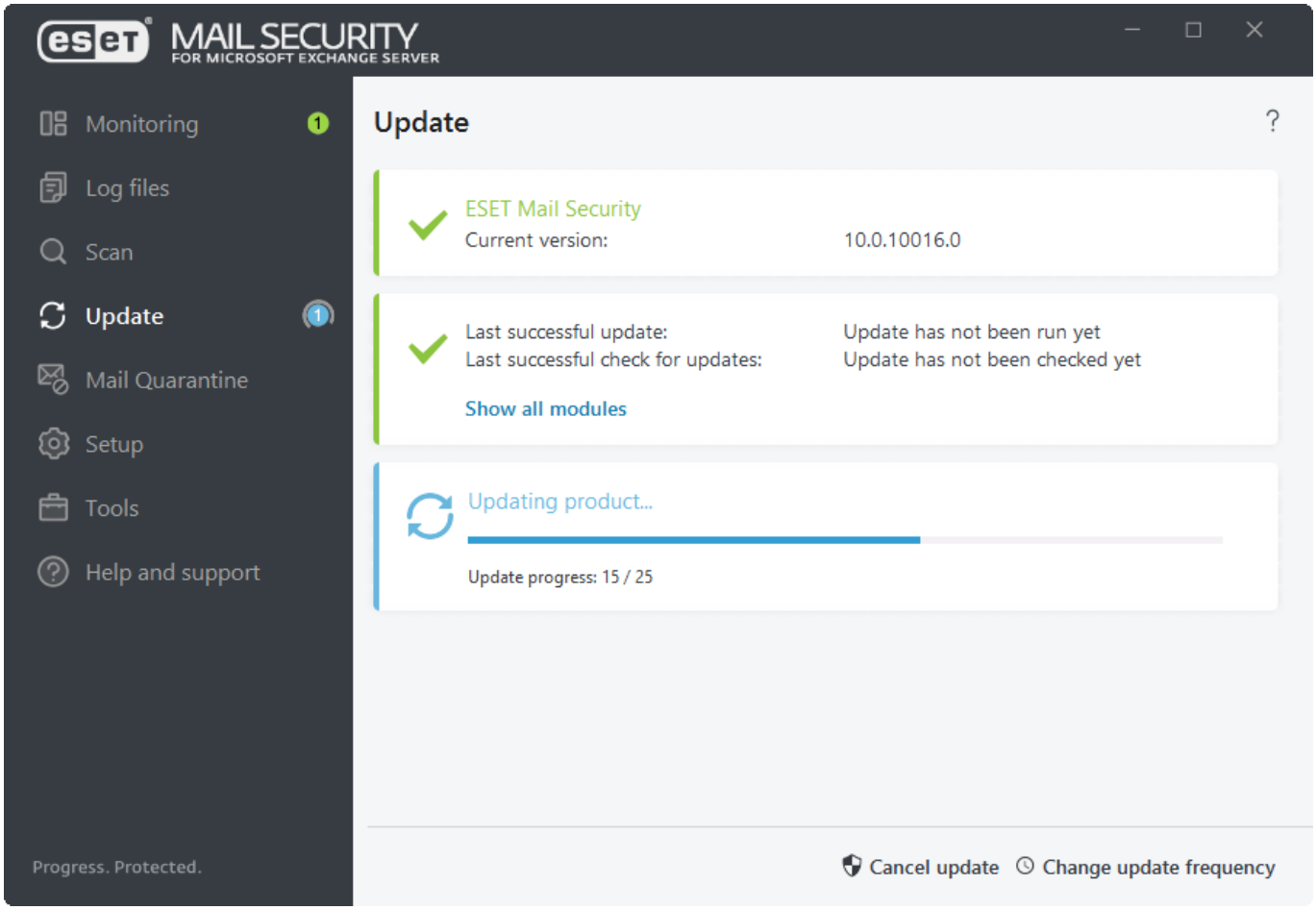
Los archivos de registro se buscan de arriba a abajo, comenzando desde su posición actual (el registro que está resaltado). La búsqueda para cuando encuentra el primer registro correspondiente. Presione **F3** para buscar el siguiente registro o haga clic con el botón derecho y seleccione **Buscar** para refinar sus opciones de búsqueda.

Actualización

En la sección Actualización, puede ver el estado actual de actualización de su ESET Mail Security, incluyendo la fecha y hora de la última actualización exitosa. La actualización habitual de ESET Mail Security es la mejor forma de mantener el máximo nivel de seguridad en el servidor.

El módulo de actualización garantiza que el programa esté siempre al día de dos maneras: actualizando el motor de detección y los componentes del sistema. La actualización del motor de detección y de los componentes del programa constituye una parte importante de la protección completa contra el código malicioso.

> Si aún no ha ingresado a Clave de licencia, no podrá recibir actualizaciones y se le solicitará que active su producto. Para ello, navegue a **Ayuda y asistencia técnica** > **Activar producto**.



Versión actual

La versión compilada de ESET Mail Security.

Última actualización exitosa

Es la fecha de la última actualización. Asegúrese de que la fecha sea reciente, lo que significa que los módulos están al día.

Última búsqueda de actualizaciones correcta

La fecha del último intento por actualizar módulos.

Mostrar todos los módulos

Para abrir la lista de los módulos instalados.

Buscar actualizaciones

La actualización de los módulos constituye una parte fundamental para mantener una protección completa contra códigos maliciosos.

Cambiar frecuencia de actualización

Puede editar la programación de la tarea para la Actualización automática de rutina de las tareas programadas.

Si no comprueba las actualizaciones a la mayor brevedad posible, se visualizará uno de los siguientes mensajes:

Mensaje de error	Descripciones
La actualización de los módulos no está al día	Este error aparecerá luego de varios intentos fallidos de actualizar el módulo. Es recomendable verificar la configuración de la actualización. El motivo más común de este error es el ingreso incorrecto de los datos de autenticación o la configuración incorrecta de las opciones de conexión.
Error de actualización de módulos - El producto no está activado	La clave de licencia no se ha ingresado correctamente en la configuración de actualización. Es recomendable que compruebe sus datos de autenticación. La **Configuración avanzada** (**F5**) contiene opciones de actualización adicionales. Haga clic en **Ayuda y soporte** > Administrar licencia en el menú principal para ingresar una clave de licencia nueva.
Se produjo un error al descargar los archivos de actualización	Una causa posible de este error es la configuración de la conexión a Internet incorrecta. Es recomendable verificar su conectividad a Internet; para ello, abra cualquier sitio web en su navegador. Si el sitio web no se abre, es probable que la conexión a Internet no esté establecida o que haya problemas de conectividad en el equipo. Consulte el problema con su proveedor de servicios de Internet (ISP) si su conexión está inactiva.
Error 0073 de actualización de módulos	Haga clic en **Actualizar** > **Buscar actualizaciones**. Para obtener más información, visite este artículo de la base de conocimientos.

> Es posible que las opciones del servidor proxy para distintos perfiles de actualización difieran entre sí. En este caso, configure los distintos perfiles de actualización en **Configuración avanzada F5** al hacer clic en **Actualizar** > Perfil.

Cuarentena de correo

Los mensajes de correo electrónico y sus componentes, como los archivos adjuntos, se ponen en Cuarentena de correo y no en cuarentena tradicional de archivos. La Cuarentena de correo es una forma más cómoda de administrar el spam, los archivos adjuntos infectados que contienen malware o los mensajes de phishing. Hay diversas razones por las que los mensajes de correo electrónico entran en la Cuarentena de correo, según el ESET Mail Security módulo de protección que gestione el mensaje (Anti-malware, Antispam, Anti-Phishing, Protección contra la suplantación de identidad del remitente o Reglas).

Filtrado por íconos

Puede utilizar iconos para filtrar los mensajes con la finalidad de ver sólo los archivos adjuntos, los correos electrónicos o los correos electrónicos con archivos adjuntos.

Periodo

Seleccione el periodo de tiempo respecto del cual desea ver los correos electrónicos en cuarentena. Cuando selecciona **Personalizado**, puede especificar un rango (Fecha desde y Fecha hasta).

Nodos del clúster

Seleccione los nodos de clúster de los cuales desea ver los correos electrónicos en cuarentena.

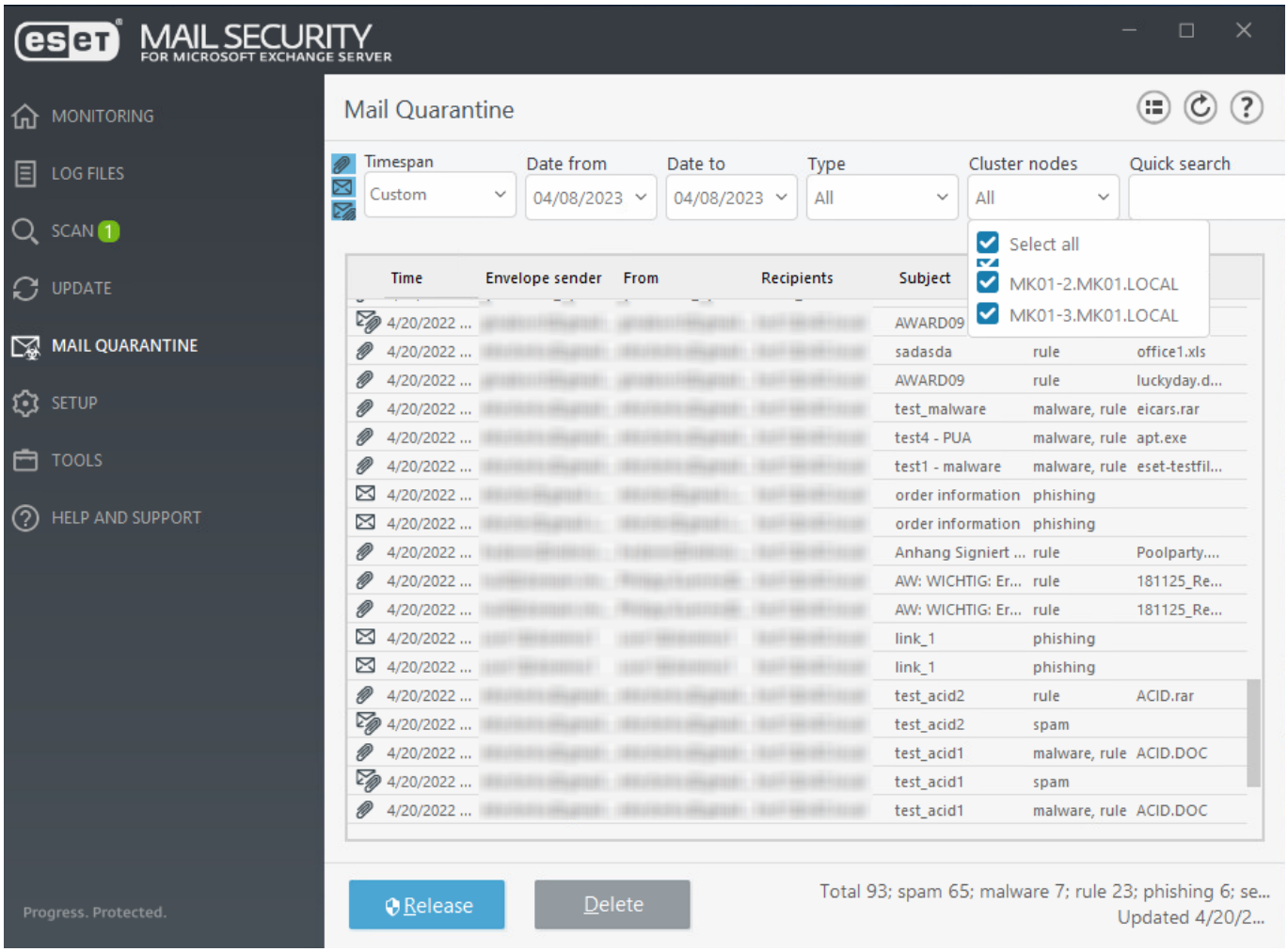
Búsqueda rápida

Ingrese una cadena en el cuadro de texto para filtrar los correos electrónicos que se muestran (se busca todas las columnas).

Tipo

Utilice las casillas de verificación para seguir filtrando por tipo (spam, malware, reglas, phishing o remitente suplantado).

> Los datos del administrador de Cuarentena de correo no se actualizan de manera automática, recomendamos hacer clic en **Actualizar** de manera periódica para ver los elementos más actuales en la Cuarentena de correo.



Liberar

Libera los correos electrónicos a los destinatarios originales mediante el directorio de reproducción nueva y los elimina de la cuarentena. Haga clic en Sí para confirmar la acción. Si el elemento en cuarentena es un adjunto de la carpeta de pública deshabilitada para el correo, el botón Liberar no estará disponible.

> Cuando se libera un correo electrónico de cuarentena, ESET Mail Security ignora el encabezado `To:` MIME porque se puede alterar fácilmente. En cambio, usa la información del destinatario original del comando `RCPT TO:` adquirida durante la conexión de SMTP. De esta manera, se garantiza que el destinatario correcto del correo reciba el mensaje liberado de cuarentena.

> Si ejecuta un entorno en clúster y envía un mensaje de la cuarentena, los demás nodos de ESET Mail Security no volverán a poner el mensaje en cuarentena. Se consigue mediante la sincronización de las reglas entre los nodos del clúster.

Liberar a

Si no desea liberar un correo electrónico a todos los destinatarios, use esta opción para seleccionar destinatarios

específicos que recibirán el correo electrónico liberado. Esta opción solo está disponible para mensajes con varios destinatarios.

Eliminar

Elimina elementos de la cuarentena. Haga clic en **Sí** para confirmar la acción. Los elementos que se eliminan mediante la ventana principal del programa se eliminan de la vista de cuarentena pero se conservan en el almacenamiento. Éstos se borran automáticamente posteriormente (después de tres días de forma predeterminada).

Eliminar de forma permanente

Quita elementos de la vista de cuarentena y los elimina del almacenamiento. Haga clic en **Sí** para confirmar la acción.

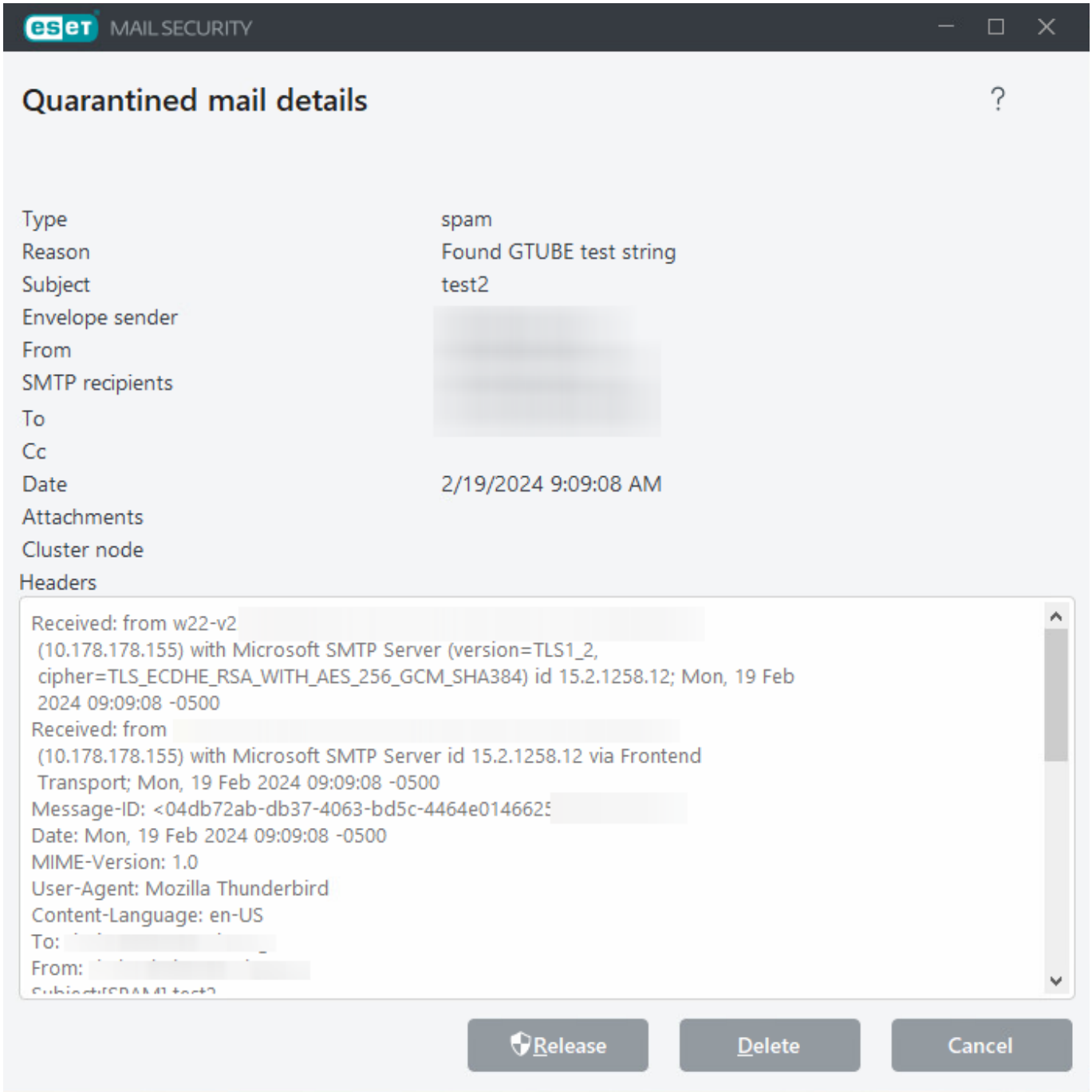
Detalles del correo en Cuarentena

Haga doble clic en el mensaje en cuarentena o haga clic con el botón derecho y elija **Mostrar detalles**. Se abrirá una nueva ventana con detalles sobre el mensaje de correo electrónico en cuarentena. También puede consultar los encabezados de correo electrónico RFC originales para obtener más detalles.

Detalles del adjunto en Cuarentena

Al hacer doble clic en un archivo adjunto, el cuadro de diálogo de detalles es diferente comparado con el cuadro de diálogo de detalles del mensaje de correo electrónico. Los encabezados RFC no están disponibles, sino que se visualiza un área con un texto del sobre adjunto. Puede escribir texto personalizado del sobre adjunto cuando lo libere de la cuarentena de correo.

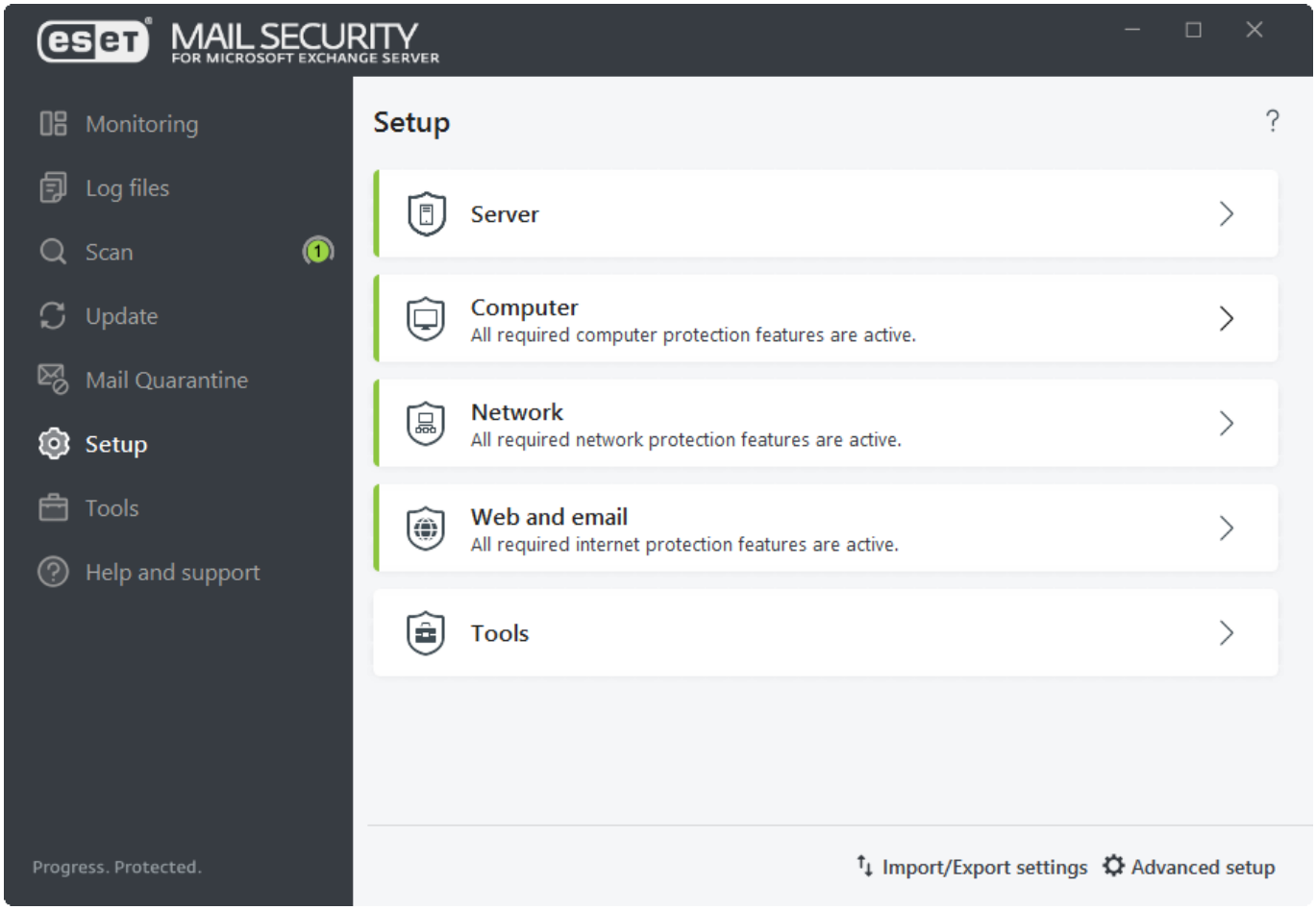
También hay acciones disponibles en el menú contextual. Si lo desea, haga clic en **Liberar**, **Eliminar** o **Eliminar permanentemente** para ejecutar una acción con un mensaje de correo electrónico en cuarentena. Haga clic en **Sí** para confirmar la acción. Si elige **Eliminar de manera permanente** el mensaje se eliminará también del sistema de archivos, a la inversa que **Eliminar** que eliminará el elemento de la vista del administrador de la Cuarentena de correo.



Configuración

La ventana del menú Configuración contiene las siguientes secciones:

- Servidor
- Equipo
- Red
- Internet y correo electrónico
- Herramientas - Registro de diagnósticos



Para deshabilitar temporalmente los módulos individuales, junto al módulo apropiado, haga clic en el interruptor verde. Esto puede disminuir el nivel de protección de su servidor.

Para volver a habilitar la protección de un componente de seguridad deshabilitado, junto al módulo apropiado, haga clic en el interruptor rojo. El componente regresará su estado de habilitado.

Para acceder a configuraciones detalladas para un componente de seguridad específico, haga clic en el ícono de engranaje.

Importar/exportar las configuraciones

Carga los parámetros de configuración mediante un archivo de configuración *.xml* o guarda los parámetros de configuración actuales en un archivo de configuración.

Configuración avanzada

Configure las opciones y los ajustes avanzados en función de sus necesidades. Para acceder a la pantalla **Configuración avanzada** desde cualquier parte del programa, presione **F5**.

Servidor

Verá una lista de los componentes que puede habilitar o deshabilitar con el interruptor. Para configurar los ajustes para un elemento específico, haga clic en la rueda dentada.

Protección antivirus

Defiende el sistema ante ataques malintencionados mediante el control de archivos, correos electrónicos y comunicaciones por Internet.

Protección antispam

Integra varias tecnologías (tales como RBL, DNSBL, huellas digitales, verificación de reputación, análisis de contenido, reglas, creación manual de listas blancas y negras, etc.) para alcanzar el nivel máximo de detección de amenazas por correo electrónico.

Protección antiphishing

Analiza el cuerpo del mensaje de los mensajes de correo electrónico entrantes para enlaces de phishing (URL).

La exploración de base de datos del buzón de Microsoft 365

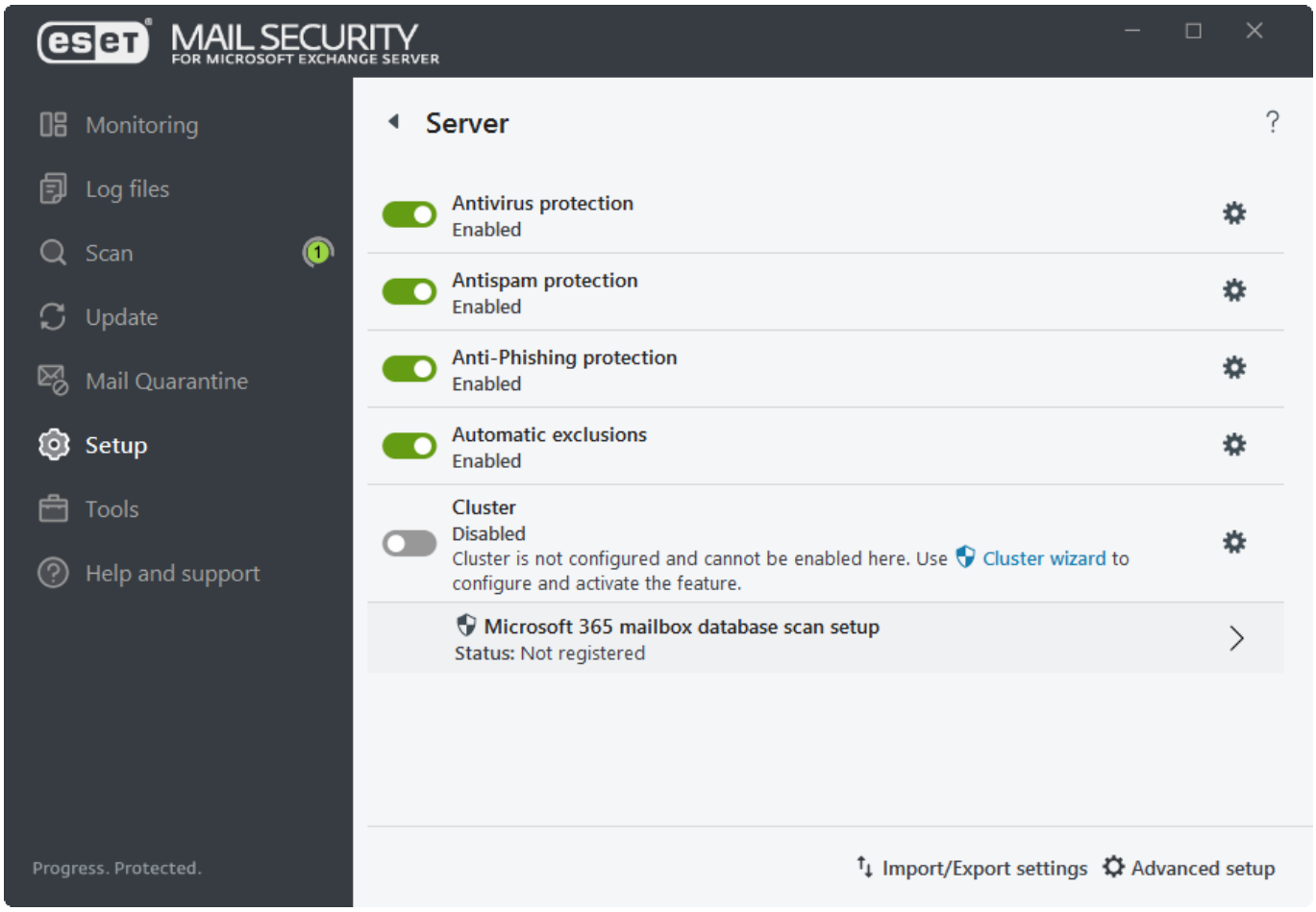
Para activar esta función, registre el explorador ESET Mail Security.

Exclusiones automáticas

Identifica las aplicaciones críticas del servidor y los archivos del sistema operativo críticos y los agrega automáticamente a la lista de exclusiones. Esta funcionalidad ayuda a minimizar el riesgo de conflictos potenciales e incrementar el rendimiento general del servidor mientras se ejecuta un programa de detección de amenazas.

Clúster

Para configurar y activar el clúster ESET.



Equipo

ESET Mail Security tiene todos los componentes que se necesitan para garantizar una protección significativa del servidor como ordenador. Este módulo le permite habilitar/deshabilitar y configurar los siguientes componentes:

Protección del sistema de archivos en tiempo real

Todos los archivos se exploran cuando se abren, crean o ejecutan en el equipo para detectar código malicioso. Para la Protección del sistema de archivos en tiempo real, también hay una opción para **Configurar** o **Editar exclusiones,** que abrirá la ventana de configuración Exclusiones donde puede excluir archivos y carpetas de la exploración.

Control del dispositivo

Este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado.

Sistema de prevención de intrusiones basado en el host (HIPS)

El sistema monitorea los sucesos que ocurren dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.

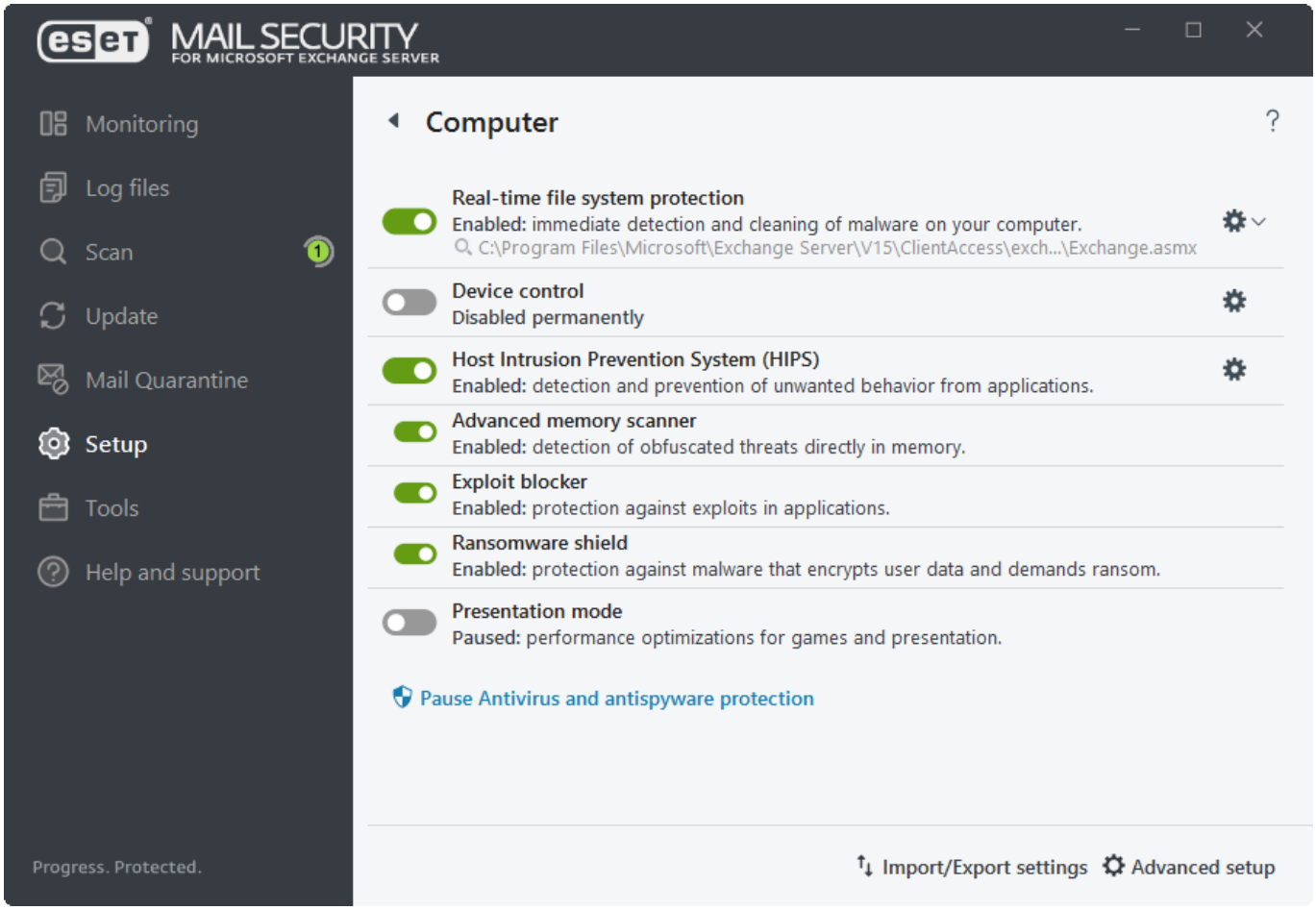
- Advanced memory scanner
- Bloqueador de exploits
- Escudo contra ransomware

Modo presentación

Una función para los usuarios que requieren usar el software en forma ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. Recibirá un mensaje de advertencia (riesgo potencial en la seguridad) y la ventana principal del programa se pondrá de color naranja una vez habilitado el Modo presentación.

Pausar la protección antivirus y antispyware

Cuando deshabilite temporalmente la protección antivirus y antispyware, puede seleccionar el periodo de tiempo por el que desea que el componente seleccionado esté deshabilitado mediante el uso del menú desplegable y, luego, haga clic en **Aplicar** para deshabilitar el componente de seguridad. Para volver a habilitar la protección, haga clic en **Habilitar la protección antivirus y antispyware** o use la barra.



Red

Esto se logra al autorizar o denegar conexiones de red individuales en función de sus reglas de filtrado. Ofrece protección contra ataques desde equipos remotos y bloquea algunos servicios que pueden ser peligrosos.

El módulo Red le permite habilitar o deshabilitar y configurar los siguientes componentes:

Protección contra ataques en la red (IDS)

Analiza el contenido del tráfico de red y protege de los ataques de red. El tráfico que es considerado perjudicial será bloqueado.

Protección contra Botnets

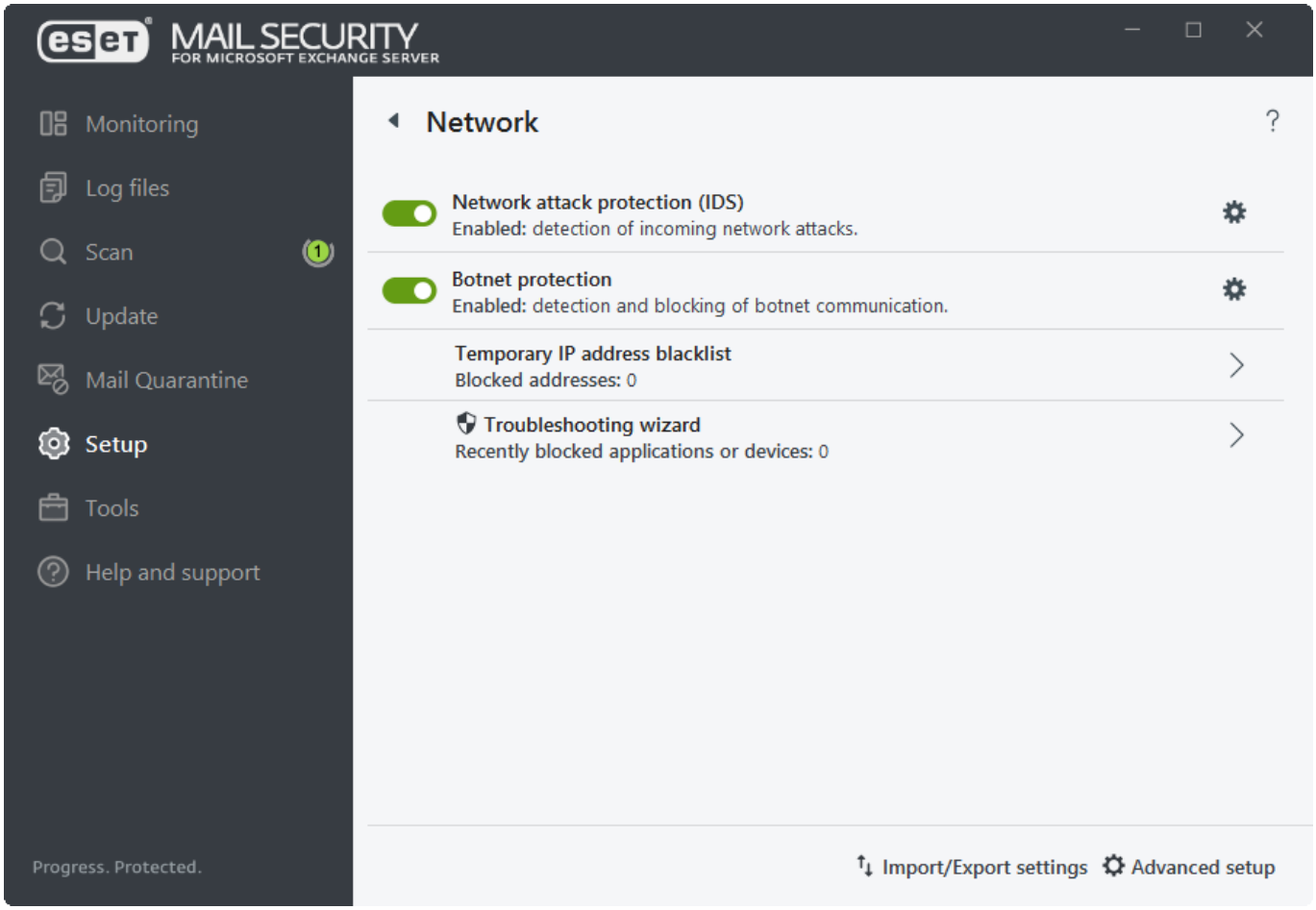
Detección y bloqueo de comunicación de botnet. Identifica el malware en el sistema rápida y precisamente.

Lista negra temporal de direcciones IP (direcciones bloqueadas)

Ver una lista de direcciones IP que han sido detectadas como la fuente de ataques y agregadas a la lista negra para bloquear la conexión durante cierto período de tiempo.

Asistente para la resolución de problemas (aplicaciones o dispositivos recientemente bloqueados)

Lo ayuda a resolver problemas de conectividad causados por la protección contra ataques de la red.



Asistente para la resolución de problemas de red

El asistente para la resolución de problemas vigila todas las conexiones bloqueadas y le guiará a lo largo del proceso de resolución de problemas para corregir los problemas de protección contra ataques a la red con aplicaciones o dispositivos específicos. Luego, el asistente le sugerirá un nuevo conjunto de reglas que deberá aplicar si las aprueba.

Seleccione un periodo de tiempo en el menú desplegable durante el que se haya bloqueado la comunicación. Una lista de comunicaciones bloqueadas recientemente muestra la descripción general del tipo de aplicación o del dispositivo, la reputación y el número total de aplicaciones y dispositivos bloqueados durante ese periodo. Si desea obtener más información sobre la comunicación bloqueada, haga clic en **Detalles**.

El siguiente paso es desbloquear la aplicación o el dispositivo en el que está experimentando problemas de conectividad.

Al hacer clic en Desbloquear, se permitirá la comunicación bloqueada anteriormente. Si sigue experimentando problemas con una aplicación o su dispositivo no funciona como se espera, haga clic en **La aplicación sigue sin funcionar**. Todas las comunicaciones bloqueadas anteriormente para ese dispositivo se permitirán. Si el problema persiste, reinicie el equipo.

Haga clic en **Mostrar cambios** para ver las reglas creadas por el asistente.

Haga clic en **Desbloquear otro** para resolver problemas de comunicación con un dispositivo o una aplicación distintos.

Internet y correo electrónico

Internet y correo electrónico le permite habilitar o deshabilitar y configurar los siguientes componentes:

Protección del acceso a la Web

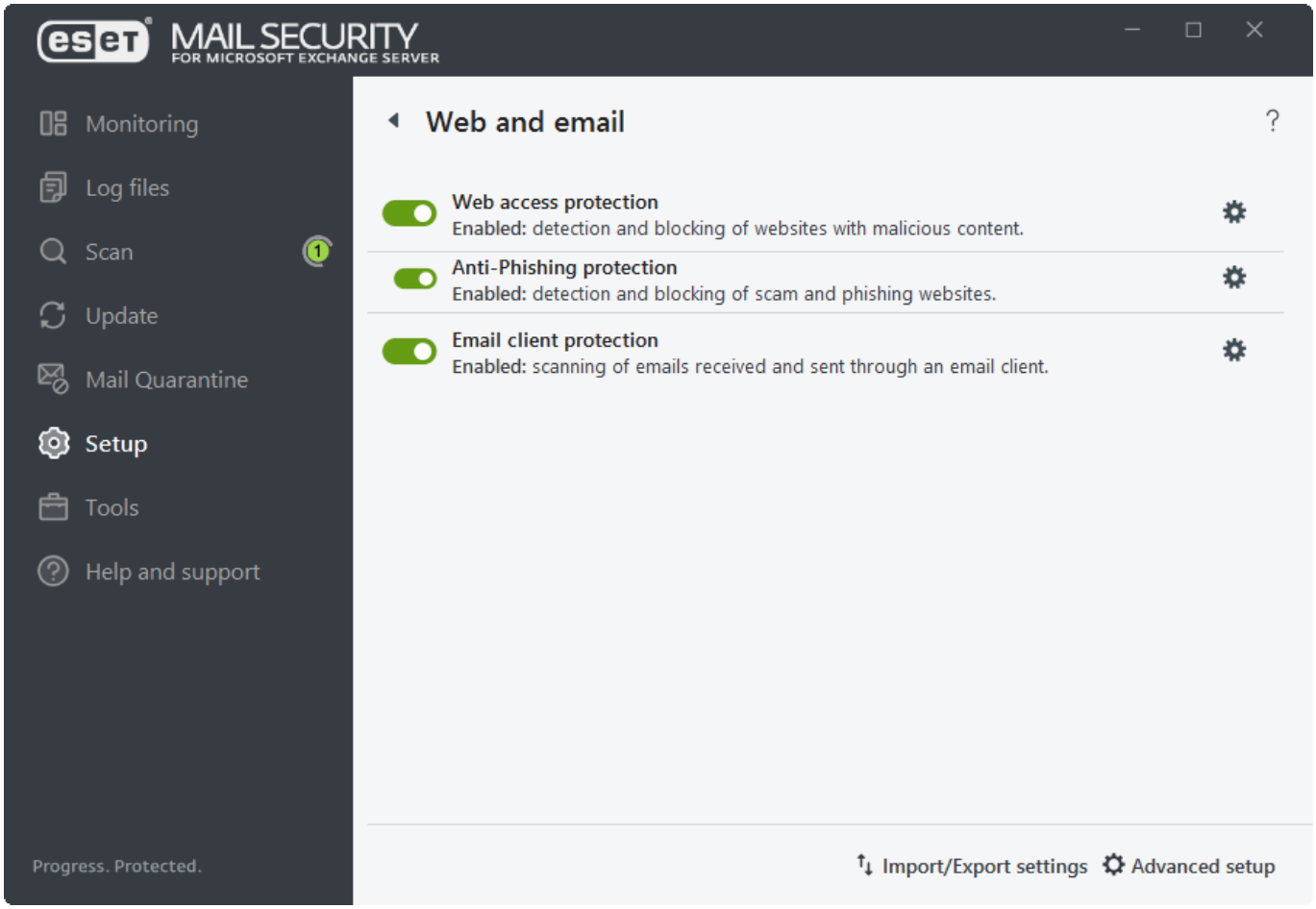
Si se encuentra habilitada, se explora todo el tráfico que pase a través de HTTP o HTTPS en busca de software malintencionado.

Protección antiphishing

Lo protege de sitios web ilegítimos disfrazados de legítimos que intentan obtener contraseñas, datos bancarios y demás información confidencial.

Protección del cliente de correo electrónico

Supervisa las comunicaciones recibidas a través de los protocolos POP3 e IMAP.

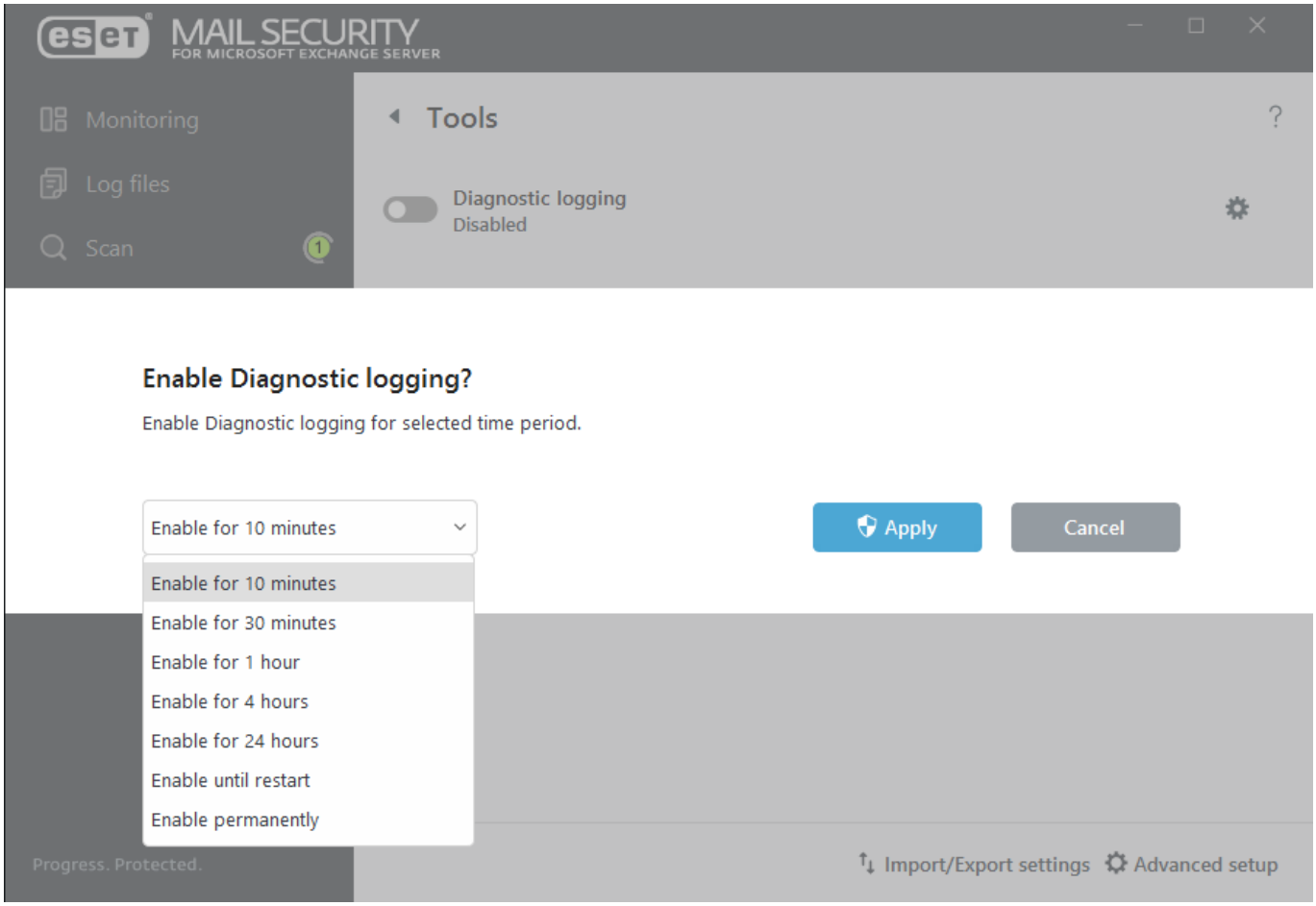


Herramientas - Registro de diagnósticos

Puede habilitar Registro de diagnósticos cuando requiera información detallada sobre el comportamiento de una característica específica de ESET Mail Security, por ejemplo, al solucionar problemas. Al hacer clic en el símbolo de engranaje, puede configurar para qué características deben recolectarse los registros de diagnóstico.

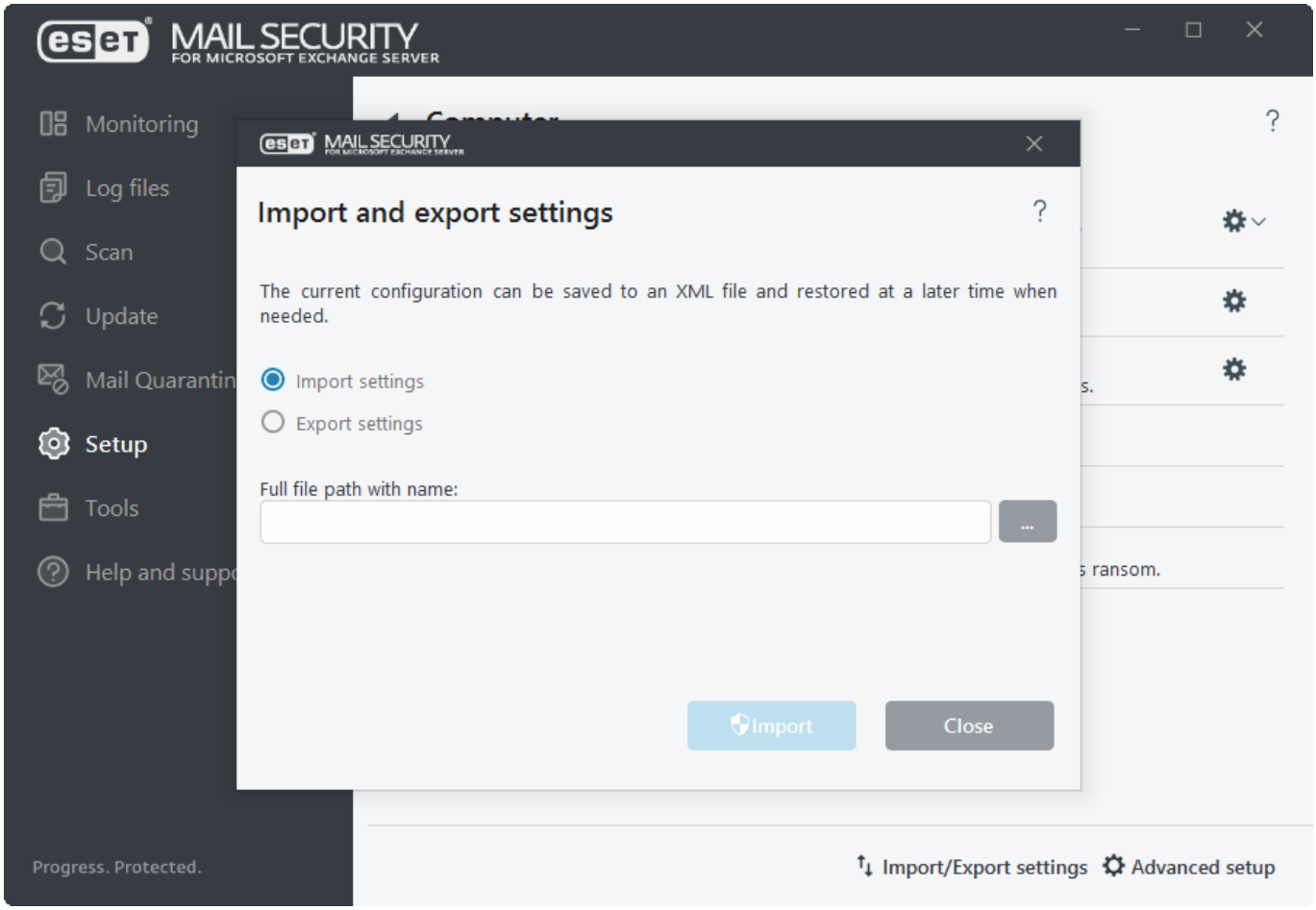
Elija por cuánto tiempo estará habilitado (10 minutos, 30 minutos, 1 hora, 4 horas, 24 horas, hasta el próximo

reinicio del servidor o permanentemente). Una vez activado el registro de diagnóstico, ESET Mail Security reunirá registros detallados de acuerdo con las funciones habilitadas.



Importar y exportar una configuración

La función de configuración de importación/exportación es útil si necesita realizar una copia de seguridad de la configuración actual de su ESET Mail Security. También puede utilizar la función de importación para distribuir o aplicar la misma configuración a otros servidores con ESET Mail Security. Los ajustes se exportan a un archivo *.xml*.

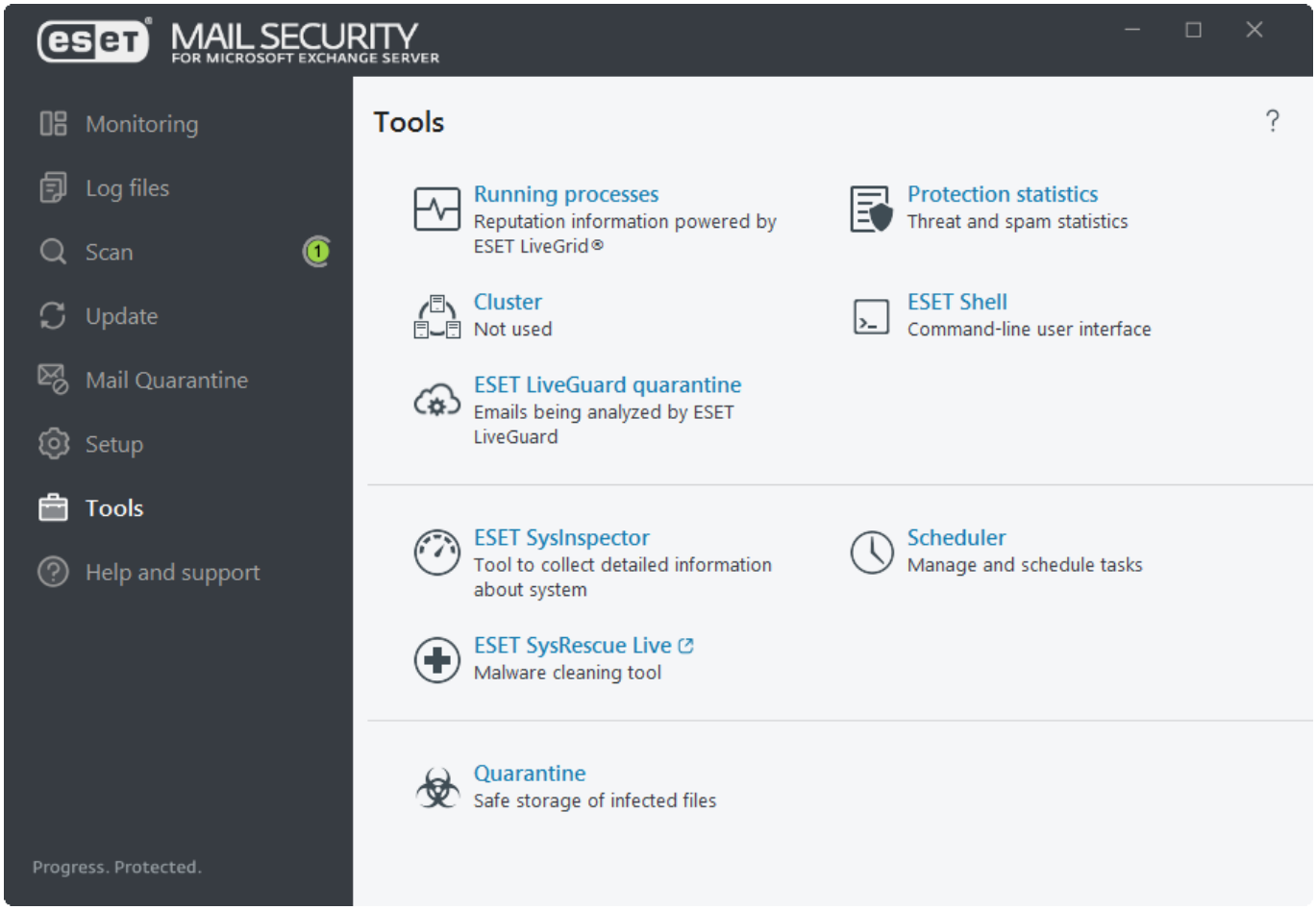


Si no tiene permisos para escribir el archivo exportado en el directorio especificado, puede encontrarse con un error al exportar las configuraciones.

Herramientas

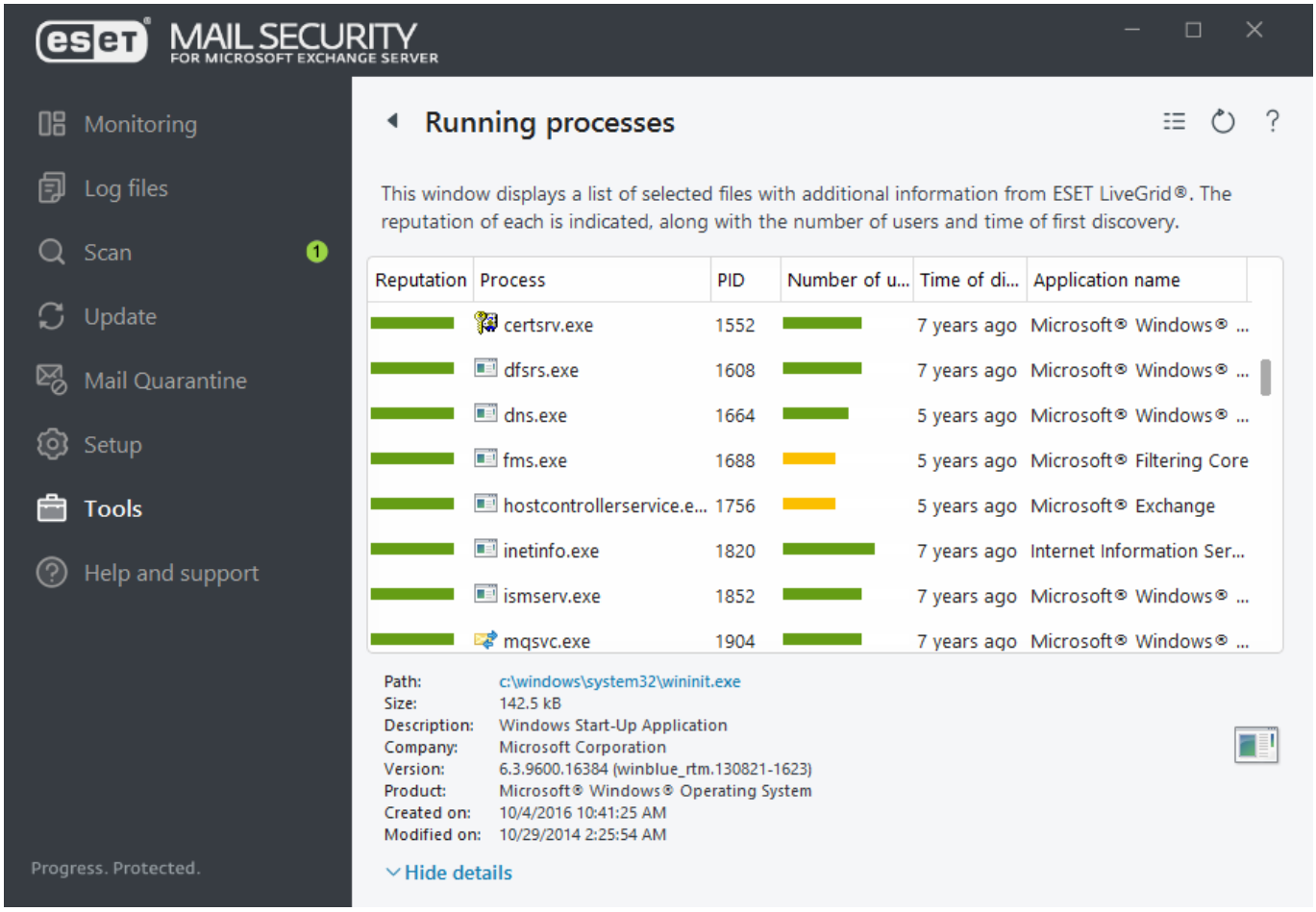
Las siguientes características están disponibles para la administración de ESET Mail Security:

- Procesos activos
- Estadísticas de la protección
- Clúster
- Shell de ESET
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live
- Tareas programadas
- Enviar el archivo para su análisis
- Cuarentena



Procesos activos

Los procesos activos muestran los programas o procesos activos en su equipo y mantiene a ESET informado de manera instantánea y continua sobre las nuevas infiltraciones. ESET Mail Security proporciona información detallada sobre los procesos activos para proteger a los usuarios con la tecnología ESET LiveGrid® habilitada.



Las aplicaciones conocidas marcadas como Seguras (en verde) no están infectadas (figuran en la lista blanca) y se excluyen de la exploración, ya que de esta forma se mejora la velocidad de exploración correspondiente a la exploración del equipo a petición o la protección del sistema de archivos en tiempo real en el equipo.

Reputación	**En la mayoría de los casos, la tecnología ESET Mail Security y ESET LiveGrid® determina la reputación del objeto a partir de una serie de reglas heurísticas que examinan las características de cada objeto (archivos, procesos, claves de registro, etc.) y después estima su potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asigna un nivel de riesgo desde el valor 9: segura (en color verde) hasta 0: peligroso (en color rojo).**
Proceso	El nombre de la imagen del programa o proceso que se está ejecutando actualmente en el equipo. También puede usar el Administrador de tareas de Windows para ver todos los procesos en ejecución en el equipo. Puede abrir el Administrador de tareas al hacer clic con el botón secundario en un área vacía de la barra de tareas seleccionado, posteriormente, el Administrador de tareas, o al presionar Ctrl + Shift + Esc en su teclado.
PID	Es un identificador de procesos activos en los sistemas operativos de Windows.
Cantidad de usuarios	La cantidad de usuarios que usan una aplicación específica. Estos datos se recopilan con la tecnología ESET LiveGrid®.
Hora del descubrimiento	Período de tiempo desde el descubrimiento de la aplicación por la tecnología ESET LiveGrid®.
Nombre de la aplicación	Nombre determinado de un programa al cual pertenece este proceso.

> Cuando una aplicación se marca como Desconocida (naranja), no necesariamente es un software malicioso. Por lo general, solo se trata de una aplicación nueva. Si no está seguro con respecto al archivo, use la función Enviar la muestra para su análisis para enviar el archivo al laboratorio de virus de ESET. Si el archivo resulta ser una aplicación maliciosa, se agregará su detección en una de las próximas actualizaciones del motor de detección.

Mostrar detalles

La siguiente información aparecerá en el sector inferior de la ventana:

- **Ruta**: ubicación de una aplicación en su equipo.
- **Tamaño**: tamaño del archivo ya sea en kB (kilobytes) o MB (megabytes).
- **Descripción**: características del archivo según la descripción proporcionada por el sistema operativo.
- **Empresa**: nombre del proveedor o del proceso de la aplicación.
- **Versión**: información proporcionada por el desarrollador de la aplicación.
- **Producto**: nombre de la aplicación y/o nombre comercial.
- **Creada el**: fecha y hora de la creación de una aplicación.
- **Modificada el**: Última fecha y hora en que se modificó una aplicación.

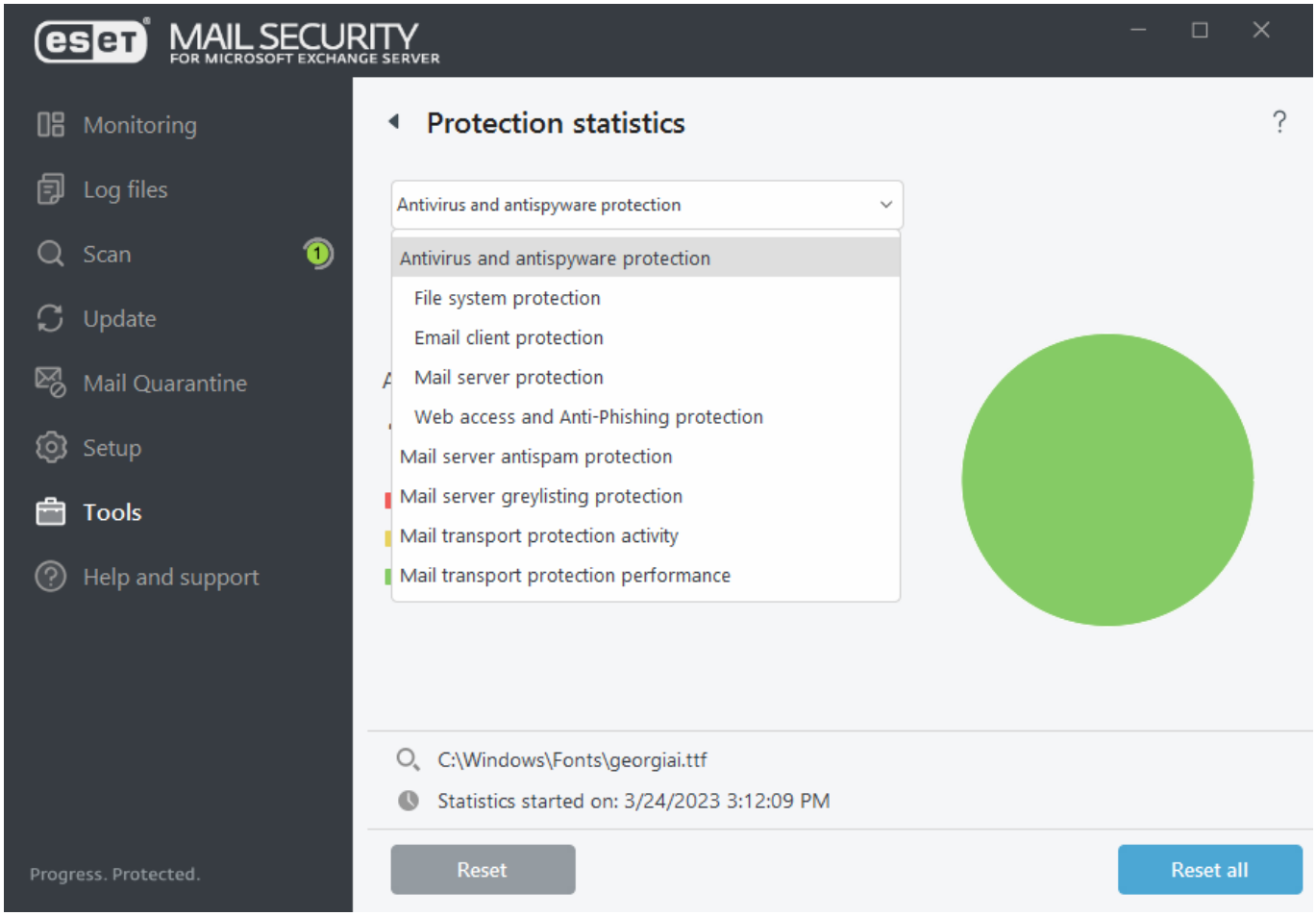
Agregar a exclusiones de procesos

Haga clic derecho en un proceso en la ventana de Procesos en ejecución para excluirlo de la exploración. Se agregará su ruta a la lista de Exclusiones de procesos.

Estadísticas de la protección

Para ver los datos estadísticos relacionados con los módulos de protección de ESET Mail Security, seleccione el módulo de protección aplicable en el menú desplegable. Las estadísticas incluyen información como el número de todos los objetos explorados, el número de objetos infectados, el número de objetos limpiados y el número de objetos limpios.

Pase el ratón por encima de un objeto junto al gráfico y sólo los datos de ese objeto específico se mostrarán. Para borrar la información estadística del módulo de protección actual, haga clic en **Restablecer**. Para borrar los datos de todos los módulos, haga clic en **Restablecer todo**.



Los siguientes gráficos de estadísticas están disponibles en ESET Mail Security:

Protección antivirus y antispyware

Muestra la cantidad general de objetos infectados y desinfectados.

Protección del sistema de archivos

Muestra los objetos que fueron leídos o escritos en el sistema de archivos.

Protección de Hyper-V

Muestra la cantidad general de objetos infectados, desinfectados y limpios (únicamente en sistemas con Hyper-V).

Protección del cliente de correo electrónico

Muestra los objetos que fueron enviados o recibidos por clientes de correo electrónico únicamente.

Protección del acceso a la Web y Anti-Phishing

Muestra los objetos descargados por los navegadores web únicamente.

Protección del servidor de correo

Muestra estadísticas anti-malware del servidor de correo.

Protección antispam del servidor de correo

Muestra el historial de las estadísticas de antispam. Cantidad de los objetos excluidos en la exploración (con base en reglas, mensajes internos, conexiones autenticadas, etc.).

Protección por listas grises del servidor de correo

Incluye las estadísticas antispam generadas por el método de creación de listas grises.

Actividad de la protección del transporte de correo

Muestra los objetos verificados, bloqueados y eliminados por el servidor de correo.

Rendimiento de la protección del transporte de correo

Muestra los datos procesados por VSAPI/Agente de transporte en B/s.

Actividad de la protección de la base de datos del buzón de correo

Muestra los objetos procesados por VSAPI (cantidad de objetos verificados, en cuarentena y eliminados).

Rendimiento de la protección de la base de datos del buzón de correo

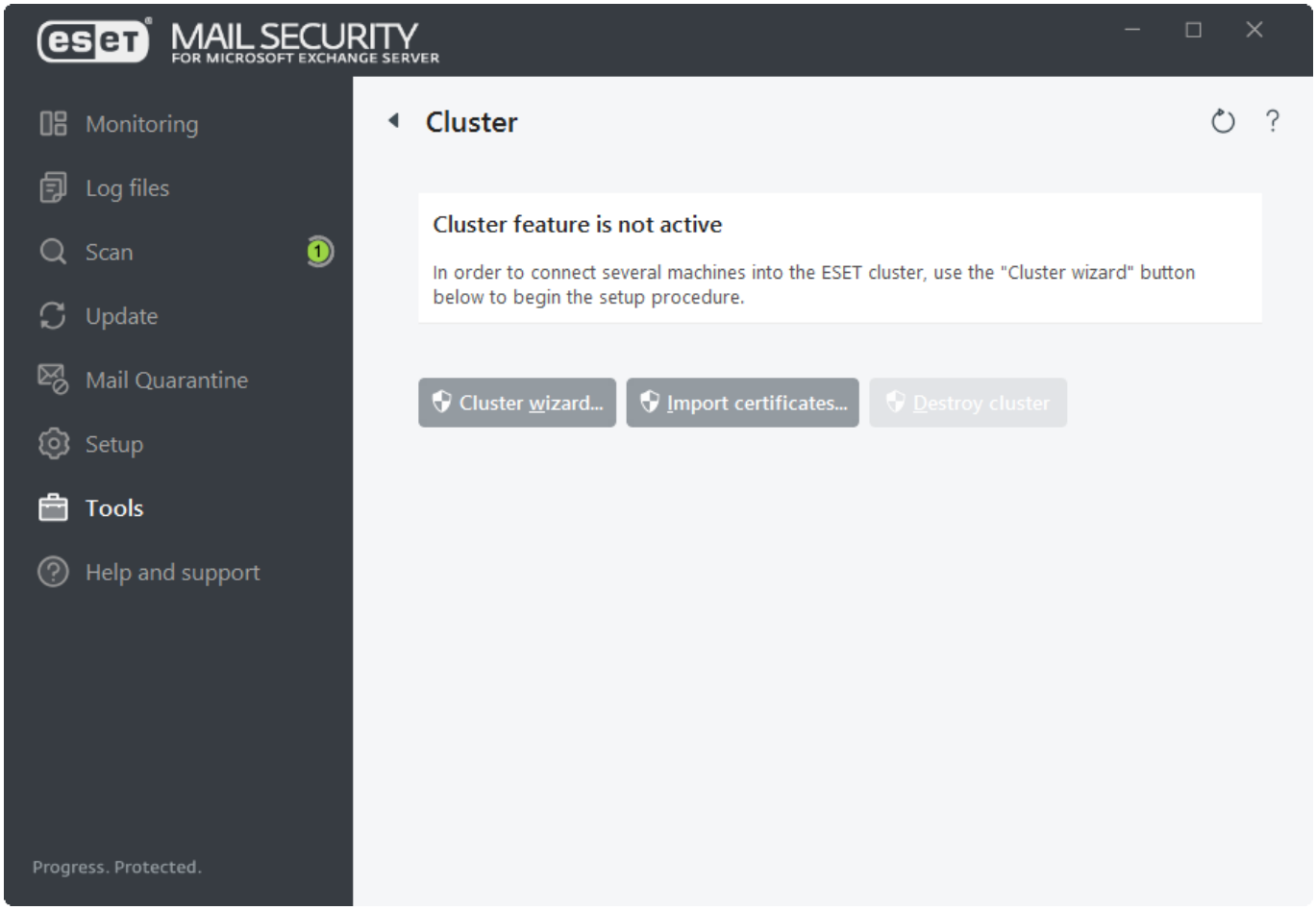
Muestra la información procesada por VSAPI (cantidad de promedios distintos para Hoy, para los Últimos 7 días y los promedios Desde el último reinicio).

Clúster

El Clúster de ESET es una infraestructura de comunicación P2P de la línea de productos ESET para Microsoft Windows Server. Usar el Clúster de ESET es ideal si tiene una infraestructura de Exchange con varios servidores, como DAG.

Esta infraestructura permite que los productos del servidor de ESET se comuniquen entre sí e intercambien información, como la configuración y las notificaciones, y pueden sincronizar las bases de datos de listas grises y sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias de productos. Un ejemplo de dichos grupos es un grupo de nodos en un Clúster de Windows Failover o Equilibrio de carga de la red (NLB) con un producto ESET instalado donde sea necesario contar con la misma configuración del producto a lo largo de todo el clúster. Los Clústeres de ESET aseguran esta consistencia entre las instancias.

> i La configuración de la interfaz del usuario y las tareas programadas no se sincronizan entre los nodos del clúster de ESET. Esto es a propósito. Por ejemplo, para evitar la ejecución programada y simultánea de una exploración de base de datos a pedido en todos los nodos del clúster, lo que provocaría problemas de rendimiento innecesarios.
> Los registros de protección del servidor de correo electrónico se mantienen separados para cada nodo del clúster; por lo tanto, los registros no se sincronizan. Puede utilizar la función Exportar al servidor syslog en cada nodo para duplicar los registros en el servidor Syslog en formato CEF o para utilizarlos con la herramienta SIEM. También puede usar exportar a registros de servicios y aplicaciones de Windows si prefiere recopilar los registros desde ese nivel.



> la creación de los clústeres de ESET entre ESET Mail Security y Seguridad de archivos de ESET para Linux no son compatibles.

Al configurar el Clúster de ESET, hay dos formas de agregar nodos:

- **Autodetectar** – Si tiene un clúster de Windows de conmutación por error/NLB existente, Autodetectar agregará de forma automática sus nodos miembros al clúster de ESET.
- **Examinar**: para agregar los nodos en forma manual, ingrese los nombres de servidor (ya sean miembros del mismo grupo de trabajo o del mismo dominio).

> Cuando se libera un correo electrónico de cuarentena, ESET Mail Security ignora el encabezado `To:` MIME porque se puede alterar fácilmente. En cambio, usa la información del destinatario original del comando `RCPT TO:` adquirida durante la conexión de SMTP. De esta manera, se garantiza que el destinatario correcto del correo reciba el mensaje liberado de cuarentena.

Una vez que haya agregado los nodos a su clúster de ESET, el siguiente paso es la instalación de ESET Mail Security en cada uno de ellos. Esto se hace en forma automática durante la configuración del clúster de ESET. Credenciales necesarias para la instalación remota de ESET Mail Security en otros nodos de clúster:

- **Escenario de dominio**: credenciales del administrador de dominios.
- **Escenario de un grupo de trabajo**: debe asegurarse de que todos los nodos usen las mismas credenciales de la cuenta del administrador local

En un clúster de ESET, también puede usar una combinación de nodos agregados en forma automática como parte de los clústeres de Windows Failover/NLB existentes y los nodos agregados en forma manual (siempre que

se encuentren dentro del mismo dominio).

No puede combinar los nodos de dominio con los nodos de grupos de trabajo.

Otro requisito para el uso de un clúster de ESET es que la función **Compartir archivos e impresoras** debe encontrarse habilitada dentro del Firewall de Windows antes de forzar la instalación de ESET Mail Security en los nodos del clúster de ESET.

Puede agregar los nuevos nodos a un clúster de ESET existente en cualquier momento a través del Asistente de clúster.

Certificados de importación

Se utilizan certificados para ofrecer autenticación máquina a máquina robusta cuando se utiliza HTTPS. Para cada clúster de ESET hay una jerarquía de certificados independiente. La jerarquía tiene un certificado raíz y un conjunto de certificados de nodo firmados por el certificado raíz. La clave privada del certificado raíz se destruye después de crear todos los certificados de nodo. Al agregar un nuevo nodo al clúster, se crea una nueva jerarquía de certificados. Navegue hasta la carpeta que contiene los certificados (que fueron generados durante el asistente de clústeres). Seleccione el archivo del certificado y haga clic en **Abrir**.

Destruir clúster

Es posible desarmar los clústeres de ESET. Cada nodo escribirá un informe en su registro de eventos sobre la destrucción del clúster de ESET. Luego, todas las reglas del firewall de ESET se eliminan del Firewall de Windows. Los nodos anteriores vuelven a su estado anterior y pueden volver a usarse en otro clúster de ESET, de ser necesario.

Asistente del clúster - Seleccionar nodos

El primer paso al configurar un clúster de ESET es agregar los nodos. Para agregar los nodos, puede usar la opción **Autodetectar** o **Explorar**. Asimismo, puede ingresar el nombre del servidor dentro del cuadro de texto y hacer clic en **Agregar**.

Autodetectar

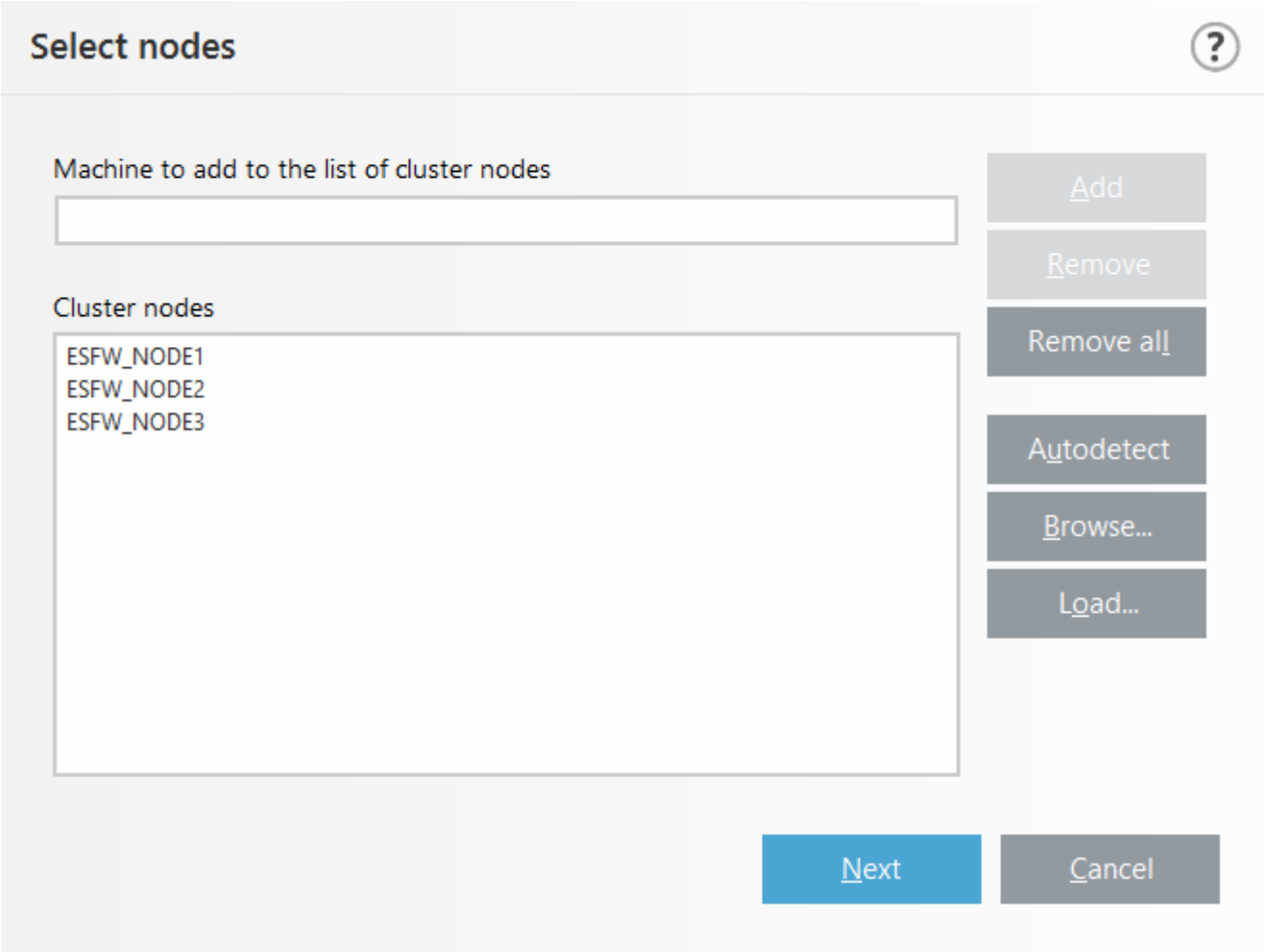
Agrega en forma automática los nodos desde un clúster de Windows Failover Cluster/Network Load Balancing (NLB) Cluster. Para poder agregar los nodos en forma automática, es necesario que el servidor que usa para crear el clúster de ESET sea parte de este clúster de Windows Failover Cluster/NLB Cluster. El clúster NLB debe tener habilitada la opción **Permitir control remoto** en las propiedades de clúster para que el pueda detectar los nodos en forma correcta. Una vez que tenga la lista de los nodos agregados recientemente.

Examinar

Para buscar y seleccionar los equipos dentro de un Domain o un Workgroup. Este método permite agregar los nodos al clúster de ESET de forma manual. Otra forma de agregar los nodos es escribir el nombre del host del servidor que desea agregar y hacer clic en **Agregar**.

Cargar

Para importar la lista de nodos del archivo.



Para modificar los **Nodos de clúster** en el listado, seleccione el clúster que desea quitar y haga clic en **Eliminar**, o para vaciar la lista completa, haga clic en **Eliminar todos**.

Si ya cuenta con un clúster de ESET, puede agregarle los nodos nuevos en cualquier momento. Los pasos a seguir son los mismos.

> i todos los nodos que se mantienen en el listado deben encontrarse en línea y ser accesibles. Por defecto, el host local se agrega a los nodos de clúster.

Asistente del clúster - Configuración del clúster

Define el nombre del clúster y los atributos específicos de la red (si es necesario).

Nombre del clúster

Escriba un nombre para su clúster y haga clic en Siguiente.

Puerto de escucha (el puerto predeterminado es 9777)

En caso de que ya esté utilizando el puerto 9777 en su entorno de red, especifique otro número de puerto que no esté en uso.

Abrir puerto en Windows firewall

Cuando se selecciona, se crea una regla en el Firewall de Windows.

Asistente del clúster - Configuración de instalación de clúster

Defina el modo de distribución del certificado y si se instala el producto en otros nodos o no.

Distribución de certificados

- **Remoto automático**: el certificado se instalará en forma automática.
- **Manual**: **Haga clic en Generar** y seleccione la carpeta adecuada en donde almacenar los certificados. Se creará un certificado de raíz al igual que un certificado por cada nodo, incluido el que se usa (máquina local) para configurar el clúster de ESET. Para inscribir el certificado en la máquina local, haga clic en **Sí**.

Instalación del producto a otros nodos

- **Remoto automático**:ESET Mail Security se instalará automáticamente en cada nodo (siempre y cuando los sistemas operativos sean de la misma arquitectura).
- **Manual**: Instalación ESET Mail Security manual (por ejemplo, cuando cuenta con diferentes arquitecturas de sistemas operativos en algunos de los nodos).

Enviar licencia a nodos sin un producto activado

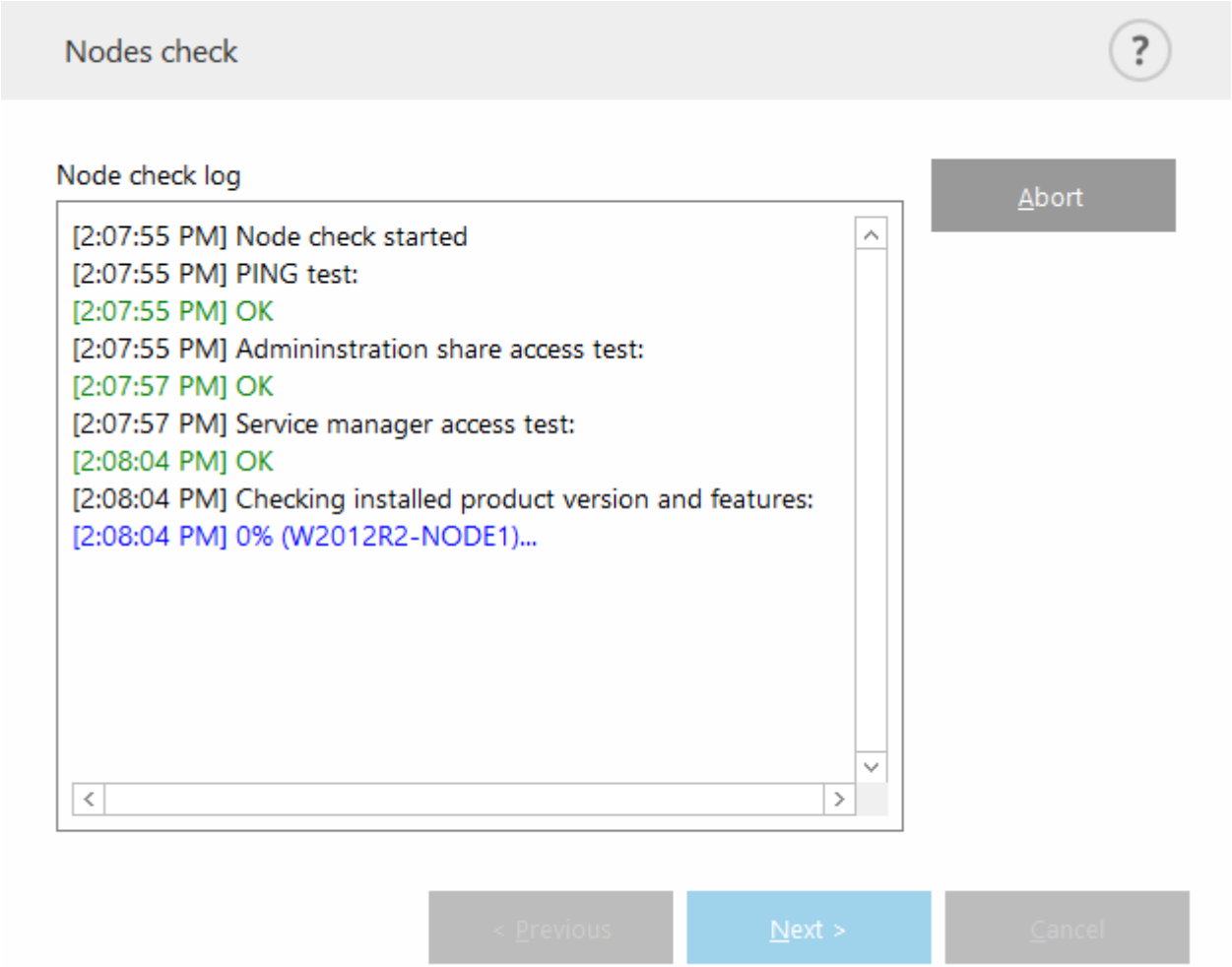
ESET Security activará automáticamente ESET Solutions instalada en los nodos sin licencias.

> Para crear un Clúster de ESET con una arquitectura de los sistemas operativos mixtos (32 y 64 bits), instale ESET Mail Security en forma manual. Los sistemas de operación en uso se detectarán en los pasos siguientes y verá esta información en la ventana de registro.

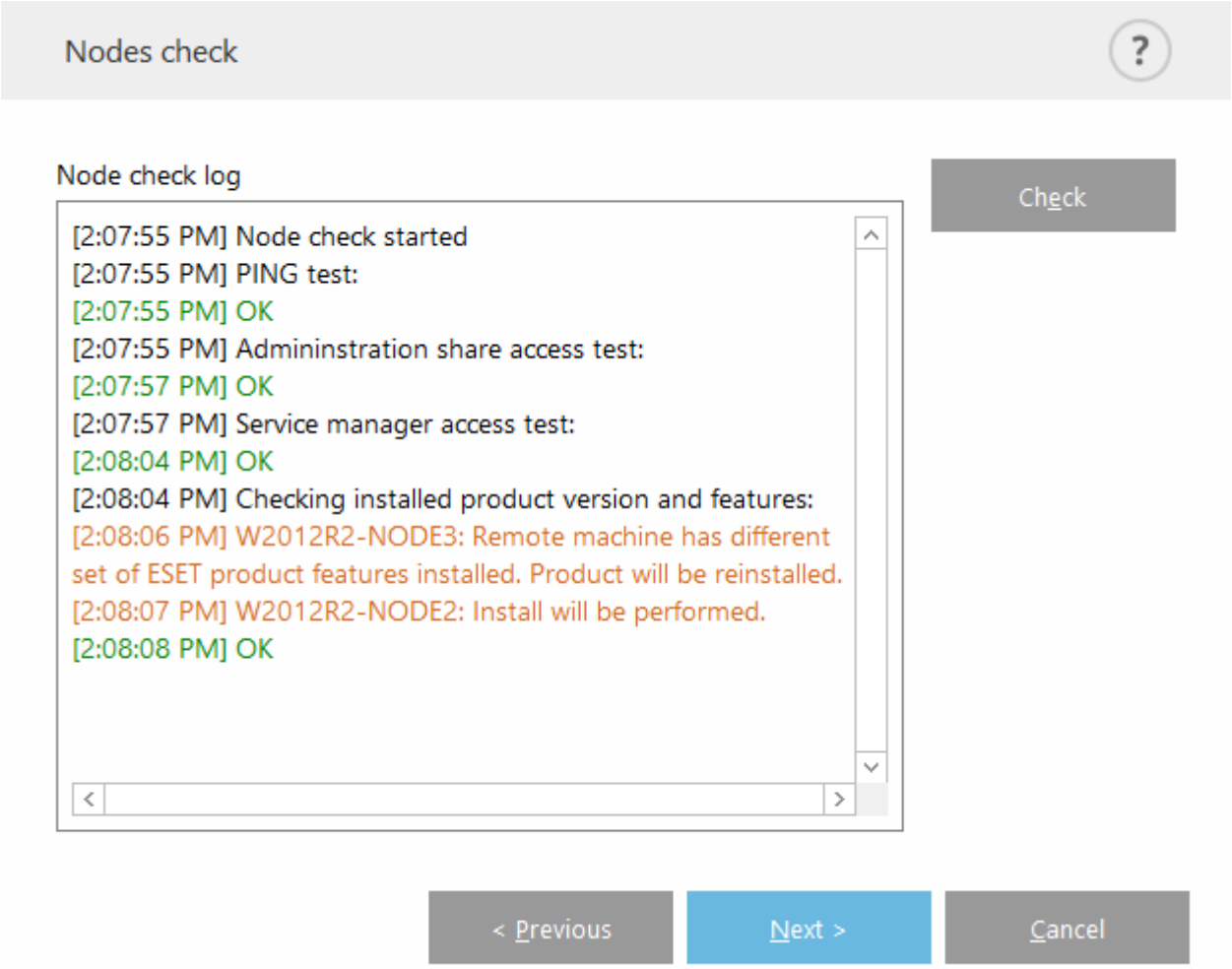
Asistente del clúster - Verificación de nodos

Luego de especificar los detalles de la instalación, se lleva a cabo una verificación del nodo. La siguiente información se mostrará en el **Registro de verificación de nodos**:

- verifique que todos los nodos existentes se encuentren en línea
- verifique que se pueda acceder a todos los nodos
- el nodo se encuentra en línea
- se puede acceder a la porción de administrador
- es posible la ejecución remota
- las versiones de producto correctas (o ningún producto) se instalaron
- verifique que los nuevos certificados estén presentes

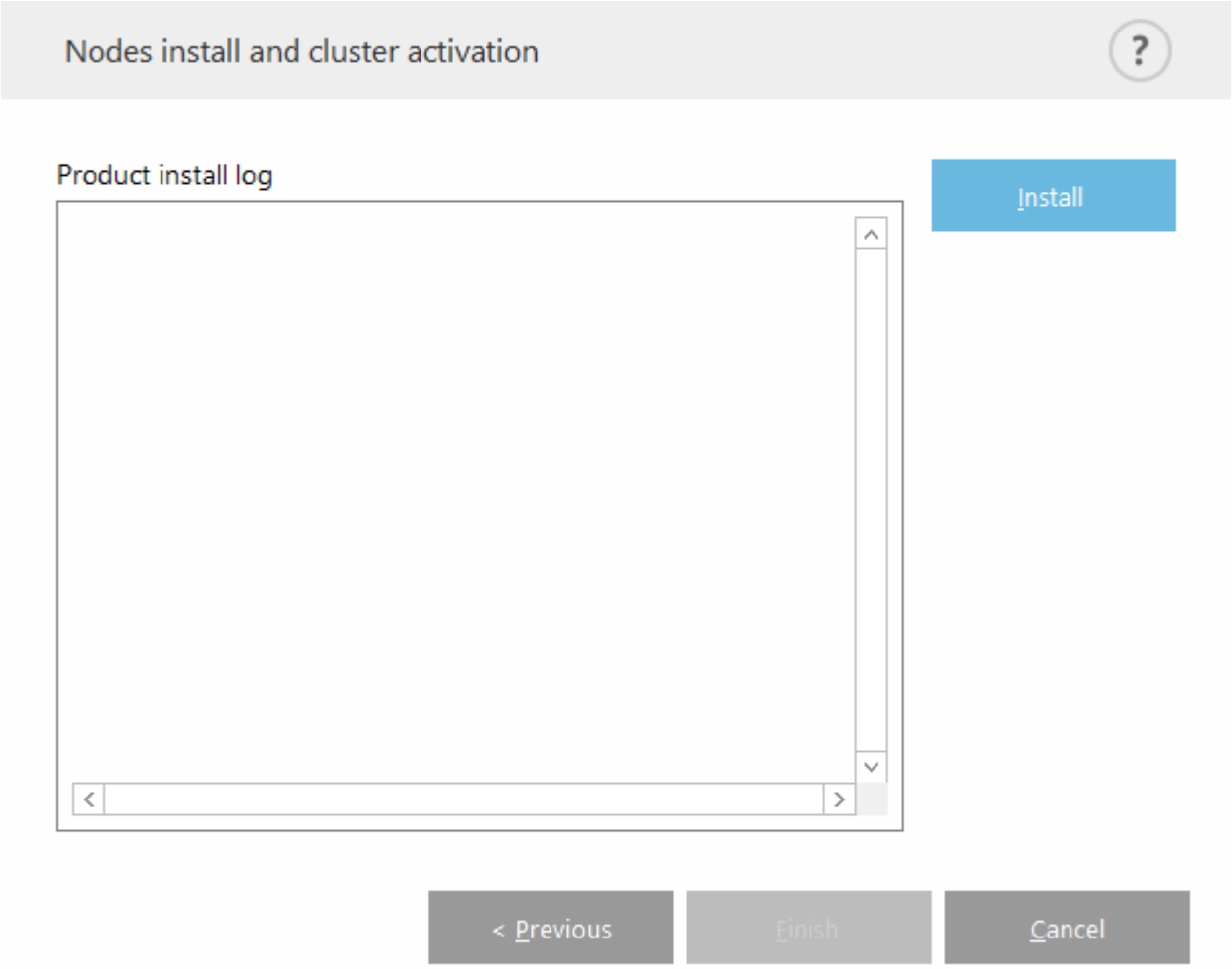


Verá el informe una vez que finalice la verificación del nodo:

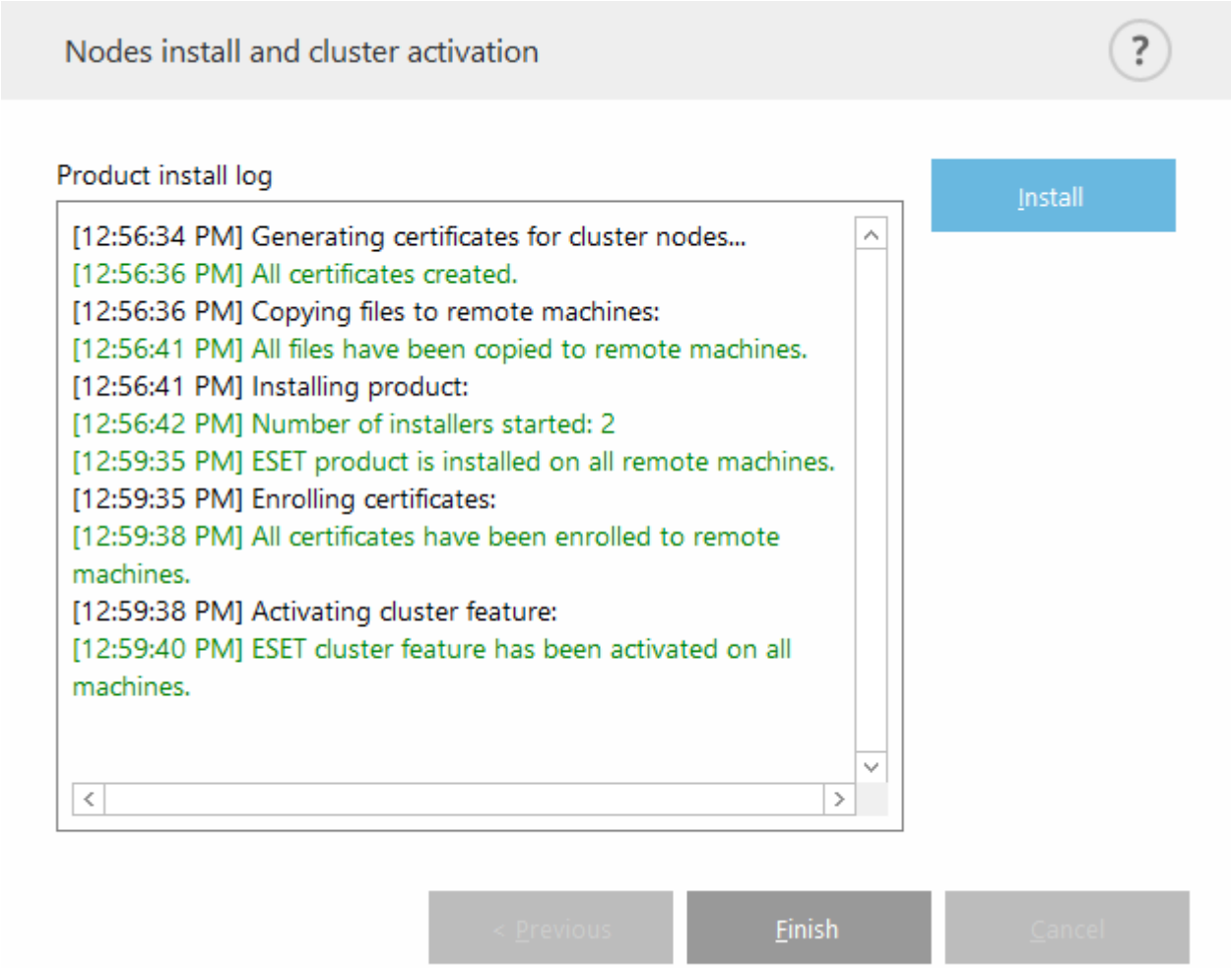


Asistente del clúster - Instalación de nodos

Cuando se instala en una máquina remota durante la inicialización del clúster de ESET, el asistente intentará localizar el instalador en el directorio *%ProgramData%\ESET\ESET Security\Installer*. Si no se encuentra el paquete del instalador en esa ubicación, se le solicitará localizar el archivo del instalador.



> Al intentar usar la instalación remota automática para un nodo con una arquitectura diferente (32 bit vs 64 bit), se detectará y se indicará realizar una instalación manual.



Una vez que haya configurado el clúster de ESET en forma correcta, aparecerá como habilitado en la página **Configuración** > **Servidor**.

> Si ya se encuentra instalada una versión anterior de ESET Mail Security en algunos nodos, se le notificará que se requiere la última versión en estas máquinas. Actualizar ESET Mail Security puede causar un reinicio automático.

Asimismo, puede verificar su estado actual en la página de estado del clúster (**Herramientas** > **Clúster**).

Shell de ESET

eShell (abreviación de Shell de ESET) es una interfaz de línea de comandos para ESET Mail Security. Es una alternativa a la interfaz gráfica de usuario (GUI). eShell cuenta con todas las características y opciones que la GUI normalmente le brinda. eShell permite configurar y administrar el programa completo sin necesidad de usar la GUI.

Además de todas las funciones y funcionalidades disponibles en la GUI, también ofrece la opción de automatizar tareas mediante la ejecución de scripts para configurar, modificar la configuración o realizar una acción. Asimismo, eShell puede resultar útil para quienes prefieren usar la línea de comandos en lugar de la GUI.

Para la funcionalidad completa, le recomendamos abrir eShell con Ejecutar como administrador. Lo mismo se aplica a la ejecución de un solo comando del símbolo del sistema de Windows (cmd). Abra el símbolo del sistema mediante **Ejecutar como administrador**. Si no puede ejecutar el símbolo del sistema como administrador, no se le permitirá ejecutar los comandos debido a la falta de permisos.

eShell se puede ejecutar en dos modos:

1. **Modo interactivo**: es útil cuando desea trabajar con eShell (no solamente ejecutar un único comando), por ejemplo, para aquellas tareas como cambiar la configuración, visualizar registros, etc. Puede usar el modo interactivo si aún no se familiarizó aún con los comandos. El modo interactivo hace que el desplazamiento por eShell sea más sencillo. Además, muestra los comandos disponibles que puede usar dentro de un contexto determinado.

2. **Comando simple/modo de procesamiento por lotes**: puede usar este modo si solamente necesita ingresar un comando sin ingresar al modo interactivo de eShell. Esto puede realizarlo desde el Símbolo de sistema de Windows al escribir en `eshell` con los parámetros apropiados.

```
eshell get status or eshell computer set real-time status disabled 1h
```

Para ejecutar ciertos comandos (como el segundo ejemplo anterior) en modo de procesamiento por lotes/script, primero debe configurar una serie de configuraciones. De lo contrario, recibirá un mensaje de **Acceso denegado**. Esto es por razones de seguridad.

Los cambios de configuración son necesarios para usar los comandos eShell de símbolo del sistema de Windows. Obtenga más información sobre cómo ejecutar archivos por lotes.

Hay dos maneras de entrar en modo interactivo en eShell:

1. Desde el **menú de inicio de Windows**: Iniciar > Todos los programas > ESET > ESET Mail Security > ESET Shell

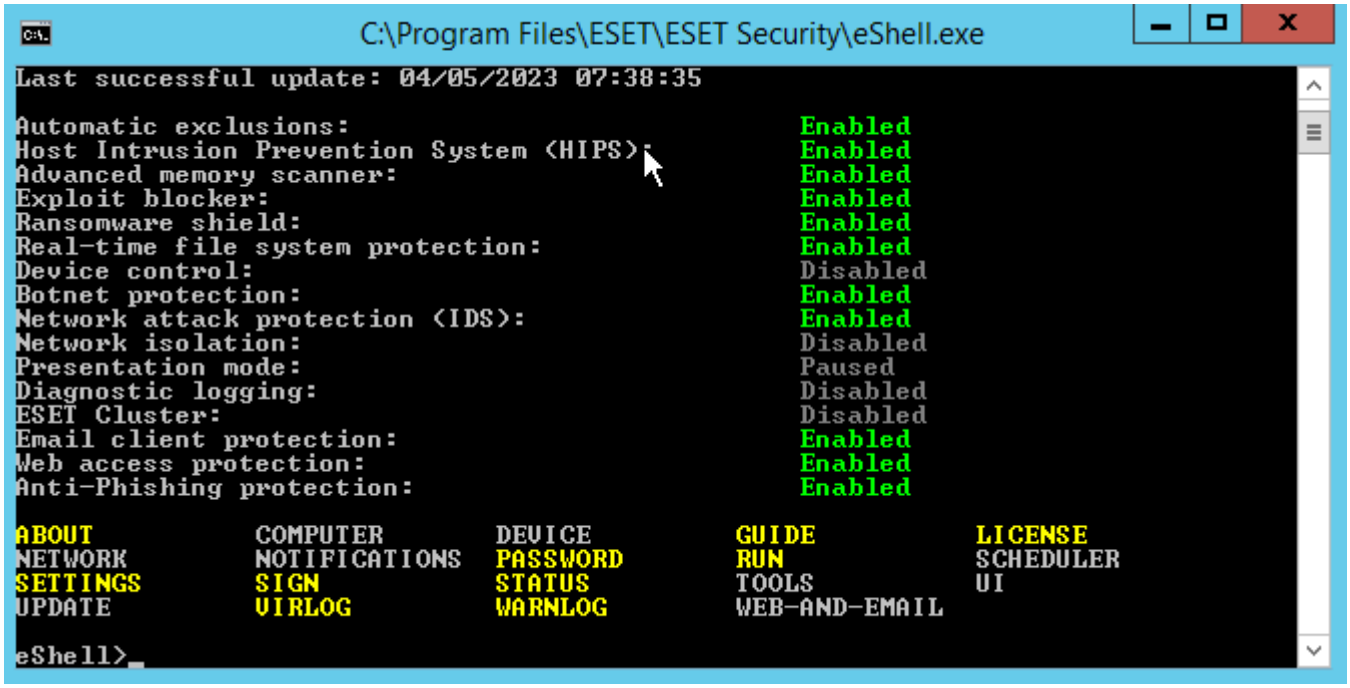
2. Desde **Símbolo del sistema de Windows**, tras escribir `eshell` y presionar la tecla Intro

Si obtiene un error `'eshell' not recognized as an internal or external command`, esto se debe a que las nuevas variables de entorno no fueron cargadas por su sistema luego de la instalación de ESET Mail Security.
Abra un nuevo Símbolo del sistema e intente iniciar eShell nuevamente. Si sigue recibiendo un error o tiene una Instalación de núcleo de ESET Mail Security, inicie eShell usando una ruta absoluta, por ejemplo `"%PROGRAMFILES%\ESET\ESET Mail Security\eShell.exe"` (debe utilizar `""` para que el comando funcione).

Al ejecutar eShell en modo interactivo por primera vez, se mostrará la pantalla de primera vista (guía).

Si quiere mostrar la primera pantalla de ejecución en el futuro, escriba el comando `guide`. Le muestra algunos ejemplos básicos de uso de eShell con Sintaxis, Prefijo, Ruta del comando, Formas abreviadas, Alias, etc.

La próxima vez que ejecute eShell, verá esta pantalla:



> Los comandos no distinguen mayúsculas de minúsculas. Puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Personalización de eShell

Puede personalizar eShell en contexto `ui eshell`. Puede configurar alias, colores, lenguaje, política de ejecución para scripts, configuración de comandos ocultos y mucho más.

Uso

Sintaxis

Los comandos deben formatearse con la sintaxis correcta para que funcionen y pueden estar compuesto por prefijos, contextos, argumentos, opciones, etc. Esta es la sintaxis general que se usa en eShell:

[<prefix>] [<command path>] <command> [<arguments>]

> Ejemplo (para activar la protección de documentos):
> `SET COMPUTER SCANS DOCUMENT REGISTER ENABLED`

`SET`: un prefijo

`COMPUTER SCANS DOCUMENT`: ruta a un comando en particular, un contexto al cual pertenece dicho comando

`REGISTER`: el comando en sí

`ENABLED`: un argumento para el comando

Al usar `?` como un argumento para el comando se mostrará la sintaxis para ese comando específico. Por ejemplo, `STATUS ?`le mostrará la sintaxis del comando `STATUS`:

SINTAXIS:

`[get] status`

OPERACIONES:

`get`: Mostrar el estado de todos los módulos de protección

Puede observar que `[get]` está entre corchetes. Quiere decir que el prefijo `get` es el prefijo predeterminado para el comando `status`. Esto significa que, cuando usted ejecuta `status` sin especificar un prefijo, se utilizará en realidad el prefijo predeterminado (en este caso,`get status`). Al usar comandos sin un prefijo, se ahorra tiempo al escribir. Por lo general, `get` es el prefijo predeterminado para la mayoría de los comandos, pero debe asegurarse cuál es el predeterminado para un comando en particular y qué es exactamente lo que usted desea ejecutar.

> i Los comandos no distinguen mayúsculas de minúsculas. Puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Prefijo/operación

Un prefijo es una operación. El prefijo `GET` le dará información acerca de cómo está configurada una característica determinada de ESET Mail Security, o le mostrará un estado (como `GET COMPUTER REAL-TIME STATUS`, que le mostrará el estado de protección actual). El prefijo `SET` configurará la funcionalidad o cambiará su estado (`SET COMPUTER REAL-TIME STATUS ENABLED` activará la protección).

Estos son los prefijos que eShell permite usar. Un comando puede soportar, o no, alguno de los siguientes prefijos:

GET	devuelve la configuración/estado actual
SET	establece un valor/estado
SELECT	selecciona un elemento
ADD	agrega un elemento
REMOVE	quita un elemento
CLEAR	elimina todos los elementos/archivos
START	inicia una acción
STOP	detiene una acción
PAUSE	pone una acción en pausa
RESUME	reanuda una acción
RESTORE	restaura las configuraciones/el objeto/el archivo predeterminado
SEND	envía un objeto o un archivo
IMPORT	importa desde un archivo
EXPORT	exporta a un archivo

> i Los prefijos como `GET` y `SET` se usan con muchos comandos; pero algunos comandos (como `EXIT`) no utilizan un prefijo.

Ruta del comando/contexto

Los comandos se ubican en contextos que conforman una estructura con forma de árbol. El nivel superior del árbol es “root”. Cuando ejecuta eShell, está en el nivel root:

eShell>

Puede ejecutar un comando desde allí o ingresar el nombre del contexto para navegar dentro del árbol. Por ejemplo, al ingresar el contexto TOOLS, se mencionarán todos los comandos y subcontextos disponibles.

Los elementos amarillos son los comandos que se pueden ejecutar y los grises son los subcontextos que se pueden ingresar. Un subcontexto contiene más comandos.

Si necesita volver a un nivel superior, use .. (dos puntos).

> ✔ Por ejemplo, si usted se encuentra aquí:
> eShell computer real-time>
> escriba .. para ir a un nivel superior, a:
> eShell computer>

Si quiere regresar a la raíz desde eShell computer real-time> (dos niveles más abajo que la raíz), simplemente escriba .. .. (dos puntos y dos puntos separados por un espacio). Al hacerlo, subirá dos niveles, que, en este caso, es la raíz. Utilice la barra invertida \ para regresar directamente a la raíz desde cualquier nivel, independientemente de la profundidad del árbol del contexto en la que se encuentre. Si desea ir a un contexto específico en niveles superiores, solo use el número adecuado de comandos .. para llegar al nivel deseado, con el espacio como separador. Por ejemplo, si quiere subir tres niveles, use .. ..

La ruta es relativa al contexto actual. Si el comando está incluido en el contexto actual, no ingrese una ruta. Por ejemplo, para ejecutar GET COMPUTER REAL-TIME STATUS ingrese:

GET COMPUTER STATUS: si usted está en el nivel root (la línea de comandos muestra eShell>)

GET STATUS: si usted está en el nivel COMPUTER (la línea de comandos muestra eShell computer>)

.. GET STATUS: si usted está en el nivel COMPUTER REAL-TIME (la línea de comandos muestra eShell computer real-time>)

Puede usar un solo . (punto) en lugar de dos .. porque un solo punto es una abreviatura de los dos puntos.

. GET STATUS: si usted está en el nivel COMPUTER REAL-TIME (la línea de comandos muestra eShell computer real-time>)

Argumento

Un argumento es una acción que se realiza para un comando específico. Por ejemplo, el comando CLEAN-LEVEL (ubicado en COMPUTER REAL-TIME ENGINE) puede usarse con los siguientes argumentos:

rigorous: Reparar siempre la detección

safe: Reparar detección si es seguro. Caso contrario, conservar.

normal: Reparar detección si es seguro. Caso contrario, consultar

none: preguntar siempre al usuario final

Otro ejemplo son los argumentos ENABLED o DISABLED, que se usan para habilitar o deshabilitar cierta característica o función.

Forma simplificada/comandos abreviados

eShell le permite abreviar los contextos, los comandos y los argumentos (siempre y cuando el argumento sea un modificador o una opción alternativa). No es posible abreviar un prefijo o un argumento que sea un valor concreto, como un número, un nombre o una ruta. Puede usar los números1 y 0, en lugar de los argumentos Enabled y Disabled.

```
computer set real-time status enabled        =>        com set real stat 1
computer set real-time status disabled        =>        com set real stat 0
```

Ejemplos de la forma abreviada:

```
computer set real-time status enabled        =>        com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext        =>        com excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1        =>        com excl rem det 1
```

En el caso de que dos comandos o contextos comiencen con las mismas letras (por ejemplo, ADVANCED y AUTO-EXCLUSIONS y usted ingresa A como comando abreviado), eShell no podrá decidir cuál de estos dos comandos desea ejecutar. Aparecerá un mensaje de error y la lista de los comandos que comienzan con “A”, desde donde usted podrá elegir uno:

eShell>a

El siguiente comando no es único: a

Los siguientes subcontextos están disponibles en el contexto de COMPUTER:

ADVANCED

AUTO-EXCLUSIONS

Si se agrega una o más letras (por ejemplo, AD en lugar de simplemente A) eShell entrará en el subcontexto ADVANCED debido a que ahora es único. Lo mismo sucede con los comandos abreviados.

> Para asegurarse de que el comando se ejecute como lo necesita, es recomendable no abreviar los comandos, los argumentos, etc. y usar la forma completa. De esta manera, eShell ejecutará exactamente lo que usted requiere y se evitarán errores no deseados. Es verdadero para archivos o scripts de procesamiento por lotes.

Finalización automática

Esta nueva característica se introdujo en eShell 2.0 y es muy similar a la terminación automática en Símbolo del sistema de Windows. Mientras que Símbolo del sistema de Windows completa rutas de archivos, eShell completa nombres de comandos, contextos y operaciones. No es compatible con la finalización de argumentos.

Si escribe un comando, solo presione la tecla Tab para completar o repasar el ciclo de variaciones disponibles.

Presione Shift + Tab para retroceder en el ciclo. No es compatible con la combinación de forma abreviada y la finalización automática. Use una de las dos.

Por ejemplo, cuando escribe `computer real-time additional`, si se presiona Tab, no ocurrirá nada. En cambio, si escribe `com` y, luego, presiona Tab para completar `computer` + Tab, y `real` + Tab, y `add` + Tab, presione Intro. Escriba `on` + Tab y siga presionando la tecla Tab para repasar todas las variaciones disponibles: `on-execute-ah, on-execute-ah-removable, on-write-ah, on-write-archive-default`, etc.

Alias

Un alias es un nombre alternativo que se puede usar para ejecutar un comando (siempre y cuando el comando tenga un alias asignado). Hay algunos alias predeterminados:

`(global) close`: exit

`(global) quit`: exit

`(global) bye`: exit

`warnlog`: tools log events

`virlog`: tools log detections

`(global)` El comando puede usarse en cualquier lugar, independientemente del contexto actual. Un comando puede tener varios alias asignados. Por ejemplo, el comando `EXIT` tiene los alias `CLOSE`, `QUIT` y `BYE`. Cuando quiere salir de eShell, puede usar el comando `EXIT` en sí o cualquiera de sus alias.

El alias `VIRLOG` es un alias para el comando `DETECTIONS`, que está ubicado en el contexto `TOOLS LOG`. De esta manera, el comando detecciones se encuentra disponible en el contexto ROOT`ROOT`, lo que simplifica el acceso a (no tiene que ingresar `TOOLS` y, luego, al contexto `LOG` y ejecutarlo directamente desde `ROOT`).

eShell le permite definir sus alias. El comando `ALIAS` se encuentra en el contexto `UI ESHELL`.

Configuraciones protegidas por contraseña

Las configuraciones de ESET Mail Security pueden estar protegidas por una contraseña. Puede establecer una contraseña con la interfaz gráfica de usuario o eShell por medio del `set ui access lock-password`.

Luego, deberá ingresar esta contraseña, de forma interactiva, para algunos comandos (como aquellos que cambian las configuraciones o modifican datos). Si planea trabajar con eShell por un período más prolongado y no

desea ingresar la contraseña reiteradamente, puede hacer que eShell recuerde la contraseña por medio del comando `set password` (ejecutar desde `root`). Su contraseña se completará en forma automática para cada uno de los comandos ejecutados que requieran de contraseña. Se recuerda hasta que salga de eShell, lo que significa que deberá volver a usar el comando `set password` cuando inicie una nueva sesión y quiera que eShell recuerde su contraseña.

Guía / Ayuda

Cuando ejecute el comando `GUIDE` o `HELP`, se mostrará la pantalla de “primera vista” donde se explica cómo usar eShell. El comando está disponible desde el contexto `ROOT` (`eShell>`).

Historial de comandos

eShell mantiene un historial de los comandos ejecutados previamente. Solo se aplica a los comandos de la sesión interactiva de eShell actual. Cuando haya salido de eShell, el historial de comandos quedará vacío. Use las teclas de flecha arriba y abajo del teclado para navegar por el historial. Al encontrar el comando que buscaba, puede ejecutarlo nuevamente o modificarlo sin necesidad de escribir el comando completo desde el comienzo.

CLS / Borrar los datos de la pantalla

El comando `CLS` puede usarse para borrar la pantalla. Funciona de la misma manera que con el Símbolo de comandos de Windows o interfaces de línea de comandos similares.

EXIT / CLOSE / QUIT / BYE

Para cerrar o salir de eShell, puede usar cualquiera de estos comandos (`EXIT`, `CLOSE`, `QUIT` o `BYE`).

Comandos

Esta sección enumera algunos comandos eShell básicos con descripciones.

> i Los comandos no distinguen mayúsculas de minúsculas. Puede usar letras en mayúscula o en minúscula y el comando igualmente se ejecutará.

Comandos de ejemplo (incluidos en el contexto de `ROOT`):

ACERCA DE

Presenta una lista informativa acerca del programa. Muestra información como:

- Nombre del producto de seguridad de ESET instalado y el número de la versión.
- Sistema operativo y detalles del hardware básicos.
- Nombre de usuario (dominio incluido), nombre completo del equipo (FQDN, si el servidor es miembro de un dominio(y nombre de Puesto.
- Los componentes instalados del producto de seguridad de ESET, incluyendo el número de la versión de cada componente.

RUTA CONTEXTUAL:

`root`

CONTRASEÑA

Para ejecutar comandos protegidos por contraseña, el programa le solicita ingresar una contraseña por razones de seguridad. Esto se aplica a los comandos que deshabilitan la protección y a los que pueden afectar la configuración de ESET Mail Security. Cada vez que ejecute este tipo de comandos, se le solicitará que ingrese una contraseña. Puede definir la contraseña para evitar tener que ingresar la contraseña todas las veces. eShell recordará e ingresará en forma automática cuando se ejecute un comando protegido por contraseña.

> Su contraseña funciona únicamente para la sesión interactiva actual de eShell. Al salir de eShell, la contraseña definida perderá su vigencia. Cuando vuelva a iniciar eShell, deberá definir nuevamente la contraseña.

La contraseña definida también se puede usar al ejecutar archivos o scripts por lotes sin firmar. Asegúrese de establecer la Directiva de ejecución del shell de ESET para tener Acceso completo al ejecutar archivos por lote sin firmar. Aquí se muestra un ejemplo de un archivo de procesamiento por lotes de ese tipo:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Este comando concatenado define una contraseña y deshabilita la protección.

> Recomendamos que use archivos por lote firmados, si es posible. De esta manera, evitará tener contraseñas sin formato en el archivo por lotes (su utiliza el método descrito anteriormente). Consulte Archivos por lote/Secuencia de comandos (sección Archivos por lote firmados) para obtener más detalles.

RUTA CONTEXTUAL:

`root`

SINTAXIS:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERACIONES:

`get`: mostrar la contraseña

`set`: establecer o borrar la contraseña

`restore`: borrar la contraseña

ARGUMENTOS:

`plain`: cambiar al tipo de la contraseña como un parámetro

`password`: contraseña

set password plain <yourpassword>: establece la contraseña que se usará para los comandos protegidos por contraseña
restore password: borra la contraseña

get password: use este comando para ver si la contraseña está configurada o no (esto solo muestra asteriscos "*", pero no muestra la contraseña), cuando no hay ningún asterisco, significa que la contraseña no está establecida
set password plain <yourpassword>: use este comando para establecer la contraseña definida
restore password: este comando borra la contraseña definida

ESTADO

Muestra información acerca del estado de protección en tiempo real de ESET Mail Security y le permite pausar o reanudar la protección (similar a la ventana del programa principal).

RUTA CONTEXTUAL:

computer real-time

SINTAXIS:

[get] status

set status enabled | disabled [10m | 30m | 1h | 4h | temporary]

restore status

OPERACIONES:

get: devuelve la configuración o el estado actual

set: establece el valor o el estado

restore: restaura la configuración predeterminada, el objeto o el archivo

ARGUMENTOS:

enabled: Habilitar la protección/función

disabled: Deshabilitar la protección/función

10m: Deshabilitar durante 10 minutos

30m: Deshabilitar durante 30 minutos

1h: Deshabilitar durante 1 hora

4h: Deshabilitar durante 4 horas

temporary: Deshabilitar hasta el reinicio

No puede deshabilitar todas las características de protección con un solo comando. Usando el comando status puede administrar los módulos y las características de protección uno por uno. Cada módulo o características de protección tiene su comando status.

Lista de características con el comando `status`:

Característica	Contexto y comando
Exclusiones automáticas	`COMPUTER AUTO-EXCLUSIONS STATUS`
Sistema de prevención de intrusiones basado en el host (HIPS)	`COMPUTER HIPS STATUS`
Protección del sistema de archivos en tiempo real	`COMPUTER REAL-TIME STATUS`
Control de dispositivos	`DEVICE STATUS`
Protección contra Botnets	`NETWORK ADVANCED STATUS-BOTNET`
Protección contra ataques en la red (IDS)	`NETWORK ADVANCED STATUS-IDS`
Aislamiento de red	`NETWORK ADVANCED STATUS-ISOLATION`
Clúster de ESET	`TOOLS CLUSTER STATUS`
Registro de diagnósticos	`TOOLS DIAGNOSTICS STATUS`
Modo de presentación	`TOOLS PRESENTATION STATUS`
Protección contra phishing	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Protección del cliente de correo electrónico	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Protección del acceso a la Web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Es un alias del comando `DETECTIONS`. Es útil cuando se necesita ver información sobre las infiltraciones detectadas.

WARNLOG

Es un alias del comando `EVENTS`. Es útil cuando se necesita ver información sobre los distintos eventos.

Accesos directos de teclado

El eShell admite accesos directos de teclado (similar al símbolo del sistema de Microsoft Windows *cmd.exe*). Use determinadas teclas (combinaciones de teclas) del teclado para realizar acciones en eShell. Por ejemplo, mostrar el historial de comandos, repetir parte del comando de historial, mover una palabra o borrar una línea.

Accesos directos disponibles:

F1: imprime los caracteres del comando de historial real uno por uno.

F2, X: repite parte del comando de historial; hasta el carácter X.

F3: escribe el comando de historial real.

F4, X: comenzando desde la posición actual del cursor en el comando real; elimina hasta el carácter X.

F5: igual que la FLECHA HACIA ARRIBA.

F7: muestra el historial de comandos.

ALT + F7: borra el historial de comandos.

F8: retrocede por el historial de comandos, pero solo muestra los comandos que coincidan con el texto actual en el símbolo del sistema.

F9: ejecuta un comando específico desde el historial de comandos.

FLECHA DERECHA: igual que F1.

CTRL + HOME: borre la línea a la izquierda.

CTRL + FIN: borra la línea a la derecha.

CTRL + FLECHA IZQUIERDA: mueve una palabra a la izquierda.

CTRL + FLECHA DERECHA: mueve una palabra a la derecha.

Archivos por lotes/ Cifrado

Puede usar eShell como una herramienta poderosa de cifrado para automatización. Para usar el archivo por lotes con eShell, cree uno con un eShell y realice comandos en el mismo.

```
eshell get computer real-time status
```

También puede vincular comandos, lo cual a veces es necesario. Por ejemplo, Si desea escribir una tarea programada determinada, escriba lo siguiente:

```
eshell select scheduler task 4 "&" get scheduler action
```

La selección del elemento (tarea número 4 en este caso) por lo general se aplica solo a una instancia de eShell que se esté ejecutando. Si quisiera ejecutar estos dos comandos uno tras otro, el segundo comando fallaría con el error “`"No task selected or selected task no longer exists"`”.

Por motivos de seguridad, la política de ejecución está ajustada como **Scripts limitados** de forma predeterminada. Esta configuración le permite usar eShell como herramienta de supervisión, pero no le permitirá efectuar cambios en la configuración de ESET Mail Security mediante la ejecución de un script. Si intenta ejecutar un script con comandos que pueden afectar a la seguridad, por ejemplo, desactivar la protección, verá el mensaje **Acceso denegado**. Le recomendamos usar archivos de lote firmados para ejecutar comandos que realicen cambios sobre la configuración.

Para cambiar la configuración mediante un único comando ingresado manualmente en la Solicitud de Comando de Windows, debe otorgar acceso completo de eShell (no recomendado). Para otorgar acceso completo, utilice `ui eshell shell-execution-policy` en el modo Interactivo de eShell en sí, o a través de la interfaz gráfica de usuario en **Configuración avanzada** (**F5**) > **Interfaz del usuario** > ESET Shell.

Archivos por lotes firmados

eShell le permite asegurar archivos por lotes comunes (**.bat*) con una firma. Los scripts se firman con la misma contraseña que se usa para proteger las configuraciones. Para firmar un script primero debe habilitar la protección de las configuraciones. Esto se puede hacer a través de la ventana principal del programa, o desde eShell con el comando `set ui access lock-password`. Una vez que se configura la contraseña de protección de la configuración, puede comenzar a firmar archivos en lotes.

> Debe volver a firmar todos los scripts si cambia la contraseña de la protección de configuración. De lo contrario, los scripts no podrán ejecutar el siguiente cambio de contraseña. La contraseña ingresada al firmar el script debe coincidir con la contraseña de protección de las configuraciones en el sistema destino.

Para firmar un archivo de lote, ejecute `sign <script.bat>` del contexto raíz de eShell, donde script.bat*script.bat* es la ruta al script que desea firmar. Ingrese y confirme la contraseña que se usará para firmar. Esta contraseña debe coincidir con la contraseña de protección de las configuraciones. La firma se coloca al final del archivo por lotes en forma de un comentario. Si este script ya se ha firmado, la firma se reemplazará por una nueva.

> Al modificar un archivo por lotes que ya ha sido firmado, debe volverse a firmar.

Para ejecutar un archivo por lotes firmado desde el Símbolo de sistema de Windows o como una tarea programada, use el siguiente comando:

```
eshell run <script.bat>
```

Donde *script.bat* es la ruta al archivo por lotes.

```
eshell run d:\myeshellscript.bat
```

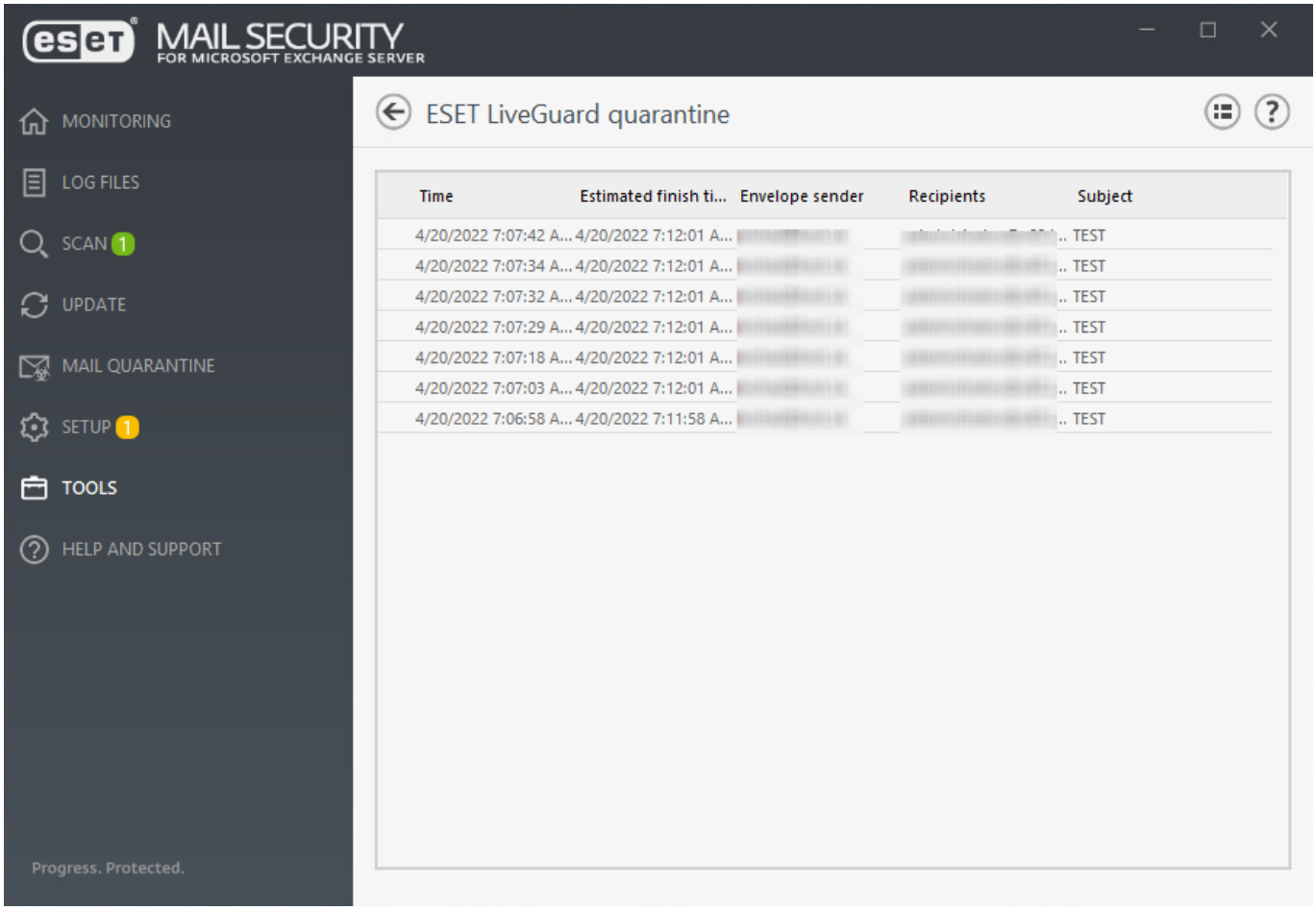
ESET LiveGuard Advanced

ESET LiveGuard Advanced brinda otra capa de seguridad mediante el uso de tecnología avanzada basada en la nube de ESET para detectar amenazas nuevas, nunca antes vistas. Es un servicio de pago, si bien es similar a ESET LiveGrid®, ESET LiveGuard Advanced le ofrece la ventaja de protegerse de posibles consecuencias provocadas por nuevas amenazas. Si ESET LiveGuard Advanced detecta código o comportamiento sospechoso, evita más actividades de amenaza al ponerlo temporalmente en cuarentena en ESET LiveGuard Advanced.

Una muestra sospechosa (archivo o mensaje de correo electrónico) se envía automáticamente a ESET Cloud, donde el servidor de ESET LiveGuard Advanced la analiza con motores de detección de malware de vanguardia. Mientras los archivos o los correos electrónicos se encuentran en cuarentena ESET LiveGuard Advanced, ESET Mail Security espera los resultados del servidor de ESET LiveGuard Advanced.

Después de completar el análisis, ESET Mail Security recibe un informe con un resumen del comportamiento de la muestra observada. Si la muestra resulta ser inofensiva, se libera de la cuarentena ESET LiveGuard Advanced, de lo contrario, se mantiene en cuarentena. Si es un falso positivo y está seguro de que el archivo o correo electrónico no es una amenaza, puede liberarlo manualmente desde la cuarentena de ESET LiveGuard Advanced antes de que ESET Mail Security reciba los resultados del servidor ESET LiveGuard Advanced.

Por lo general, los resultados de ESET LiveGuard Advanced para las muestras se reciben en pocos minutos para los mensajes de correo electrónico. Sin embargo, el intervalo de espera predeterminado es de 5 minutos. En raras ocasiones, cuando los resultados de ESET LiveGuard Advanced no llegan dentro del intervalo, se publica el mensaje. Puede cambiar el intervalo al tiempo que prefiera (entre 5 y 60 minutos, en incrementos de 1 minuto).



La característica de ESET LiveGuard Advanced es visible en ESET Mail Security sin importar su estado de activación. En caso de no tener licencia, ESET LiveGuard Advanced está inactivo. La licencia ESET LiveGuard Advanced está administrada por ESET PROTECT y la activación en sí debe realizarse desde ESET PROTECT utilizando una política.

Una vez que haya activado ESET LiveGuard Advanced, se creará su propio perfil ESET LiveGuard Advanced en el servidor ESET LiveGuard Advanced. Este perfil almacenará todos los resultados de análisis ESET LiveGuard Advanced de las muestras enviadas por su ESET Mail Security.

Para que la función ESET LiveGuard Advanced comience a hacer efecto, es necesario que cumpla con lo siguiente:

ESET Mail Security administrado a través de ESET PROTECT

ESET Mail Security activado usando la licencia ESET LiveGuard Advanced

Habilitar ESET LiveGuard Advanced en su ESET Mail Security al usar ESET PROTECT política

De este modo, podrá sacar el máximo provecho de ESET LiveGuard Advanced, así como de enviar de forma manual un archivo de muestra para el análisis ESET LiveGuard Advanced.

ESET SysInspector

ESET SysInspector es una aplicación que inspecciona minuciosamente su equipo, recopila información detallada sobre los componentes del sistema (como las aplicaciones y los controladores instalados, las conexiones de red o las entradas de registro importantes) y evalúa el nivel de riesgo de cada componente.

Esta información puede ayudar a determinar la causa del comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de códigos maliciosos.

Haga clic en **Crear** e ingrese un breve **Comentario** que describa el registro que se va a crear. Espere hasta que el registro de ESET SysInspector se haya generado (se mostrará el estado como Creado). La creación del registro puede llevar bastante tiempo, según la configuración del hardware y los datos del sistema.

La ventana ESET SysInspector muestra la siguiente información sobre los registros creados:

- **Hora**: la hora de creación del registro.
- **Comentario**: un breve comentario.
- **Usuario**: el nombre del usuario que creó el registro.
- **Estado**: el estado de la creación del registro.

Están disponibles las siguientes opciones:

- **Mostrar**: abre el registro creado. También puede hacer clic con el botón secundario en un registro y seleccionar **Mostrar** desde el menú contextual.
- **Crear**: crea un registro nuevo. Escriba un breve comentario que describa el registro que se creará y haga clic en **Crear**. Espere hasta que el registro de ESET SysInspector se haya completado (se mostrará el **Estado** como Creado).
- **Eliminar**: elimina los registros seleccionados de la lista.

Al hacer un clic con el botón secundario en uno o varios registros seleccionados, se ofrecen las siguientes opciones desde el menú contextual:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (equivale a hacer doble clic en el registro).
- **Crear**: crea un registro nuevo. Escriba un breve comentario que describa el registro que se creará y haga clic en **Crear**. Espere hasta que el registro de ESET SysInspector se haya completado (se mostrará el **Estado** como Creado).
- **Eliminar**: elimina los registros seleccionados de la lista.
- **Eliminar todo**: elimina todos los registros.
- **Exportar**: exporta el registro al archivo *.esil*. Como alternativa, elija un archivo *.xml* o comprimido *.xml*.

ESET SysRescue Live

ESET SysRescue Live es una utilidad que le permite crear un disco de arranque de unidad USB o CD/DVD de rescate. Puede arrancar un equipo infectado con sus medios de rescate y, luego, explorar para detectar malware y limpiar archivos infectados.

La ventaja principal de ESET SysRescue Live es que la solución ESET Security se ejecuta en forma independiente del sistema operativo del host, pero cuenta con acceso directo al disco y al sistema de archivos. De esta forma, es posible quitar las amenazas que normalmente no se podrían eliminar, por ejemplo, mientras el sistema operativo

está activo, etc.

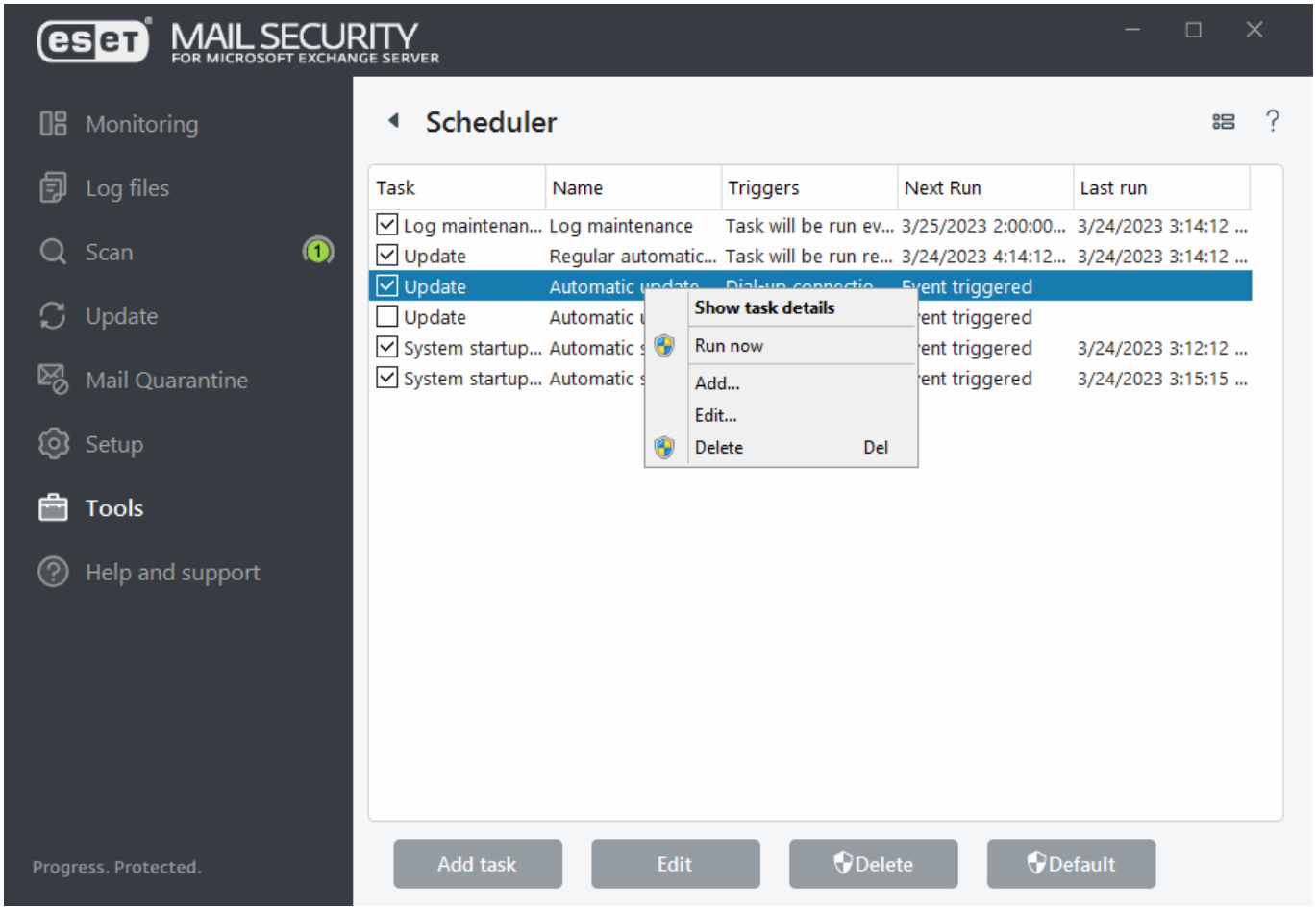
Tareas programadas

Tareas programadas administra y ejecuta las tareas programadas en función de los parámetros definidos. Puede ver una lista de todas las tareas en forma de tabla y muestra sus parámetros, como tipo de Tarea, Nombre de la tarea, Hora de ejecución y Última ejecución. Además, puede crear nuevas tareas programadas haciendo clic en Agregar tarea. Para editar la configuración de una tarea programada existente, haga clic en el botón **Editar**. Restaure la lista de las tareas programadas a la configuración predeterminada, haga clic en **Predeterminado** y, luego, en **Restaurar a predeterminado** todos los cambios que se realizaron se perderán, y esta acción no se puede deshacer.

Hay un conjunto de tareas predeterminadas definidas previamente:

- Mantenimiento de registros
- Actualización automática regular (utilice esta tarea para actualizar la frecuencia)
- Actualización automática tras conexión de acceso telefónico
- Actualización automática tras el registro del usuario
- Exploración automática de archivos durante el inicio del sistema (después del registro del usuario)
- Exploración automática de archivos durante el inicio del sistema (después de una actualización exitosa de los módulos)

Seleccione las casillas de verificación apropiadas para activar o desactivar tareas.



Para realizar las siguientes acciones, haga clic con el botón secundario en una tarea:

Mostrar detalles de la tarea	Muestra información detallada sobre una tarea programada al hacer doble clic o clic con el botón secundario en la tarea programada.
Ejecutar ahora	Ejecuta una tarea seleccionada del programador y la realiza de inmediato.
Agregar...	Inicia un asistente que le ayudará a crear una nueva tarea programada.
Editar...	Editar la configuración de una tarea programada existente (ya sea predeterminada o definida por el usuario).
Eliminar	Elimina una tarea existente.

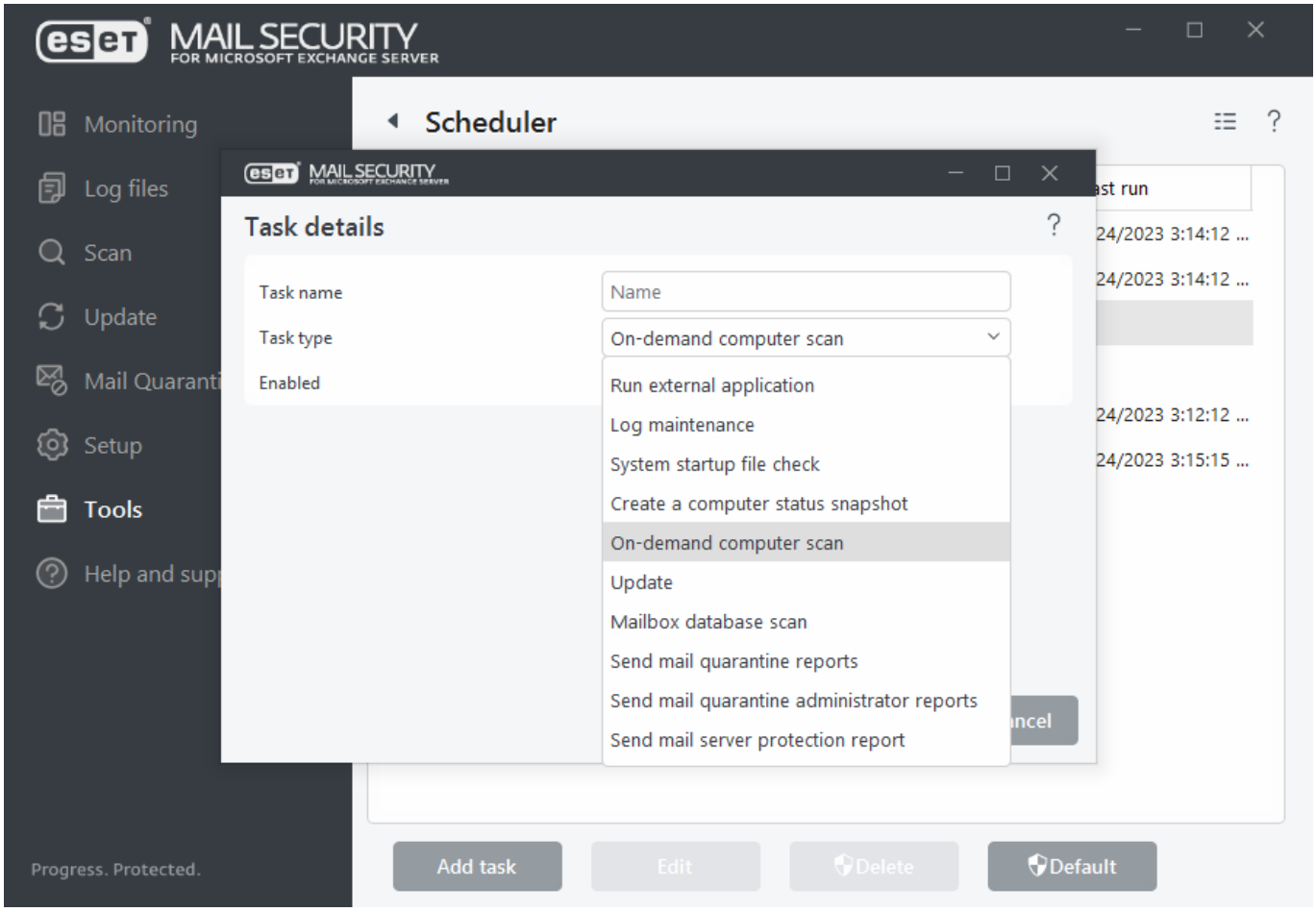
Tareas programadas: Agregar tarea

Para crear una nueva tarea programada:

1. Haga clic en **Agregar tarea**.

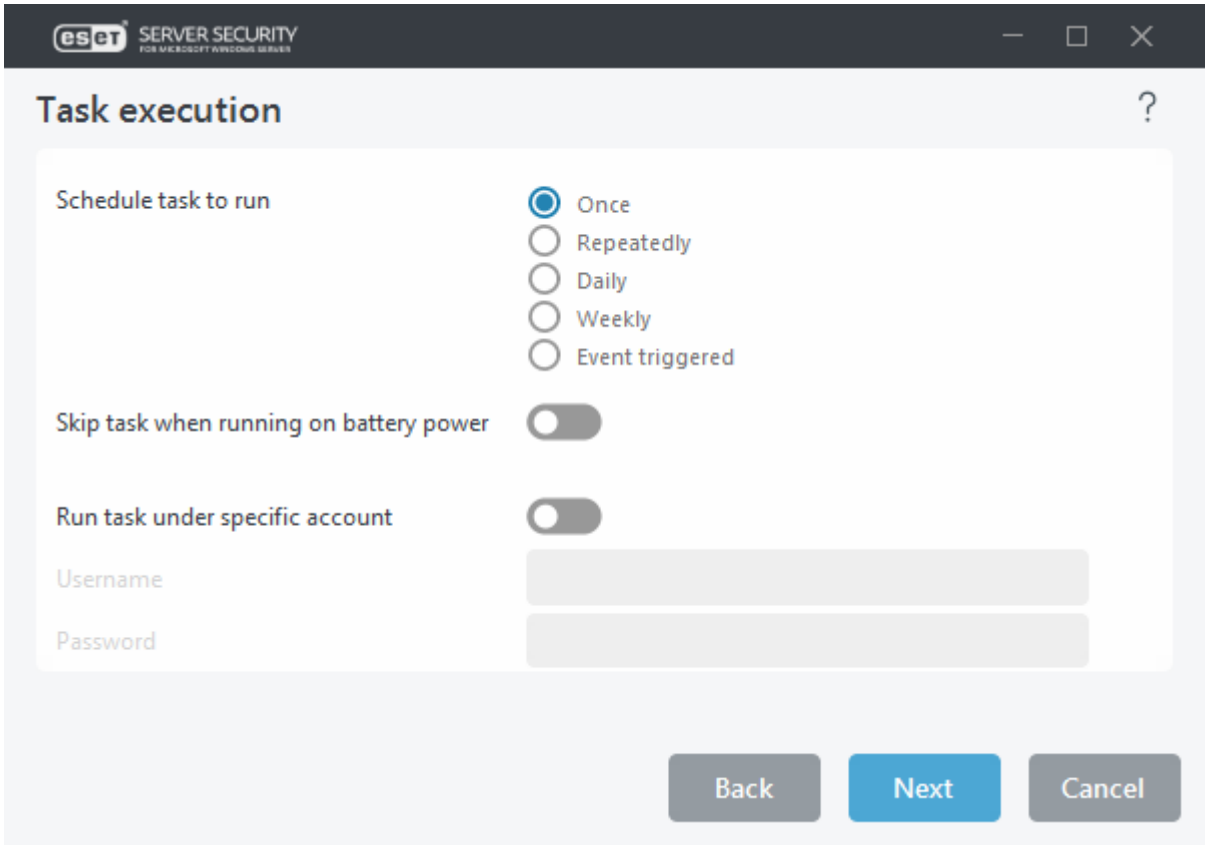
2. Ingrese un **Nombre de la tarea** y configure su tarea programada personalizada.

3. Tipo de tarea: seleccione el **tipo de tarea** correspondiente desde el menú desplegable.

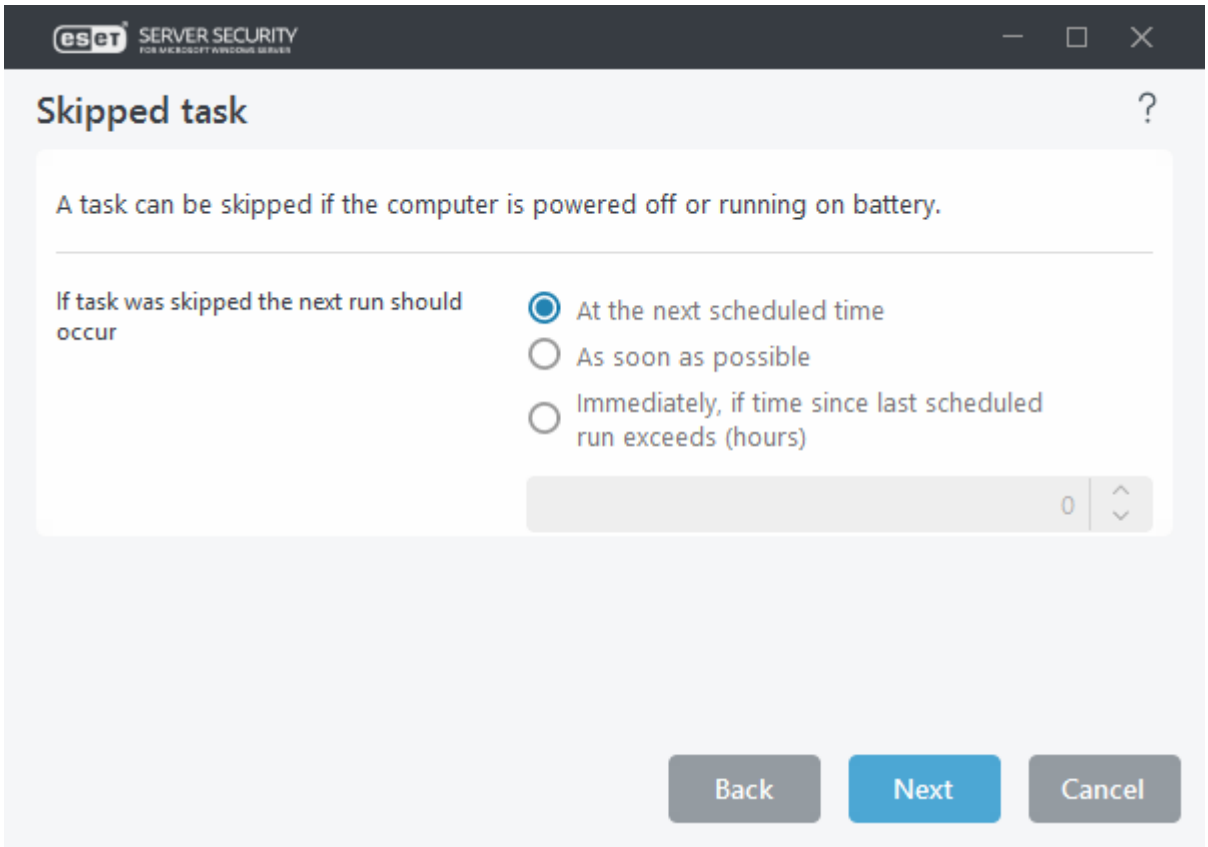


> Para desactivar una tarea, haga clic en la barra junto a **Habilitado**. Para activar la tarea más tarde, use la casilla de verificación en la vista Tareas programadas.

4. Ejecución de la tarea: seleccione una de las opciones para definir cuándo desea que se ejecute la tarea. En función de su elección, se le pedirá que elija una hora, un día, un intervalo o un evento específicos.



5. Pasar por alto tarea: si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se realizará.



6. Ejecutar aplicación: si la tarea está programada para ejecutar una aplicación externa, elija un archivo ejecutable del árbol de directorios.

7. En caso de que necesite realizar cambios, haga clic en **Atrás** para volver a los pasos anteriores y modificar los parámetros.

8. Haga clic en **Terminar** para crear la tarea o aplicar los cambios.

La nueva tarea programada aparecerá en la vista de Tareas programadas.

Tipo de tarea

El asistente de configuración es diferente para cada tipo de tarea de una tarea programada. Ingrese el **Nombre de la tarea** y seleccione el **Tipo de tarea** que desee del menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa. Puede usar una cuenta específica para ejecutar la tarea programada como (opción Ejecutar tarea en cuenta específica).

- **Mantenimiento de registros**: los archivos de registro también contienen remanentes de historiales eliminados. Esta tarea optimiza los historiales de los archivos de registro en forma habitual para que funcionen eficazmente.

- **Verificación de archivos de inicio del sistema**: verifica los archivos que tienen permiso para ejecutarse al iniciar el sistema o tras el registro del usuario.

- **Crear una instantánea de estado del equipo**: crea una instantánea del equipo de ESET SysInspector, que recopila información detallada sobre los componentes del sistema (por ejemplo, controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.

- **Exploración del equipo a petición**: explore archivos y carpetas almacenados localmente o en un recurso compartido de red (almacenamiento compartido, como NAS). Utilice una cuenta específica para ejecutar la tarea programada como (opción Ejecutar tarea en cuenta específica).

- **Actualización**: programa una tarea de actualización mediante la actualización del motor de detección y los módulos del programa.

- **Exploración de base de datos de buzón de correo**: le permite programar una exploración de la base de datos y elegir elementos para ser explorados. Básicamente, es una Exploración de la base de datos a petición.

> i Si tiene la protección de base de datos de la casilla de correo habilitada, puede programar esta tarea pero se mostrará el siguiente mensaje de error en la sección Exploración de la ventana del programa principal. Para evitar esto, asegúrese de que la protección de la base de datos de la casilla de correo esté deshabilitada durante el horario en que la Exploración de la base de datos se programó para su ejecución.

- **Enviar informes de cuarentena de correo**: programa un Informe de cuarentena de correo para enviarse por correo electrónico.

- **Enviar informes de administrador de cuarentena de correo**: programa un Informe de cuarentena de correo para enviarse por correo electrónico.

- **Enviar informe de protección del servidor de correo**: programa un informe de protección del servidor de correo.

- **Exploración del entorno**: le da la oportunidad al servidor Exchange Server de ejecutar una exploración de la base de datos en segundo plano de ser necesario.

- **Exploración de Hyper-V**: programa una exploración de los discos virtuales dentro de Hyper-V.

- **Exploración de Office 365**: programa una exploración para los ambientes de Office 365.

Para desactivar la tarea después de crearla, haga clic en el interruptor junto a **Habilitado**. Para activar la tarea más tarde, haga clic en la casilla de verificación en la vista Tareas programadas. Haga clic en **Siguiente** para continuar al siguiente paso.

Ejecución de la tarea

Seleccione una de las siguientes opciones de programación:

- **Una vez**: la tarea se realizará solo una vez en una fecha y hora específica. Para ejecutar la tarea una sola vez, en un momento dado. Especifique la fecha y hora de inicio para una sola vez en **Ejecución de la tarea**.

- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado(en minutos). Especifique la hora a la que se ejecutará la tarea todos los días en **Ejecución de la tarea**.

- **Diariamente**: la tarea se ejecutará reiteradamente todos los días a la hora especificada.

- **Semanalmente**: la tarea se ejecutará una o varias veces a la semana, en los días y a la hora especificados. Para ejecutar la tarea varias veces sólo en algunos días de la semana, empezando por el día y la hora especificados. Especifique la hora de inicio en la Hora de ejecución de la tarea. Seleccione el día o los días de la semana en los que se debe ejecutar la tarea.

- Cuando se cumpla la condición: la tarea se ejecutará luego de un suceso especificado.

Si habilita **Omitir tarea al ejecutar con batería**, la tarea no se ejecutará si el sistema funciona con baterías en el momento en que la tarea debería iniciarse. Se aplica a equipos que reciben alimentación de un SAI, por ejemplo.

Ejecutar tarea en una cuenta específica: establezca el nombre de usuario y la contraseña de una cuenta específica para ejecutar la tarea programada **Ejecutar la aplicación externa** o **Exploración del equipo a petición**. Utilícelo para ejecutar la **Exploración del equipo a petición** si desea explorar el recurso compartido de red, por ejemplo, NAS u otro almacenamiento compartido.

> i Asegúrese de que la cuenta de usuario que está usando para **Ejecutar la tarea en una cuenta específica** tiene permiso para **Registrar como un trabajo por lotes** (SeBatchLogonRight). Puede comprobar la configuración de políticas mediante la herramienta Administración de políticas de grupo (Configuración de seguridad > Políticas locales > Asignación de derechos de usuario > Iniciar sesión como trabajo por lotes).

Cuando se cumpla la condición

Cuando se programa una tarea accionada por un evento, puede especificar el intervalo mínimo entre dos ejecuciones completas de la tarea.

La tarea se puede accionar por cualquiera de los siguientes sucesos:

- Cada vez que se inicie el equipo
- La primera vez que se inicie el equipo en el día
- conexión por módem a Internet/VPN
- Actualización correcta del módulo
- Actualización correcta del producto
- Inicio de sesión del usuario – La tarea se implementará cuando el usuario inicie sesión en el sistema. Si inicia sesión en el equipo varias veces al día, seleccione 24 horas para realizar la tarea sólo en el primer inicio de sesión del día y, posteriormente, al día siguiente.
- Detección de amenazas

Ejecutar aplicación

Esta tarea programa la ejecución de una aplicación externa.

- **Archivo ejecutable**: elija un archivo ejecutable desde el árbol del directorio, haga clic en navegar ... o ingrese la ruta en forma manual.
- **Carpeta de trabajo**: defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del Archivo ejecutable seleccionado se crearán dentro de este directorio.
- **Parámetros**: parámetros de la línea de comandos de la aplicación (opcional).

Pasar por alto tarea

Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se realizará:

- **A la próxima hora programada**: la tarea se ejecutará a la hora especificada (por ejemplo, luego de 24 horas).
- **Lo antes posible**: la tarea se ejecutará lo antes posible, cuando las acciones que impiden que se ejecute la tarea dejen de ser válidas.
- **Inmediatamente, si el tiempo desde la última ejecución excede un valor específico**: Tiempo desde la última ejecución (horas): luego de seleccionar esta opción, la tarea se repetirá siempre al transcurrir el período especificado (en horas).

Informe de protección del servidor de correo electrónico

El informe de protección del servidor de correo lo mantiene informado con una descripción general de las estadísticas de protección de ESET Mail Security. Los informes estadísticos contienen información sobre el número de correos electrónicos explorados, malware detectado, phishing y spam durante el periodo

especificado. El informe se genera en función de la tarea programada y se envía por correo electrónico a los destinatarios seleccionados como un archivo adjunto en formato HTML. La salida HTML presenta los datos en forma de gráfico, muestra el promedio a largo plazo para la comparación e incluye información de tráfico para cada tipo de protección, los principales destinatarios de malware, phishing y spam.

Use las tareas programadas para que los informes de protección del servidor de correo se generen en una fecha y una hora especificadas, también como evento recurrente. Los informes programados se entregan a los destinatarios de correo electrónico seleccionados que recibirán los informes.

Vaya a **Herramientas** > **Tareas programadas** > y haga clic en **Agregar tarea** al asistente.

Escriba el **nombre de la tarea**, seleccione el **Tipo de tarea** en el menú desplegable y elija el tipo de **tarea de informe de protección del servidor de correo**.

- **Nombre del informe**: escriba el nombre del informe.
- **Intervalo de tiempo**: seleccione una de las opciones como periodo para el que se generará el informe.
- **Destinatarios**: especifique los usuarios que recibirán el informe de protección del servidor de correo. Haga clic en **Editar** para ingresar a los buzones de correo para destinatarios específicos (los buzones de correo vinculados también son compatibles). Especifique la dirección de correo electrónico del destinatario del informe y presione Intro para confirmar. Repita para agregar varios destinatarios.
- **Dirección del remitente**: especifique una dirección de correo electrónico que se mostrará como remitente del informe de protección del servidor de correo (por ejemplo, administrator@mydomain.com).
- **Informar idioma**: elija el idioma que desee en el menú desplegable. El informe se generará en el idioma seleccionado.
- **Agregar estadísticas del clúster**: cree un informe con los datos estadísticos generados para todos los miembros del nodo del clúster.

Haga clic en **Terminar**.

Resumen general de tareas programadas

Esta ventana de diálogo muestra información detallada sobre una tarea programada cuando hace doble clic en la tarea en la vista **Programador de tareas** o cuando hace clic con el botón secundario en la tarea programada y elige **Mostrar detalles de la tarea**.

Enviar muestras para su análisis

El cuadro de diálogo para el envío de muestras le permite enviar un archivo o un sitio a ESET para su análisis. Si encuentra un archivo de conducta sospechosa en su equipo o un sitio sospechoso en Internet, envíelo al laboratorio de virus de ESET para su análisis. Si el archivo resulta ser una aplicación o un sitio maliciosos, se agregará su detección a una de las próximas actualizaciones.

Para enviar el archivo por correo electrónico, comprima los archivos con WinRAR o WinZIP, protéjalos con la contraseña `infected` y envíelos a samples@eset.com. Use un tema descriptivo e incluya la mayor cantidad de información posible sobre el archivo (por ejemplo, el sitio web desde donde realizó la descarga).

Antes de enviar una muestra a ESET, verifique que cumpla con uno o ambos de los siguientes criterios:
• el programa directamente no detecta el archivo o el sitio web
• el programa detecta erróneamente el archivo o el sitio web como una amenaza
• No aceptamos archivos personales (que le gustaría que ESET explorara en busca de malware) como muestras (ESET Research Lab no realiza exploraciones bajo demanda para los usuarios)
• Use un tema descriptivo e incluya la mayor cantidad de información posible sobre el archivo (por ejemplo, el sitio web desde donde realizó la descarga).

Si no se cumple al menos uno de los requisitos anteriores, no recibirá respuesta hasta que no se aporte más información.

Seleccione la descripción que mejor se adapte a su mensaje del menú desplegable **Motivo por el cual se envía la muestra**:

- Archivo sospechoso
- Sitio sospechoso (un sitio web que se encuentra infectado por un malware)
- Archivo falso positivo (un archivo que se detecta como infectado, pero que no lo está)
- Sitio falso positivo
- Otros

Archivo/sitio

La ruta al archivo o sitio web que desea enviar.

Correo electrónico de contacto

Este correo electrónico de contacto se envía junto con los archivos sospechosos a ESET y puede usarse para contactarlo en caso de que se requiera información adicional para el análisis. El ingreso del correo electrónico de contacto es opcional. No obtendrá una respuesta de ESET, a menos que se requiera más información. Esto se debe a que nuestros servidores reciben decenas de miles de archivos por día, lo que hace imposible responder a todos los envíos.

Enviar de manera anónima

Utilice la casilla de verificación situada junto a **Enviar de manera anónima** para enviar archivos o sitios web sospechosos sin escribir su dirección de correo electrónico.

Archivo sospechoso

Signos y síntomas observados de infección de malware

Ingrese una descripción sobre la conducta de los archivos sospechosos observada en el equipo.

Origen del archivo (dirección URL o proveedor)

Ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Notas e información adicional

Aquí puede ingresar información adicional o una descripción útil la identificación del archivo sospechoso.

> aunque solo el primer parámetro es obligatorio (**Signos y síntomas observados de infección de malware**), el suministro de información adicional ayudará en forma significativa a nuestros laboratorios en el proceso de identificación de las muestras.

Sitio sospechoso

Seleccione una de las siguientes opciones del menú desplegable Problemas del sitio:

Infectados

Un sitio web que contiene virus u otro malware, distribuidos por varios métodos.

Phishing

Suele usarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal, etc. Lea más información sobre este tipo de ataque en el glosario.

Fraude

Un sitio web fraudulento o engañoso.

Otros

Puede utilizar esta opción si ninguna de las opciones anteriores es válida para el sitio que va a enviar.

Notas e información adicional

Puede ingresar información adicional o una descripción que pueda ayudar al análisis del sitio web sospechoso.

Archivo falso positivo

Le solicitamos que envíe los archivos detectados como una infección pero que no se encuentran infectados para mejorar nuestro motor de detección y ayudar a otros a estar protegidos. Los falsos positivos (FP) pueden generarse cuando el patrón de un archivo coincide con el mismo patrón incluido en el motor de detección.

> Primeros tres parámetros se requieren para identificar aplicaciones legítimas y distinguirlas del código malicioso. Al proporcionar información adicional, ayudará significativamente a nuestros laboratorios en el proceso de identificación y en el procesamiento de las muestras.

Nombre y versión de la aplicación

El título del programa y su versión (por ejemplo, número, alias o nombre del código).

Origen del archivo (dirección URL o proveedor)

Ingrese el origen del archivo (la procedencia) e indique cómo lo encontró.

Propósito de la aplicación

La descripción general de la aplicación, el tipo de aplicación (por ejemplo, navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional

Aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

Sitio falso positivo

Le recomendamos que envíe los sitios que se detectan como infectados, fraudulentos o phishing pero que no lo son. Los falsos positivos (FP) pueden generarse cuando el patrón de un sitio coincide con el mismo patrón incluido en el motor de detección. Envíenos esta página web para mejorar nuestro motor de detección y ayudar a proteger a los demás.

Notas e información adicional

Aquí puede agregar información adicional o descripciones útiles para el procesamiento del archivo sospechoso.

Otros

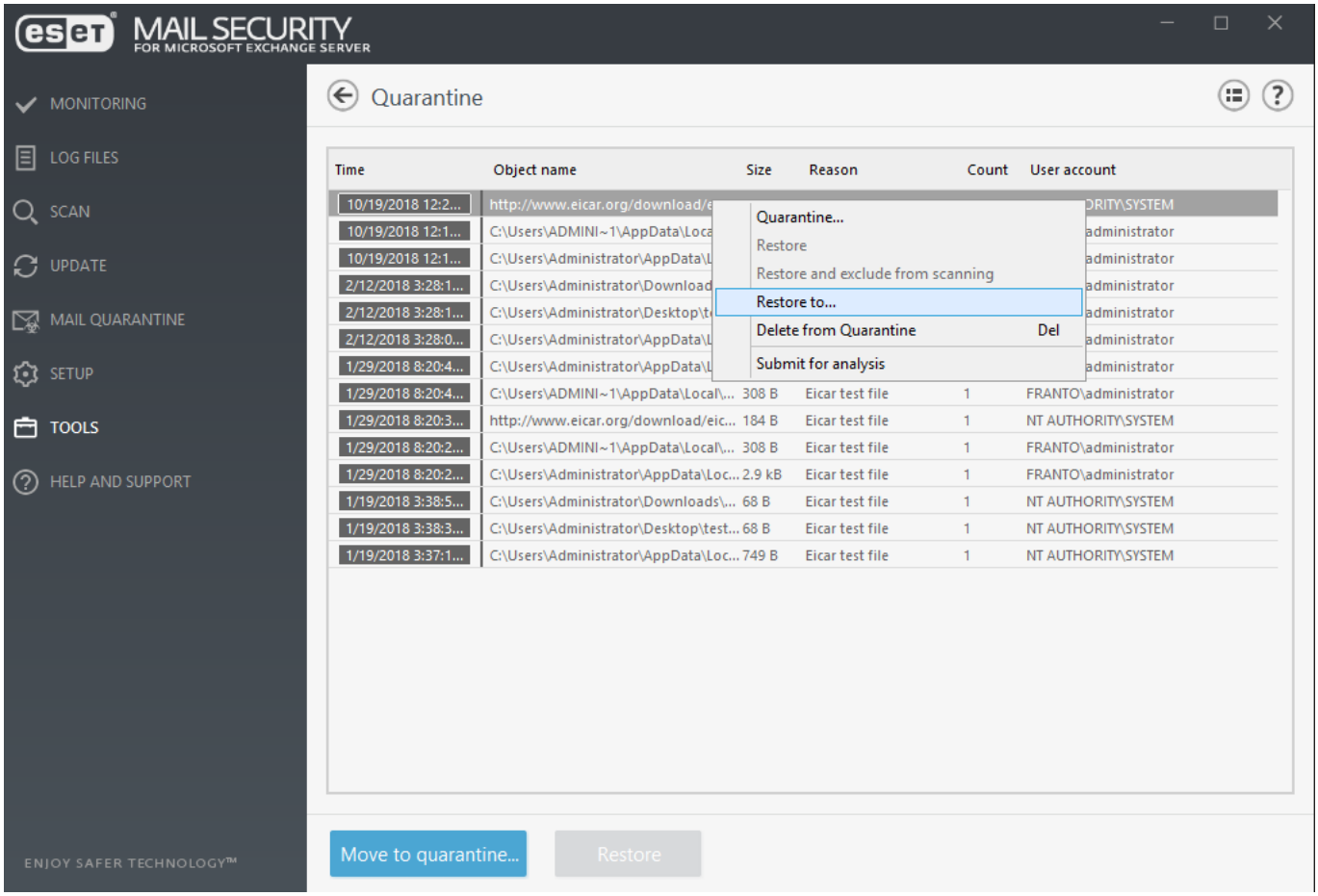
Use este formulario si el archivo no se puede categorizar como Archivo sospechoso o Falso positivo.

Motivo por el cual se envía el archivo

Ingrese una descripción detallada y el motivo por el cual envía el archivo.

Cuarentena

La función principal de la cuarentena consiste en almacenar los archivos infectados en forma segura. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o en caso de que ESET Mail Security los esté detectado erróneamente. Puede elegir poner cualquier archivo en cuarentena. Esta acción es recomendable cuando un archivo se comporta de manera sospechosa pero el explorador de malware no lo detecta. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena pueden visualizarse en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta a la ubicación original de los archivos infectados, su tamaño en bytes, el motivo (por ejemplo, objeto agregado por el usuario) y la cantidad de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias infiltraciones).

En caso de que los objetos del mensaje de correo electrónico estén en cuarentena en la cuarentena de archivos, se muestra la ruta al correo/carpeta/nombre de archivo.

Envío de archivos a cuarentena

ESET Mail Security pone automáticamente en cuarentena los archivos eliminados (si no ha deshabilitado esta opción en la ventana de alerta). Para enviar a cuarentena cualquier archivo sospechoso, haga clic en el botón **Cuarentena**. Los archivos en cuarentena se eliminarán de su ubicación original. También se puede usar el menú contextual con este propósito. Para ello, haga clic con el botón secundario en la ventana **Cuarentena** y seleccione **Cuarentena**.

Restauración desde cuarentena

Los archivos puestos en cuarentena también pueden restaurarse a su ubicación original. Para ello, use la función **Restaurar**, disponible desde el menú contextual tras hacer un clic con el botón secundario en el archivo determinado en la ventana Cuarentena. Si un archivo está marcado como una aplicación potencialmente no deseada , la opción **Restablecer y excluir de la exploración** estará disponible. Asimismo, el menú contextual ofrece la opción **Restaurar a...**, que permite restaurar un archivo en una ubicación diferente a la que tenía cuando fue eliminado.

> Si el programa puso en cuarentena un archivo no infectado por error, exclúyalo de la exploración después de restaurarlo y envíelo a Atención al cliente de ESET.

Envío de un archivo desde cuarentena

Si puso en cuarentena un archivo sospechoso que el programa no detectó o si un archivo se determinó erróneamente como infectado (por ejemplo, tras la exploración heurística del código) y luego se puso en cuarentena, envíe el archivo al laboratorio de amenazas de ESET. Para enviar un archivo desde la cuarentena, haga clic en el archivo con el botón secundario y seleccione Enviar para su análisis en el menú contextual.

Eliminar de la Cuarentena

Haga clic con el botón secundario en un elemento determinado y seleccione **Eliminar de la Cuarentena**. O seleccione el elemento que desea eliminar y presione **Eliminar** en su teclado.

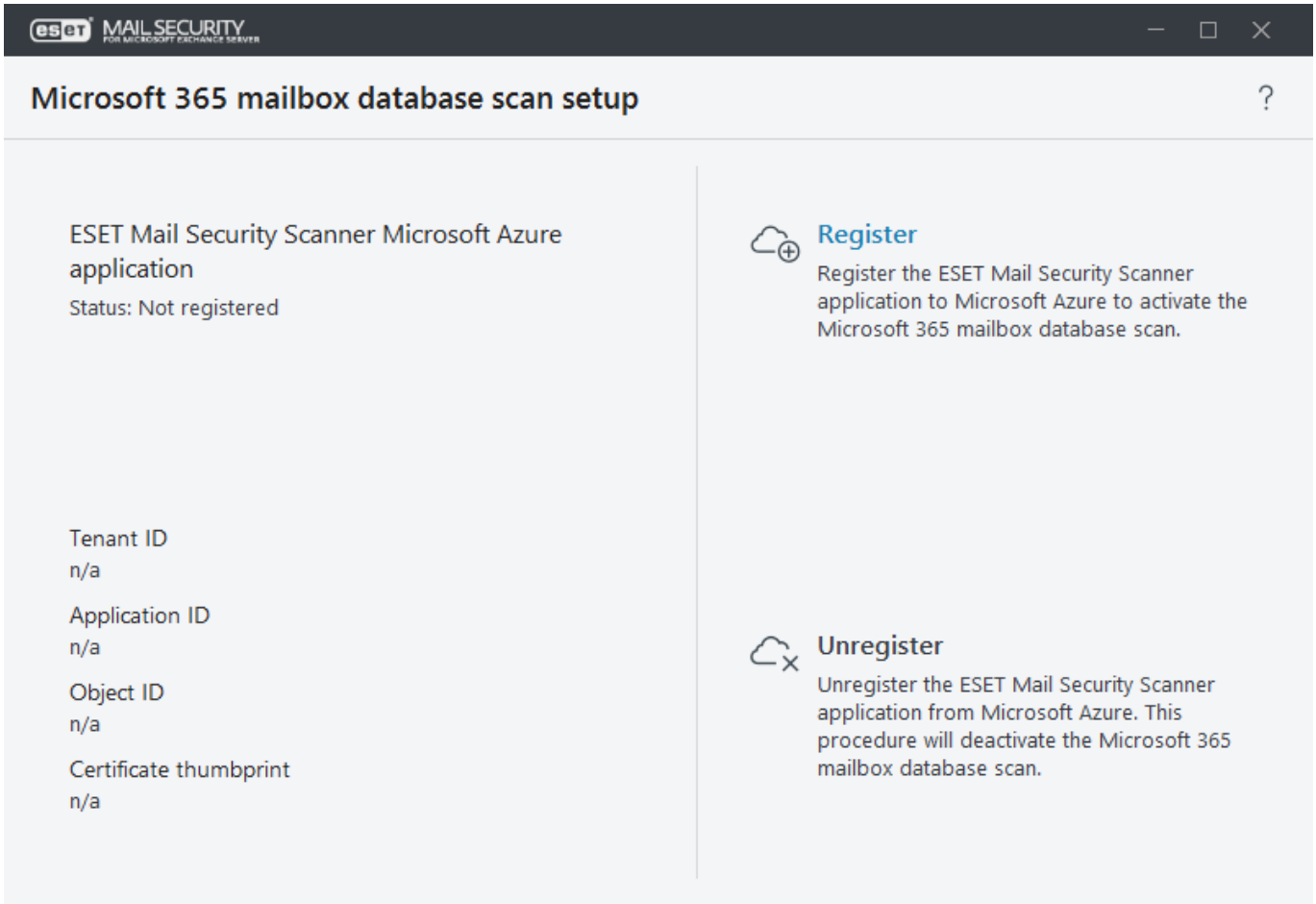
Asistente de exploración del buzón de Microsoft 365

ESET Mail Security admite la exploración de carpetas públicas y buzones remotos de Microsoft 365, como la exploración de base de datos tradicional de buzones a petición. Para activar esta característica, registre su explorador ESET Mail Security.

Vínculos rápidos:

- Registre su explorador ESET Mail Security
- Eliminar el registro del explorador ESET Mail Security

Para empezar a usar la exploración de base de datos del buzón de ESET Mail Security Microsoft 365, Registre la aplicación del explorador ESET Mail Security en Microsoft Azure. La página de configuración de la exploración del buzón de Microsoft 365 muestra su estado de registro, si ya está registrado, verá los detalles de registro (ID del inquilino, ID de la aplicación, ID del objeto y huella digital del certificado). Puede registrar o eliminar el registro de su explorador ESET Mail Security:



Tras registrar correctamente el explorador, la exploración de base de datos del buzón de Microsoft 365 estará disponible en el menú Exploración y mostrará una lista de buzones (y carpetas públicas) que pueden seleccionarse para explorar.

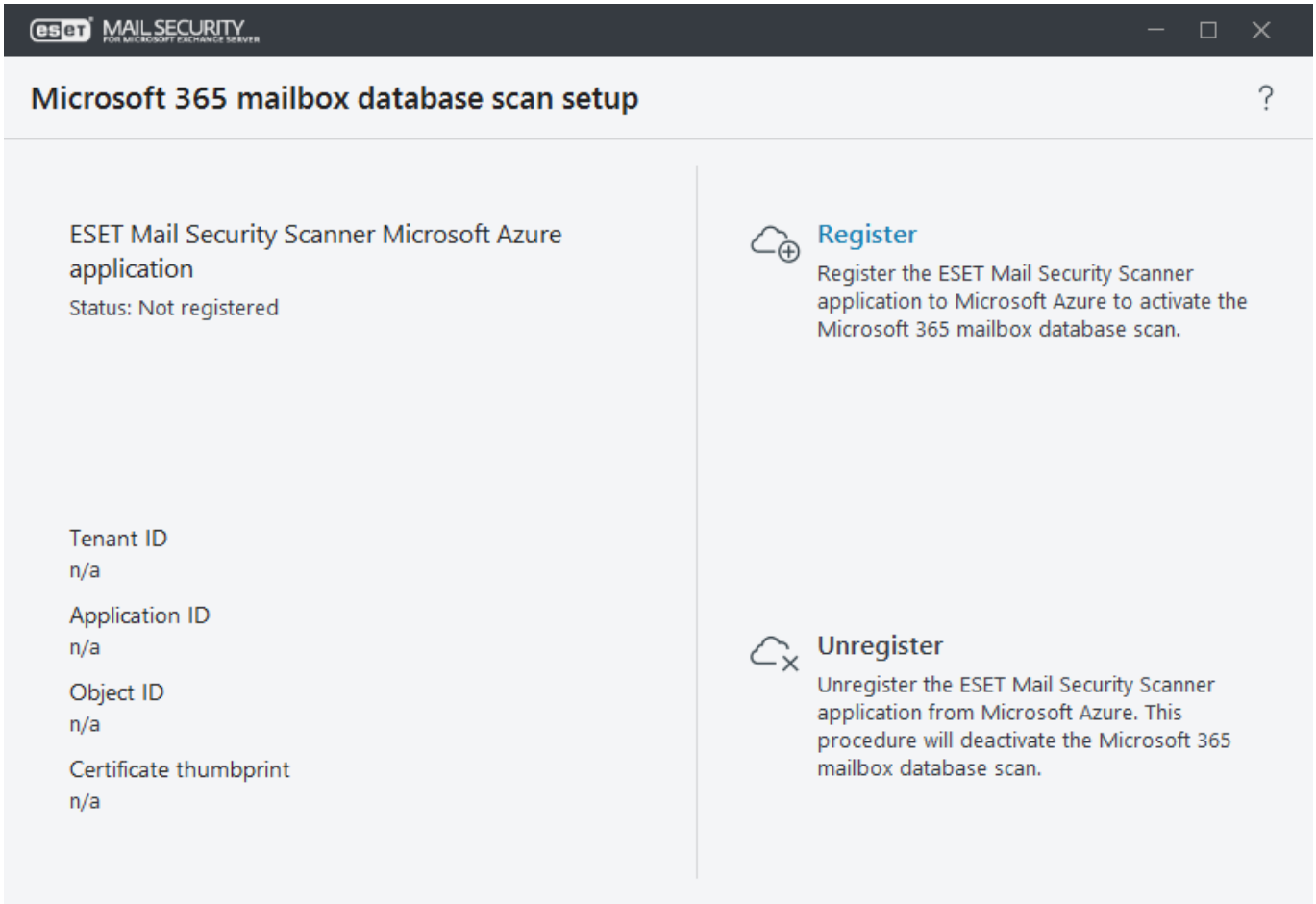
> Vuelva a registrarse con una cuenta diferente: Si quiere registrar un explorador ESET Mail Security con una nueva cuenta de Microsoft 365, debe eliminar el registro del explorador ESET Mail Security que está utilizando con su cuenta anterior y registrarse con la nueva cuenta de administrador de Microsoft 365.

Puede encontrar su explorador ESET Mail Security registrado como una aplicación en Microsoft Azure. Haga clic en **Azure Active Directory** > **Registros de aplicaciones**, en **Ver todas las aplicaciones**, encontrará la aplicación del explorador ESET Mail Security en la lista. Haga clic en la aplicación para ver sus detalles.

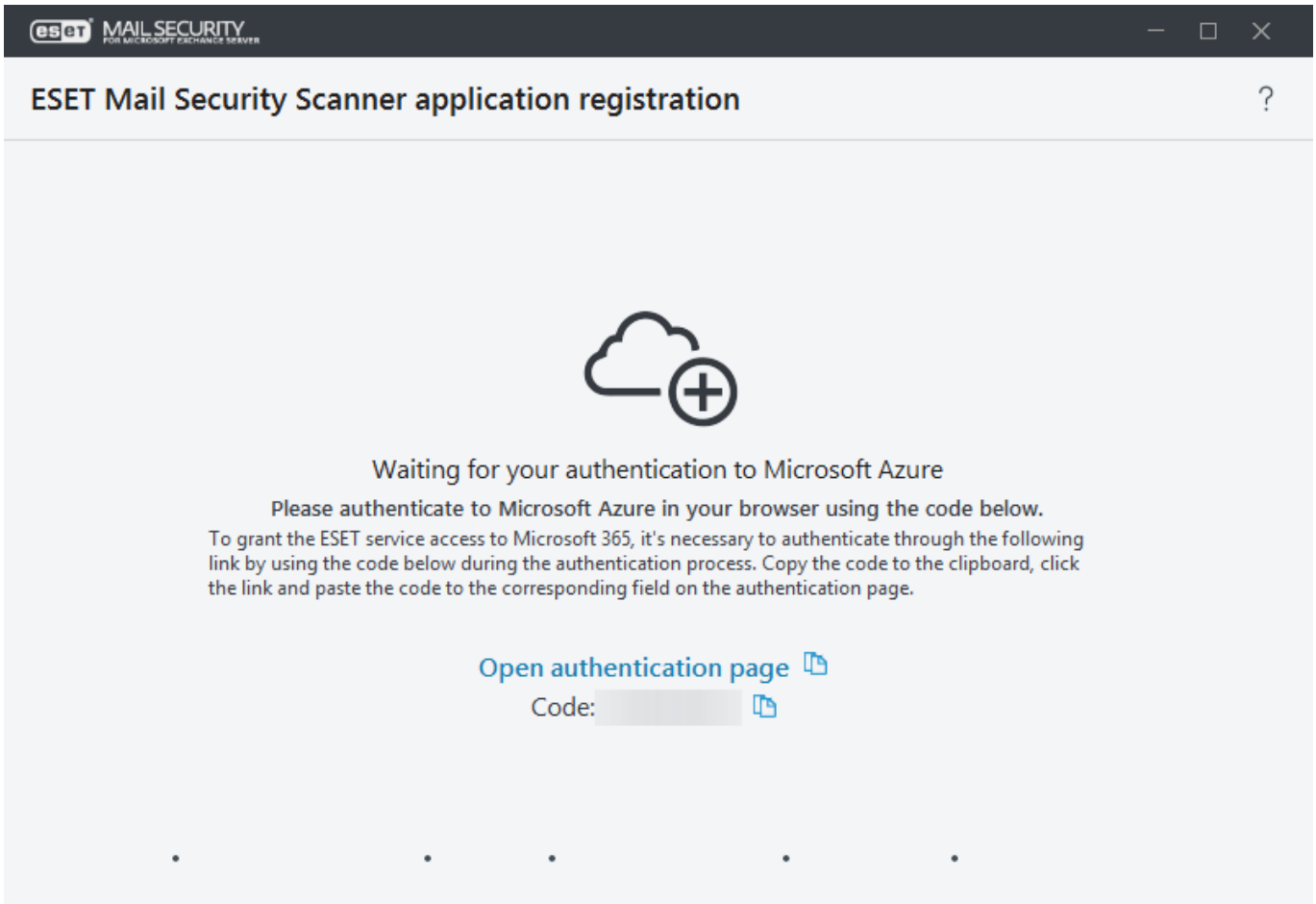
Registrar explorador ESET Mail Security

Siga los siguientes pasos para registrar la aplicación del explorador ESET Mail Security en Microsoft Azure y activar la exploración de base de datos de buzones de correo Microsoft 365:

1. Haga clic en **Registrar** para iniciar el registro del explorador ESET Mail Security y se abrirá un asistente de registro.

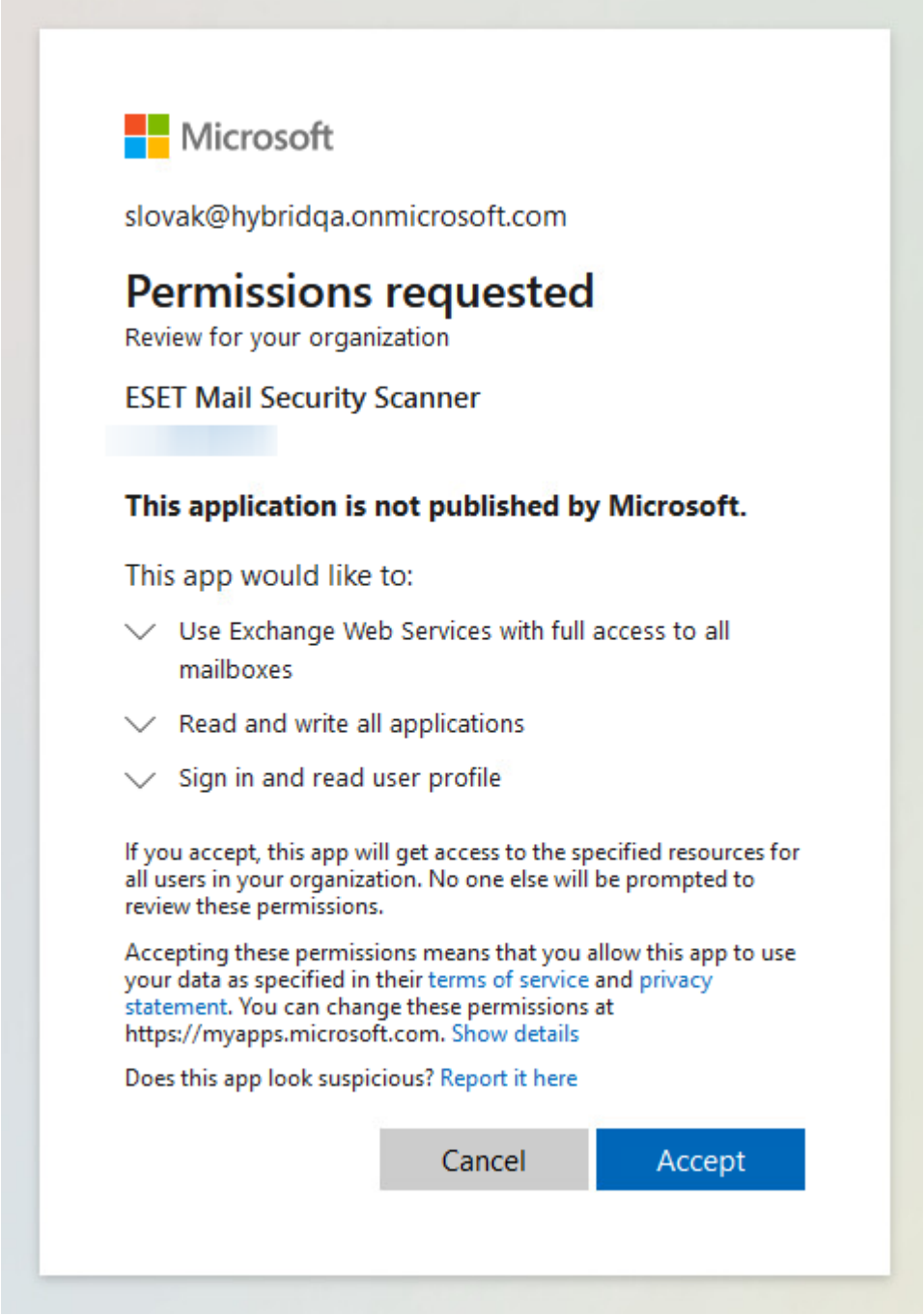


2. Copie el código proporcionado, haga clic en la **página Abrir autenticación** e introduzca el código.

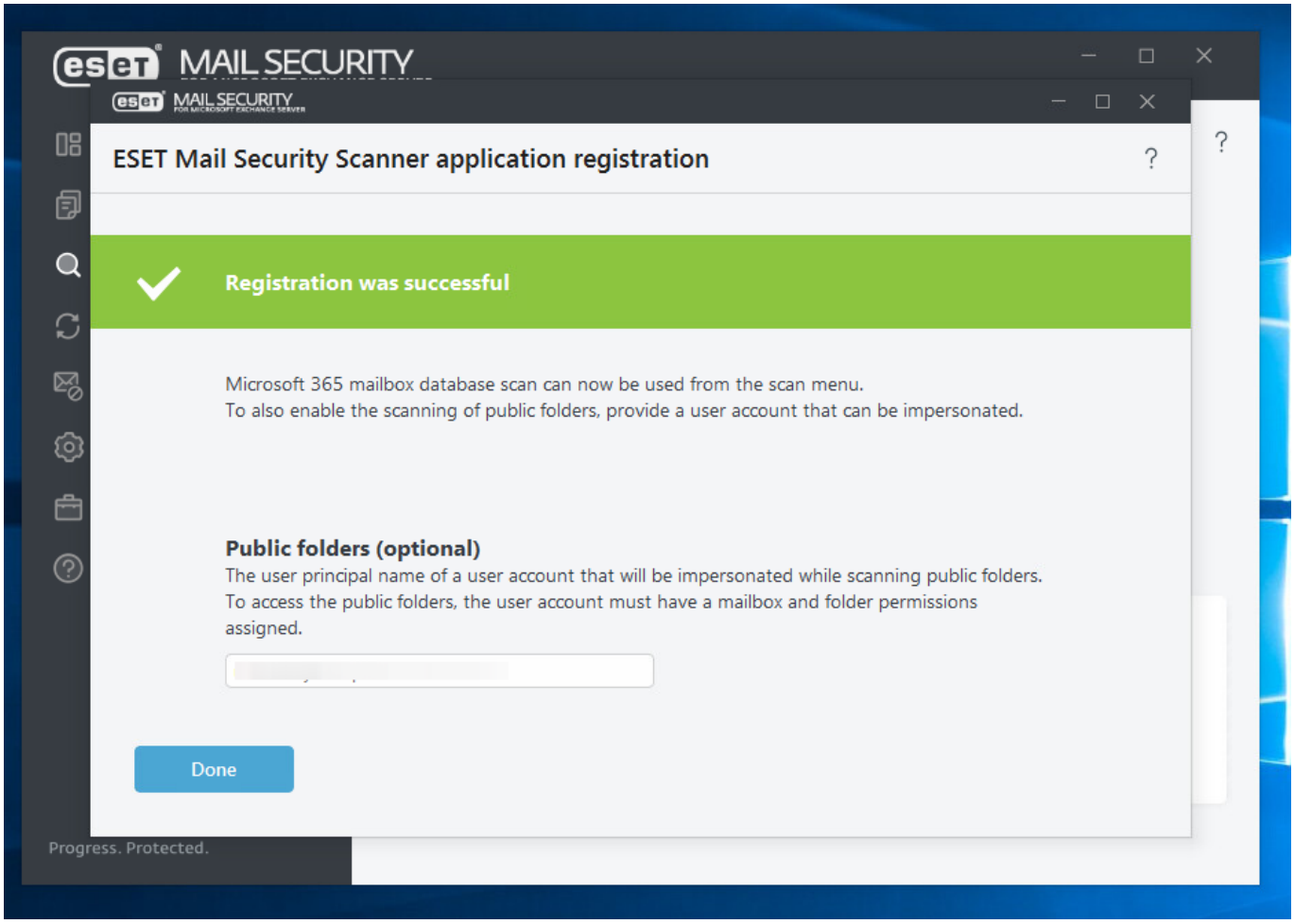


3. Se abrirá un navegador web con la página de **Seleccione una cuenta** de Microsoft. Haga clic en la cuenta que está utilizando, si está disponible, o ingrese sus credenciales de cuenta de administrador de Microsoft 365 y haga clic en **Iniciar sesión**.

4. La aplicación del explorador ESET Mail Security requiere tres tipos de permisos que se listan en el mensaje de aceptación. Haga clic en **Aceptar** para permitir que el explorador ESET Mail Security acceda a sus datos de Microsoft 365.



5. Cierre el navegador web y espere a que se complete el registro de ESET Mail Security Scanner. Verá que el mensaje **El registro se realizó correctamente**.



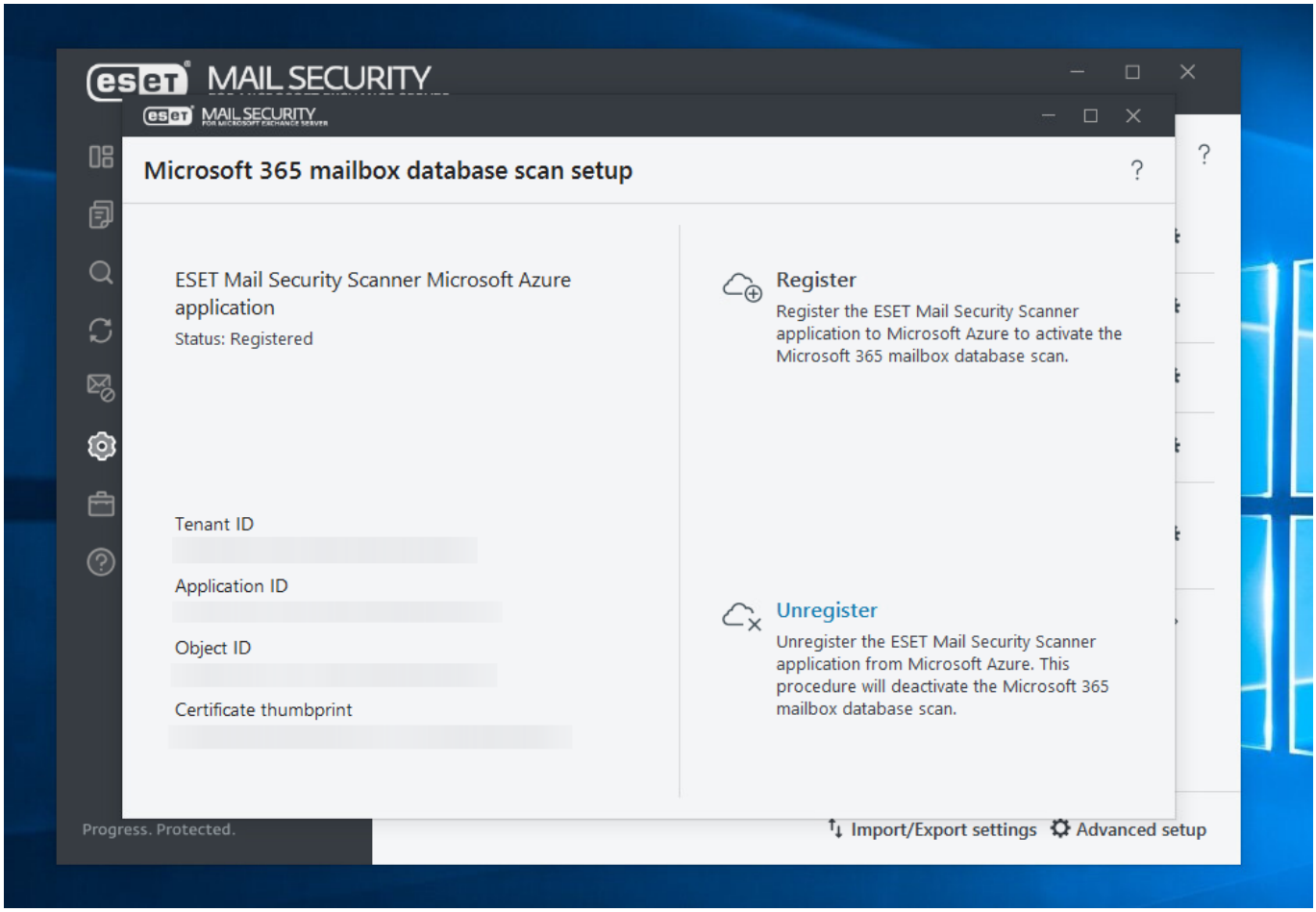
6. **Carpetas públicas (opcional)**

Si desea explorar carpetas públicas, proporcione el nombre de la cuenta de usuario principal (no se necesita contraseña) para la suplantación. Asegúrese de que esta cuenta de usuario esté configurada para tener acceso a todas las carpetas públicas. Haga clic en **Listo**.

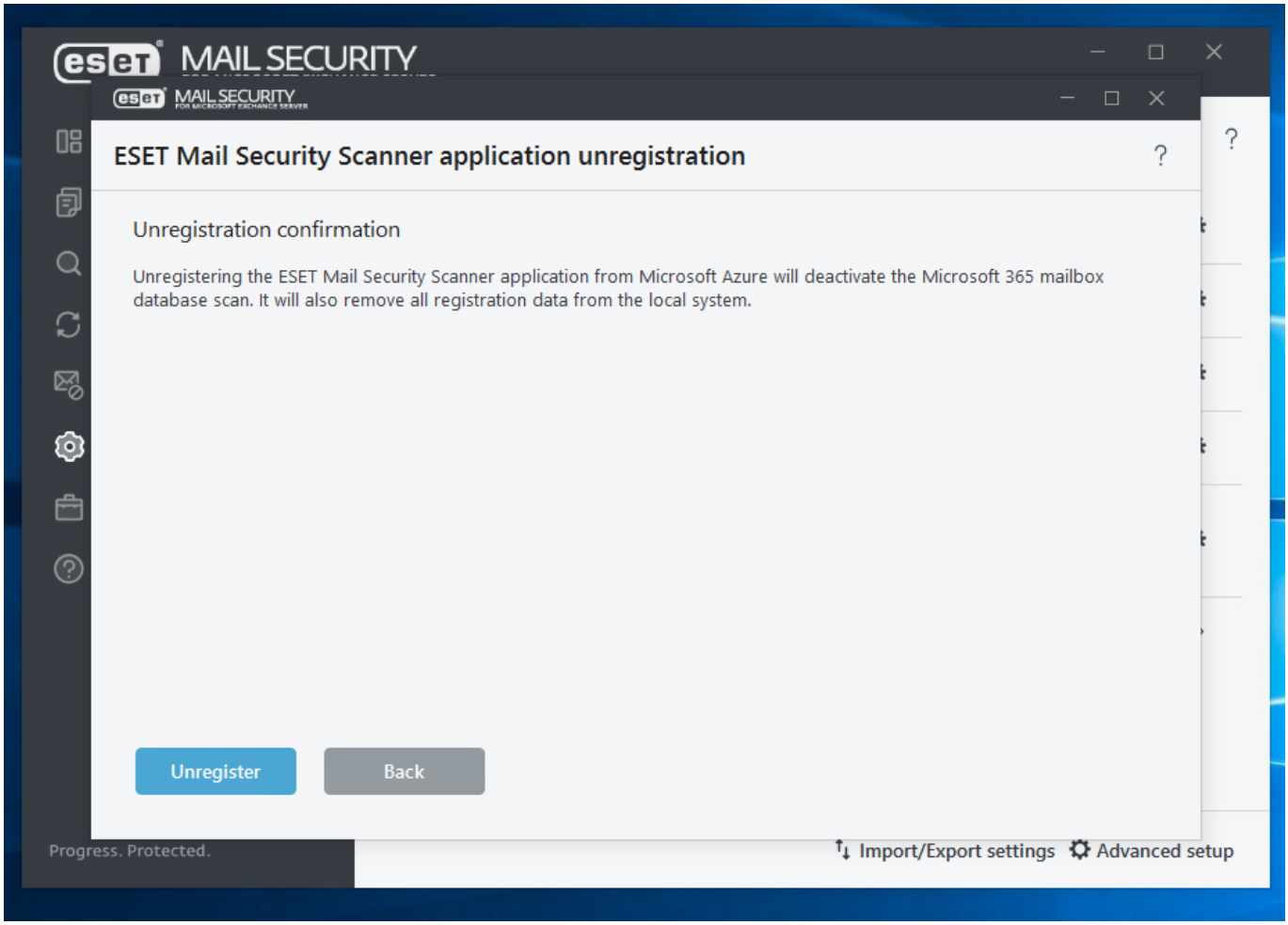
Eliminar el registro del explorador ESET Mail Security

El proceso de eliminación del registro le permite quitar el certificado y la aplicación del explorador ESET Mail Security de Microsoft Azure. Este proceso también elimina las dependencias locales y vuelve a habilitar la opción Registrar.

1. Haga clic en **Configuración** > **Servidor** > **Exploración del buzón de Microsoft 365** y, luego, haga clic en **Eliminar registro** para comenzar con el proceso de eliminación del explorador ESET Mail Security. Se abrirá un asistente de eliminación del registro.



2. Haga clic en **Eliminar registro** para confirmar que desea quitar el explorador ESET Mail Security. Espere a que se complete el la eliminación del registro de Microsoft Azul.



3. Si el registro se elimina correctamente, el asistente de eliminación del registro mostrará el mensaje **Se eliminó el registro correctamente**.

Configuración de protección para servidores

La configuración de protección del servidor es la principal opción de integración. Haga clic en el botón de alternancia para habilitar o deshabilitar la integración de la Protección de la base de datos del buzón de correo electrónico, la Protección del transporte de correo electrónico o el inicio de sesión DKIM en Exchange Server. Cuando esta opción está activada, puede configurar la configuración detallada para cada tipo de protección en su sección correspondiente. También puede modificar la prioridad del agente (asegúrese de mantener la posición de prioridad del agente ESET DKIM en el último lugar).

> Si ejecuta Microsoft Exchange Server 2010 puede elegir entre la Protección de la base de datos de correo electrónico y la Exploración de la base de datos del buzón de correo a petición, solo se puede activar un tipo de protección a la vez. Si decide usar la Exploración de base de datos del buzón de correo a petición, deberá deshabilitar la Protección de la base de datos del buzón de correo electrónico. De lo contrario, la Exploración de la base de datos del buzón de correo a petición no estará disponible.

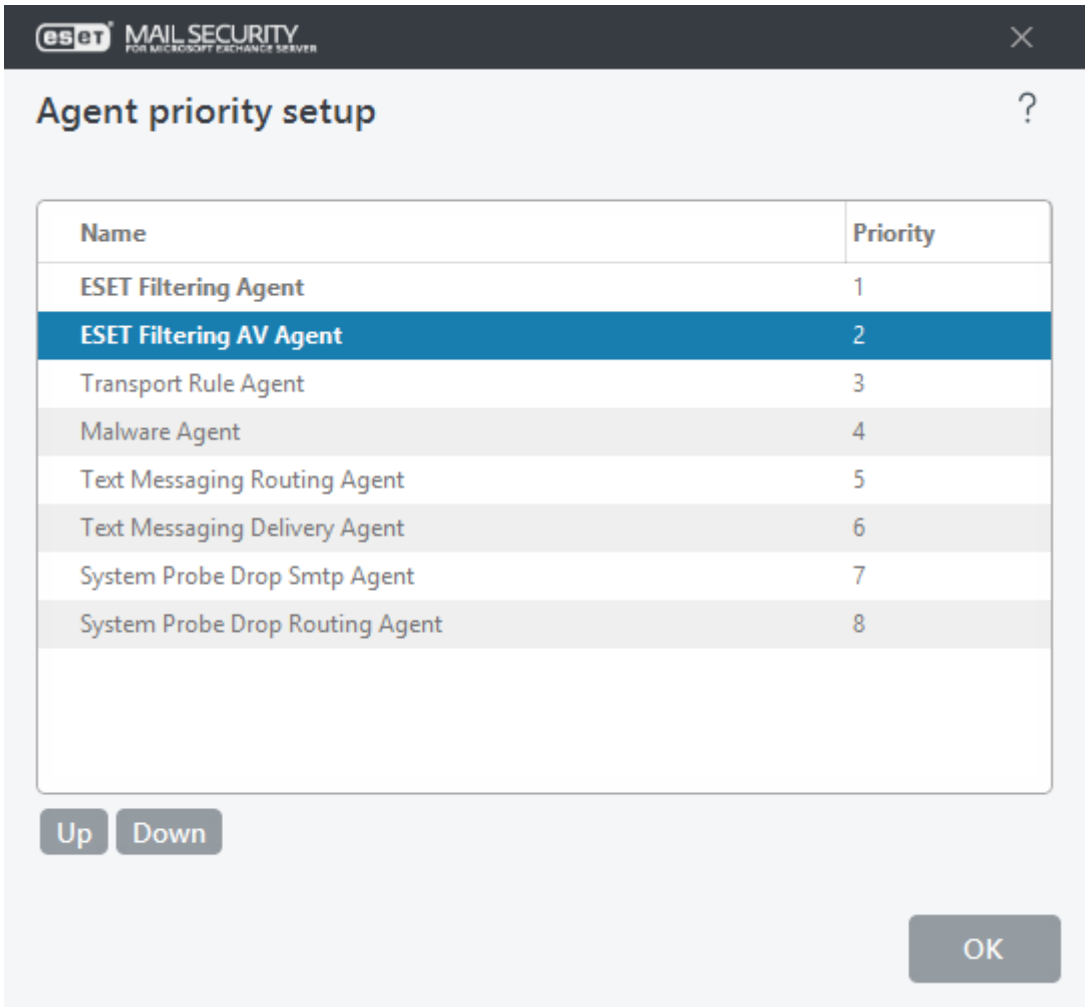
ESET Mail Security ofrece una protección significativa para Microsoft Exchange Server mediante las siguientes características:

- Antivirus y antispyware
- Protección antispam

- Protección antiphishing
- Reglas
- Protección en el transporte de correos (Exchange Server 2010, 2013, 2016, 2019)
- Protección de la base de datos del buzón de correo electrónico (Exchange Server 2010)
- Exploración de la base de datos del buzón de correo a petición (Exchange Server 2010, 2013, 2016, 2019)
- Cuarentena de correo electrónico (configuraciones del tipo de cuarentena de correo electrónico)
- Firma DKIM

Configuración de la prioridad del agente

Si es necesario, puede especificar el orden en el cual los ESET Mail Security Agentes se activan después del inicio de Microsoft Exchange Server. El valor numérico define la prioridad. Los números más bajos denotan una prioridad más alta. Se aplica a Microsoft Exchange Server 2010 y superior.



Arriba/Abajo

Incremente o reduzca la prioridad del agente seleccionado moviéndolo hacia arriba o hacia abajo en la lista de agentes. Puede cambiar la prioridad de los agentes relevantes (resaltados en negrita).

Le recomendamos que mantenga la prioridad del agente ESET DKIM en el último lugar, en la parte inferior, para asegurarse de que los encabezados estén firmados por última vez después cualquier modificación en los encabezados realizada por agentes anteriores.

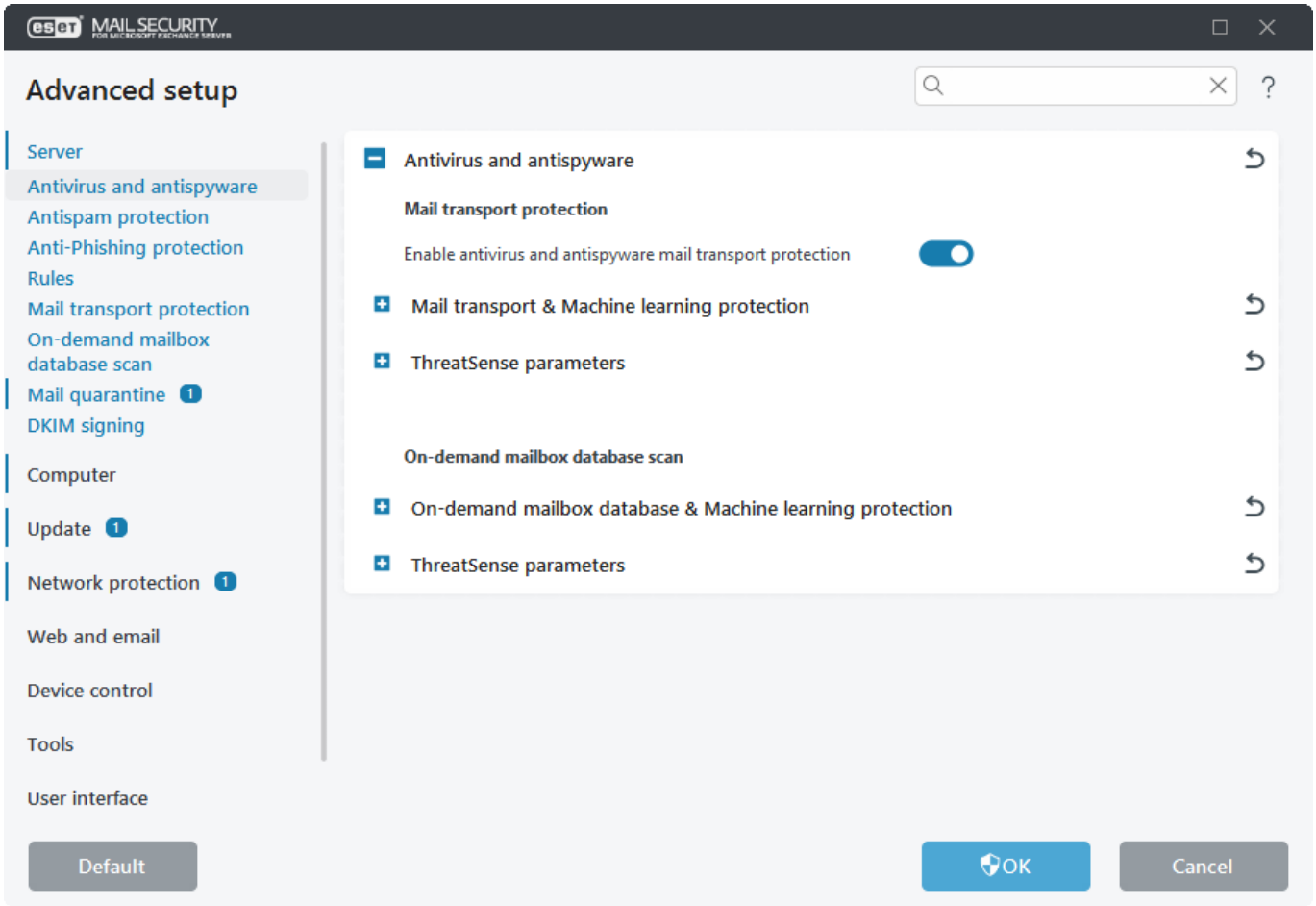
Antivirus y antispyware

En esta sección, puede configurar las opciones de antivirus y antispyware para su servidor de correo.

El agente de transporte proporciona la Protección del transporte de correo electrónico. Solo está disponible para Microsoft Exchange Server 2010 y posterior, pero su Microsoft Exchange Server debe tener el rol de servidor Transporte Edge o el rol de servidor Transporte Hub. Esto también se aplica a una instalación de servidor único con roles múltiples de Exchange Server en un equipo (siempre y cuando incluya uno de los roles de servidor Transporte Edge o Hub).

Protección del transporte de correo electrónico

Si deshabilita la opción **Habilitar la protección del transporte de correo para antivirus y antispyware**, el complemento de ESET Mail Security para Exchange Server no se sacará del proceso del servidor Microsoft Exchange. Solo pasará los mensajes sin explorarlos en busca de virus en la capa de transporte. Los mensajes se explorarán en busca de virus y spam en la capa de la base de datos del buzón de correo electrónico y se aplicarán las reglas existentes.



Protección de la base de datos de correo electrónico

Si deshabilita la opción **Habilitar la protección de la base de datos de correo electrónico para antivirus y**

antispyware, el complemento de ESET Mail Security para Exchange Server no se sacará del proceso del servidor Microsoft Exchange. Solo pasará los mensajes sin explorarlos en busca de virus en la capa de base de datos. Los mensajes se explorarán en busca de virus y spam en la capa de transporte y se aplicarán las reglas existentes.

Exploración de la base de datos del buzón de correo a petición

La Exploración de base de datos del buzón de correo a petición está disponible después de deshabilitar la **Protección de la base de datos del buzón de correo electrónico** en la sección Servidor.

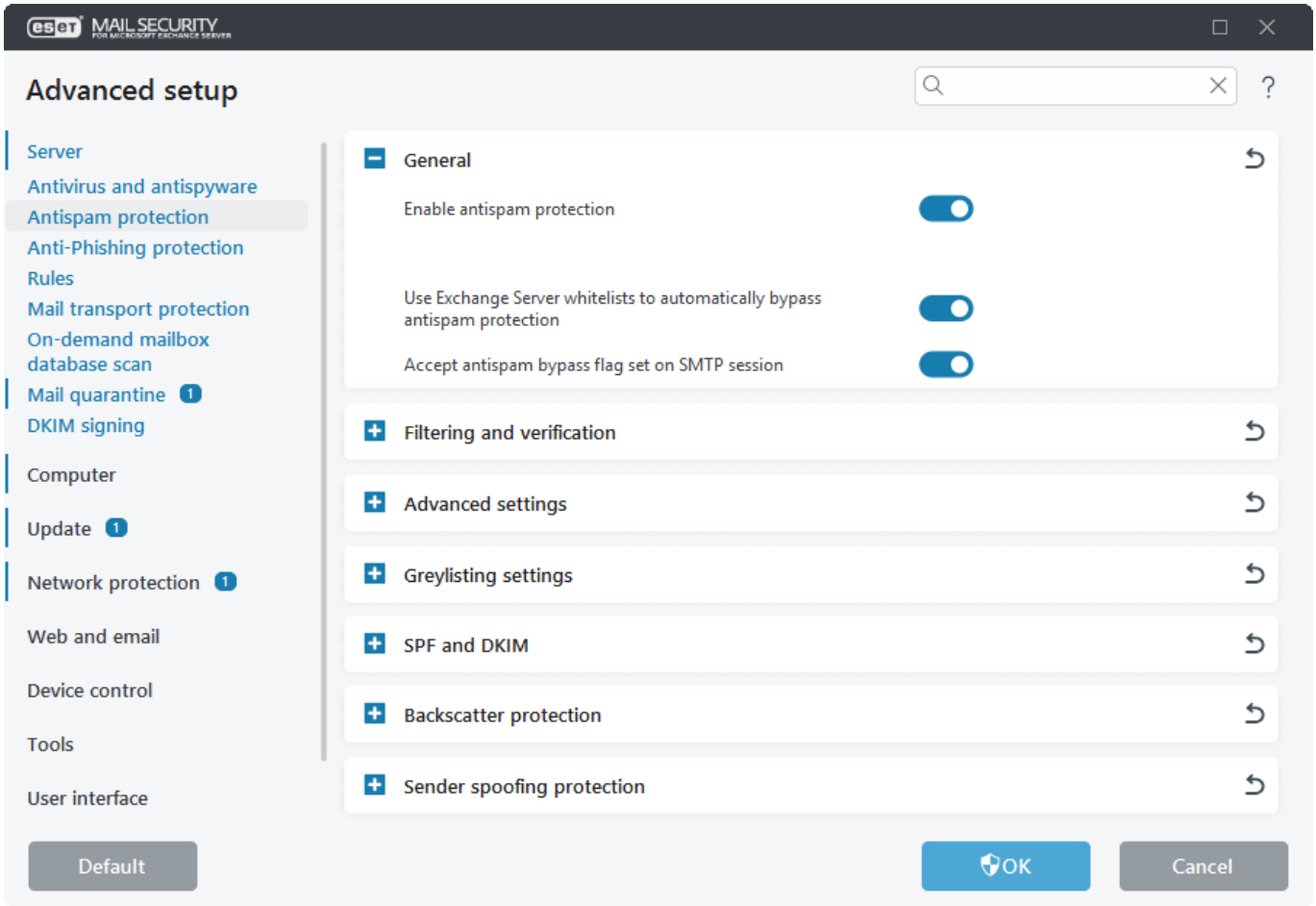
ThreatSense parámetros

Modifique los parámetros de exploración para la protección de transporte de correo, protección de la base de datos de correo electrónico y Exploración de la base de datos de buzón de correo a petición.

Protección antispam

La protección antispam de su servidor de correo está habilitada de forma predeterminada. Para deshabilitarla, haga clic en el interruptor junto a **Habilitar protección antispam**.

> Deshabilitar la protección antispam no cambiará el estado de protección. Aunque el antispam esté deshabilitado, verá **Está protegido** en verde que aún se muestra en la sección de **Supervisión** de la ventana principal del programa. Deshabilitar el Antispam no se considera una reducción en el nivel de protección.



Usar las listas blancas de Exchange Server para evadir automáticamente la protección antispam

Permite ESET Mail Security usar las “listas blancas” específicas de Exchange. Si esta opción está habilitada, se

tendrá en cuenta lo siguiente:

- La dirección IP del servidor está en la lista de IP permitidas del Exchange Server
- El indicador Omitir antispam está configurado en el buzón de correo del destinatario del mensaje
- El destinatario del mensaje cuenta con la dirección del remitente en la lista Remitentes seguros (asegúrese de haber configurado la sincronización de la lista Remitentes seguros dentro del entorno del servidor de Exchange que incluye la Agregación de lista segura)

Si se aplica alguno de estos casos en un mensaje entrante, se omitirá la verificación antispam para este mensaje; por lo tanto, no se evaluará el mensaje en busca de SPAM y se enviará al buzón de correo del destinatario.

Aceptar el indicador de evasión de antispam configurado en la sesión de SMTP

Es útil cuando ha autenticado las sesiones de SMTP entre los servidores de Exchange con la configuración de omisión de antispam. Por ejemplo, cuando cuenta con un servidor Edge y un servidor Hub, no es necesaria la exploración del tráfico entre estos dos servidores. La función **Aceptar indicador de omisión de antispam configurado en la sesión SMTP** se habilita en forma predeterminada pero solo se aplica cuando el indicador de omisión de antispam esté configurado para la sesión SMTP en el servidor Exchange. Si deshabilita **Aceptar indicador de omisión de antispam configurado en la sesión SMTP**, ESET Mail Security explorará la sesión SMTP para detectar spam independientemente de la configuración de omisión de antispam del Exchange Server.

> i Debe actualizar la base de datos antispam regularmente para que el módulo antispam proporcione la mejor protección. Para permitir las actualizaciones periódicas de la base de datos antispam, asegúrese de que ESET Mail Security tenga acceso a las direcciones IP correctas en los puertos necesarios. Para obtener más información sobre qué IP y puertos habilitar en el firewall de terceros, consulte el artículo de base de conocimiento.

Encontrará la configuración de las características en sus secciones:

- Filtro y verificación
- Configuración avanzada
- Configuración de la lista gris
- SPF y DKIM
- Protección contra retrodispersión
- Protección contra la suplantación de identidad del remitente

Filtro y verificación

Puede configurar listas de Permitidos, Bloqueados e Ignorados al especificar criterios como la dirección o el rango IP, el nombre del dominio, etc. Para agregar, modificar o eliminar criterios, haga clic en **Editar** para abrir la lista que desea administrar.

Las direcciones IP o dominios incluidos en las **listas de ignorados** no serán analizados por antispam, pero se aplicarán otras técnicas de protección antispam.
Las listas de ignorados deben contener todas las direcciones IP/nombres de dominio de la infraestructura interna. También puede incluir direcciones IP/nombres de dominio de los ISP o servidores de correo de envío externo que están actualmente en la lista negra de uno de los RBL o DNSBL (lista negra de la nube: lista de bloqueo de ESET o lista de bloqueo de terceros).
Esto le permite recibir correos electrónicos de fuentes incluidas en las listas de ignorados, aunque sus direcciones IP estén en la lista negra de la nube. Tales correos electrónicos entrantes se reciben y su contenido se inspecciona adicionalmente mediante otras técnicas de protección antispam.

Lista de IP aprobada	Coloca automáticamente en la lista blanca a los correos electrónicos que se originan desde direcciones IP especificadas. No se comprobará el contenido del correo electrónico.
Lista de IP bloqueada	Bloquea automáticamente los correos electrónicos que se originan desde direcciones IP especificadas.
Lista de IP ignorada	Lista de direcciones IP que se ignorarán durante la clasificación. Se comprobará el contenido del correo electrónico. Use la barra deslizadora Forma parte de la infraestructura interna si está colocando en la lista blanca las direcciones IP locales de la red; consulte el ejemplo a continuación.
Lista de dominios de remitentes bloqueados	Bloquea los mensajes de correo electrónico que contienen un dominio especificado en el cuerpo del mensaje. Solo se aceptan dominios con TLD (dominio de nivel superior) real.
Lista de dominios de remitentes ignorados	Los dominios especificados en el cuerpo del mensaje se ignorarán durante la clasificación. Solo se aceptan dominios con TLD (dominio de nivel superior) real.
Lista de IP de remitentes bloqueada	Bloquea los mensajes de correo electrónico que contienen una dirección IP especificada en el cuerpo del mensaje.
Lista de IP de remitentes ignorada	Las direcciones IP especificadas en el cuerpo del mensaje se ignorarán durante la clasificación.
Lista de remitentes aprobados	Envía a la lista blanca los correos electrónicos que tienen su origen en un remitente específico. Para la verificación solo se utiliza una dirección de remitente o un dominio completo, en función de la siguiente prioridad: 1.SMTP 'MAIL FROM' dirección 2.Campo del encabezado del correo electrónico "Return-Path:" 3.Campo del encabezado del correo electrónico "X-Env-Sender:" 4.Campo del encabezado del correo electrónico "From:" 5.Campo del encabezado del correo electrónico "Sender:" 6.Campo del encabezado del correo electrónico "X-Apparently-From:"
Lista de remitentes bloqueados	Bloquea los correos electrónicos procedentes de un remitente específico. Para la verificación se utilizan todas las direcciones de remitentes identificadas o todos los dominios: SMTP 'MAIL FROM' dirección Campo del encabezado del correo electrónico "Return-Path:" Campo del encabezado del correo electrónico "X-Env-Sender:" Campo del encabezado del correo electrónico "From:" Campo del encabezado del correo electrónico "Sender:" Campo del encabezado del correo electrónico "X-Apparently-From:"
Lista de dominios a IP aprobados	Coloca en la lista blanca a los correos electrónicos que se originan desde direcciones IP que son resueltas desde dominios especificados en esta lista. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.
Lista de dominios a IP bloqueados	Bloquea los correos electrónicos que se originan desde direcciones IP que son resueltas desde dominios especificados en esta lista. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.

Lista de dominios a IP ignorados	Lista de dominios que se resuelve a direcciones IP que a la vez no se verificarán durante la clasificación. Los registros del SPF (marco de directivas de remitente) se reconocen al resolver las direcciones de IP.
Lista de países bloqueados	Bloquea correos electrónicos de países especificados. El bloqueo se basa en GeoIP. Si se envía un mensaje de spam desde el servidor de correo con la dirección IP incluida en la base de datos de geolocalización para un país seleccionado en los países bloqueados, se marcará automáticamente como correo no deseado y se tomará una acción de acuerdo con los ajustes de la Acción para aceptar mensajes no deseados en la Protección de transporte de correo.

Las listas de dominio del cuerpo aceptan dominios con TLD (dominio de nivel superior) real solamente, según la Base de datos de zona de raíz de los TLD.

Si desea agregar más entradas, haga clic en **Ingresar valores múltiples** en la ventana **Agregar** y seleccione el separador que debe utilizarse. Puede ser una línea nueva, una coma o un punto y coma.

Objetivo: Excluya las direcciones IP locales de su infraestructura de la protección antispam al agregarlos a la lista Ignorar IP.
Navegue a **Configuración avanzada (F5)** > **Servidor** > **Protección antispam** > **Filtro y verificación**.
Haga clic en **Editar** junto a **lista de IP ignorada**.
Haga clic en **Agregar** y especifique el rango de direcciones IP de su infraestructura de red (formato de rango de direcciones IP *1.1.1.1-1.1.1.255*). Si fuera necesario, puede continuar agregando más rangos (o direcciones IP individuales) a la lista.
Use la barra deslizadora **Es parte de la infraestructura interna**.

Creación de listas grises y SPF

Especifique el dominio con la lista blanca de IP o la lista blanca de IP para evadir automáticamente las listas grises y SPF. Podrá ver los archivos de registro en el registro de protección SMTP. Para usar estas opciones, deberá habilitar Creación de listas grises o SPF. En el caso de SPF, deberá habilitar la configuración **Rechazar mensajes automáticamente si falla la verificación de SPF** y/o **Omitir automáticamente la creación de listas grises si la verificación de SPF es correcta**.

Utilizar listas antispam para evadir automáticamente las listas grises y SPF

Cuando se habilita, la lista de IP aprobada e ignorada se usará en conjunto con las listas blancas de IP y de dominio a IP para evitar automáticamente la creación de listas grises y SPF.

Lista blanca de IP

Puede agregar direcciones de IP, direcciones de IP con máscara, rango de IP. Puede modificar la lista con un clic en **Agregar**, **Editar** o **Eliminar**. De manera alternativa, puede importar su lista personalizada desde un archivo en lugar de agregar cada entrada de forma manual. Haga clic en **Importar** y busque el archivo que contenga las entradas que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo, seleccione **Exportar** desde el menú contextual.

Las listas blancas prevalecen sobre las listas negras; es decir, si un correo electrónico que contiene direcciones de listas blancas y negras, se incluye en una lista blanca. Solo se comprueba la última dirección del remitente y el número máximo de direcciones verificadas desde los encabezados Recibido: con las listas blancas. Todas las direcciones se comprueban con las listas negras locales.

Lista blanca de dominios a IP

Esta opción le permite especificar dominios (por ejemplo, domainname.local). Para manejar esta lista, use **Agregar**, **Eliminar** o **Eliminar todo**. Si quiere importar su lista personalizada desde un archivo en lugar de agregar cada entrada de forma manual, haga clic en **Importar** y busque el archivo que contenga las entradas que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo, seleccione **Exportar** desde el menú contextual.

> La creación de listas grises y SPF se someten a la evaluación de la protección del transporte de correo electrónico y le permiten usar las listas blancas de IP y de dominio a IP, así como las listas de IP aprobadas e ignoradas. No obstante, si utiliza reglas de SPF, ninguna de las listas blancas se tomarán en cuenta para las reglas.

Configuración avanzada de antispam

Realice estas configuraciones para que los mensajes sean verificados por servidores externos (definidos como **RBL** - Listas de bloqueo en tiempo real y **DNSBL** - Lista de bloqueo DNS) de acuerdo con sus criterios predeterminados. Los servidores RBL se consultan con direcciones IP extraídas de Received: encabezados, y los servidores DNSBL se consultan con direcciones IP y dominios extraídos del cuerpo del mensaje.

Para obtener una explicación detallada, consulte los artículos sobre RBL y DNSBL.

Número máximo de direcciones verificadas de Received: encabezados

Puede limitar la cantidad de direcciones IP verificadas por antispam. Esto involucra las direcciones IP escritas en los encabezados de Received: from. El valor predeterminado es 0, lo que significa que solo se comprueba la dirección IP del último remitente identificado.

Verificar la dirección del remitente con la lista negra de usuarios finales

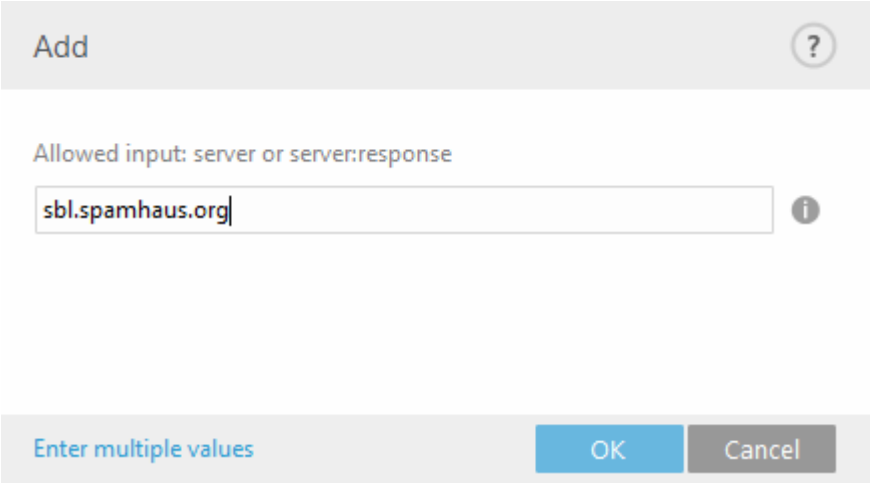
Los mensajes de correo electrónico que no se envían desde servidores de correo (equipos que no están en la lista de servidores de correo) se verifican para asegurarse de que el remitente no esté en la lista negra. Esta opción está activada de forma predeterminada. Puede desactivarla si es necesario, pero los mensajes no enviados desde servidores de correo no se verificarán con respecto a la lista negra.

> Los resultados de listas de bloqueo de terceros externas tienen prioridad sobre la lista negra de usuarios finales para las direcciones IP de los Received: from encabezados. Todas las direcciones IP (hasta el número máximo especificado de direcciones verificadas) se envían para su evaluación por servidores de terceros externos.

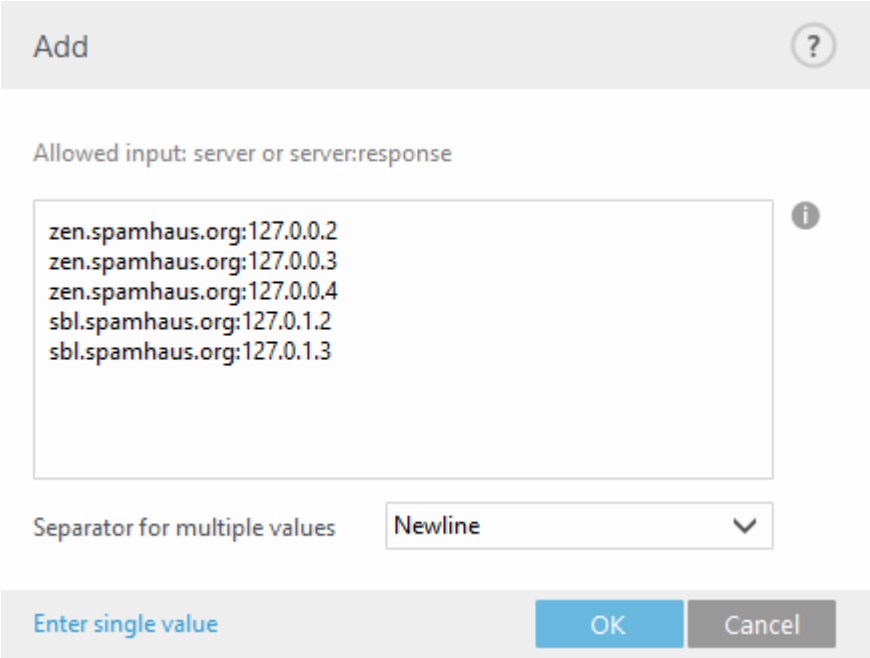
Servidores RBL adicionales

Es una lista de servidores de Listas de bloqueo en tiempo real (RBL) que se consultan cuando se analizan los mensajes.

> Cuando agrega servidores RBL adicionales, ingrese el nombre de dominio del servidor (por ejemplo, sbl.spamhaus.org). Funcionará con cualquier código de devolución que sea compatible con el servidor.



Como alternativa, puede especificar un nombre de servidor con un código de devolución en la forma de server:response (por ejemplo, zen.spamhaus.org:127.0.0.4). Al utilizar este formato, recomendamos que agregue el nombre de cada servidor y el código de devolución de manera separada, para lograr una lista completa. Haga clic en **Ingresar valores múltiples** en la ventana **Agregar** para especificar todos los nombres de servidores con sus códigos de retorno. Las entradas deben verse como el siguiente ejemplo, sus nombres reales de host de servidor RBL y los códigos de retorno pueden variar:



De manera alternativa, puede importar su lista personalizada desde un archivo () en lugar de agregar cada entrada de forma manual. Haga clic en **Importar** y busque el archivo que contenga las entradas que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo, seleccione **Exportar** desde el menú contextual.

Límite de ejecución de la consulta de RBL (en segundos)

Esta opción permite que establezca un plazo máximo para las consultas RBL. Las respuestas RBL solo se usan desde aquellos servidores RBL que responden a tiempo. Si el valor está configurado en “0”, no se aplicará el tiempo de espera.

Número máximo de direcciones verificadas contra RBL

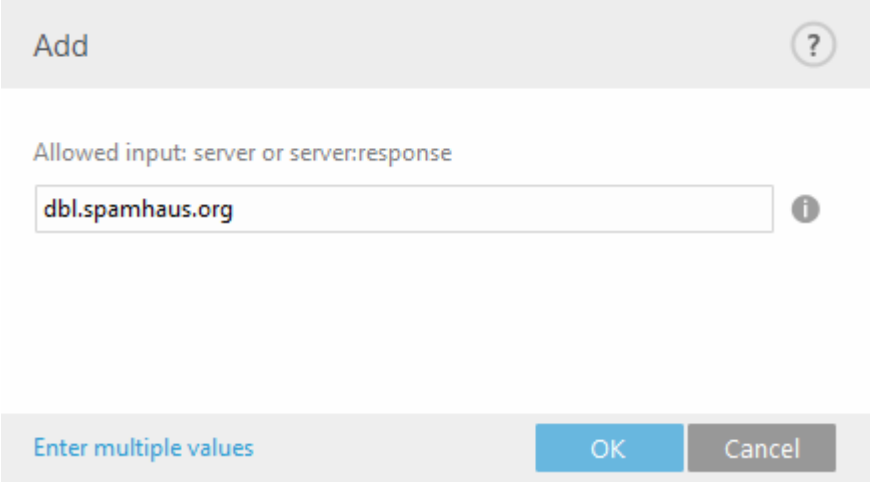
Esta opción le permite limitar la cantidad de direcciones IP que se consultan en el servidor RBL. Tenga en cuenta

que la cantidad total de las consultas RBL será la cantidad de direcciones IP en el encabezado Recibido: (hasta una cantidad máxima de dirección IP en RBL) multiplicada por la cantidad de servidores RBL determinada en la lista RBL. Si el valor está configurado en “0”, se verifica la cantidad ilimitada de encabezados recibidos. Tenga en cuenta que las direcciones IP que figuran en la lista de IP ignoradas no se cuentan para el límite de direcciones IP en RBL.

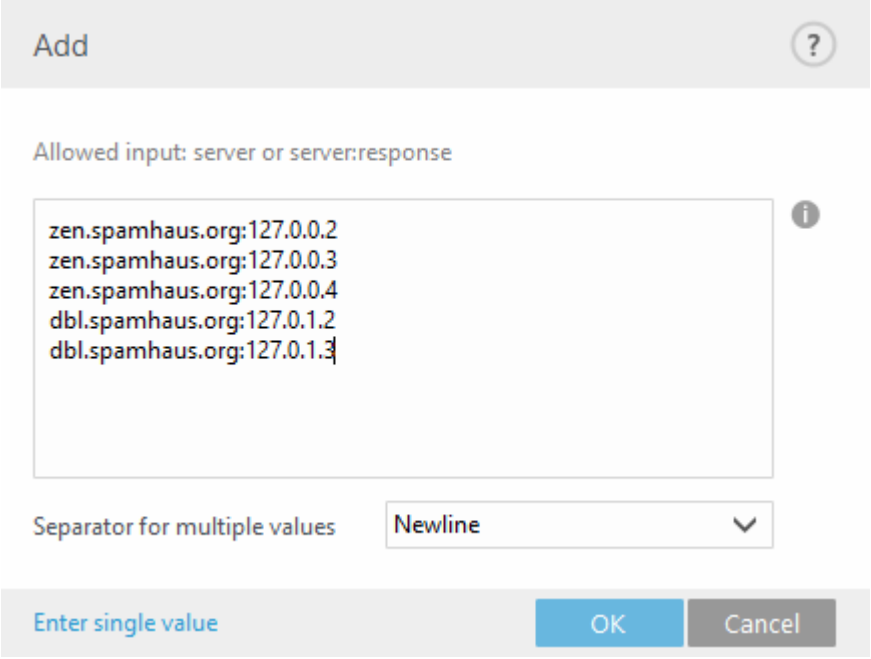
Servidores DNSBL adicionales

Es una lista de servidores de Lista de bloqueo DNS (DNSBL) que se consultan con los dominios y las direcciones IP extraídos del cuerpo del mensaje.

> Cuando agrega servidores DNSBL adicionales, ingrese el nombre de dominio del servidor (por ejemplo, dbl.spamhaus.org). Funcionará con cualquier código de devolución que sea compatible con el servidor.



Como alternativa, puede especificar un nombre de servidor con un código de devolución en la forma de server:response (por ejemplo, zen.spamhaus.org:127.0.0.4). En este caso, recomendamos que agregue el nombre de cada servidor y el código de devolución de manera separada, para obtener una lista completa. Haga clic en **Ingresar valores múltiples** en la ventana **Agregar** para especificar todos los nombres de servidores con sus códigos de retorno. Las entradas deben verse como el siguiente ejemplo, sus nombres reales de host de servidor DNSBL y los códigos de retorno pueden variar:



Límite de ejecución de la consulta de DNSBL (en segundos)

Le permite configurar un tiempo de espera máximo para todas las consultas DNSBL que deban completarse.

Cantidad máxima de dominios verificados con DNSBL

Le permite limitar la cantidad de direcciones IP que se consultan en el servidor de Lista de bloqueo DNS.

Número máximo de dominios verificados contra DNSBL

Le permite limitar la cantidad de dominios que se consultan en el servidor de Lista de bloqueo DNS.

Tamaño máximo de la exploración del archivo (KB)

Limita la exploración Antispam para los mensajes mayores al valor especificado. El valor predeterminado 0 se refiere al escaneo ilimitado del tamaño de los mensajes. Por lo general, no hay razón para limitar el análisis de antispam, pero si necesita limitarlo en determinadas situaciones, cambie el valor al tamaño requerido. Cuando se encuentra definido, el motor antispam procesará mensajes hasta el tamaño especificado e ignorará mensajes de mayor tamaño.

> El límite más pequeño posible es 12 kB. Si ajusta el valor del 1 a 12, el motor antispam siempre leerá, al menos, 12 kB.

Activar el rechazo temporal de los mensajes indeterminados

Si el motor de correo no deseado no puede determinar si el mensaje es o no CORREO NO DESEADO, lo que significa que el mensaje tiene algunas características sospechosas de CORREO NO DESEADO pero no las suficientes para marcarlo como CORREO NO DESEADO (por ejemplo, el comienzo de una campaña o el origen de un rango IP con varias clasificaciones), esta configuración (cuando está habilitada) permite ESET Mail Security el rechazo temporal de dicho mensaje, de la misma manera que lo hacen las listas grises, y permite continuar con el rechazo durante un período específico, hasta:

- El intervalo ha finalizado y el mensaje se aceptará en el siguiente intento de envío. El mensaje queda con la clasificación inicial (CORREO ELECTRÓNICO NO DESEADO o DESEADO).
- La nube antispam recopila datos suficientes y puede clasificar correctamente el mensaje antes de que finalice el intervalo.

ESET Mail Security no guarda el mensaje rechazado ya que el servidor de correo lo debe volver a enviar según SMTP RFC.

Habilitar el envío de mensajes rechazados temporalmente para su análisis

El contenido del mensaje se envía automáticamente para realizar un análisis más profundo. Esto ayuda a mejorar la clasificación de los mensajes de correo electrónico futuros.

> Es posible que los mensajes rechazados temporalmente que se envíen para análisis sean en realidad mensajes DESEADOS. En pocas ocasiones, los mensajes rechazados temporalmente pueden usarse para una evaluación manual. Habilite esta característica solo si no existen riesgos de filtrar datos potencialmente sensibles.

Configuración de la lista gris

La función **Habilitar las listas grises** activa una característica que protege a los usuarios ante el spam mediante la siguiente técnica: El agente de transporte enviará un valor devuelto SMTP de “rechazo temporal” (el predeterminado es 451/4.7.1) por cualquier correo electrónico recibido que no pertenezca a un remitente conocido. Un servidor legítimo intentará volver a enviar el mensaje luego de un tiempo de espera. Por lo general, los servidores de spam no intentarán reenviar el mensaje, ya que hacen envíos a miles de direcciones de correo electrónico y no pierden tiempo reenviando el spam. La creación de listas grises es una capa adicional de protección antispam y no produce ningún efecto en la capacidad del módulo antispam para evaluar spam.

Al evaluar la fuente del mensaje, el método de creación de listas grises tiene en cuenta las listas de Direcciones IP aprobadas, Direcciones IP ignoradas, Remitentes seguros y Permitir IP en el servidor de Exchange, así como la configuración de la propiedad Omitir antispam para el buzón de correo del destinatario. Los correos electrónicos de estas listas de remitentes/direcciones IP o los distribuidos a un buzón de correo con la opción Omitir antispam habilitada, no serán examinados por el método de detección de listas grises.

Usar solo la parte de dominio de la dirección del remitente

Esta característica ignora el nombre del remitente en la dirección de correo electrónico; solo se considera el dominio.

Sincronizar las bases de datos de creación de listas grises en el clúster de ESET

Las entradas de la base de datos de la lista gris se comparten en tiempo real entre los servidores del clúster de ESET. Cuando uno de los servidores recibe un mensaje que procesa la lista gris, esta información la difunde ESET Mail Security sobre el resto de los nodos en el clúster de ESET.

Límite de tiempo para la denegación de la conexión inicial (min.)

Cuando se envía por primera vez un mensaje y se rechaza temporalmente, este parámetro define el período durante el cual siempre se rechazará el mensaje (determinado a partir del tiempo del primer rechazo). Cuando haya transcurrido el período definido, el mensaje se recibirá correctamente. El valor mínimo para ingresar es de 1 minuto.

Tiempo de vencimiento de las conexiones no verificadas (horas)

Este parámetro define el intervalo de tiempo mínimo para guardar el trío de datos. Un servidor válido debe reenviar un mensaje deseado antes de que transcurra este período. Este valor debe ser mayor que el valor del **Límite de tiempo para la denegación de conexión inicial**.

Tiempo de vencimiento de las conexiones verificadas (días)

La cantidad mínima de días para guardar el trío de datos, durante la cual los correos electrónicos provenientes de un remitente específico se recibirán sin ninguna demora. Este valor debe ser mayor que el valor del **Tiempo de vencimiento de las conexiones no verificadas**.

Respuesta SMTP para conexiones denegadas temporalmente.

Especifique un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Ejemplo de un mensaje de respuesta de rechazo del SMTP:

Código de respuesta	Código de estado	Mensaje de respuesta
451	4.7.1	Inténtelo de nuevo más tarde

> También puede usar variables del sistema para definir la respuesta de rechazo del SMTP.

> la sintaxis incorrecta en los códigos de respuesta SMTP puede provocar que la protección por listas grises no funcione correctamente. Como resultado, es posible que los mensajes de spam se envíen a los clientes o que directamente no se envíen.

Todos los mensajes que se han evaluado usando el método de creación de listas grises se guardan en el registro de protección SMTP.

SPF y DKIM

El marco de directiva del remitente (SPF) y el correo identificado con clave de dominio (DKIM) son métodos de validación que comprueban que los mensajes de correo electrónico entrantes de dominios específicos estén autorizados por el propietario de ese dominio. Esto ayuda a proteger a los destinatarios de recibir mensajes de correo electrónico falsificado. ESET Mail Security usa también la evaluación Autenticación, informes y conformidad de mensajes basados en dominio (DMARC) para mejorar a SPF y DKIM aún más.

SPF

Una comprobación SPF verifica que un remitente legítimo haya enviado un correo electrónico. Se realiza una búsqueda de DNS para los registros del SPF del dominio del remitente para obtener una lista de direcciones IP. Si alguna de las direcciones IP de los registros del SPF coincide con la dirección IP real del remitente, el resultado de la comprobación del SPF es **Aprobado**. Si la dirección IP real del remitente no coincide, el resultado es **Error**. Sin embargo, no todos los dominios tienen registros del SPF especificados en DNS. Si no existen registros del SPF en DNS, el resultado es **No disponible**. En ocasiones, se podría exceder el tiempo de espera de la solicitud DNS; en ese caso, el resultado también es **No disponible**.

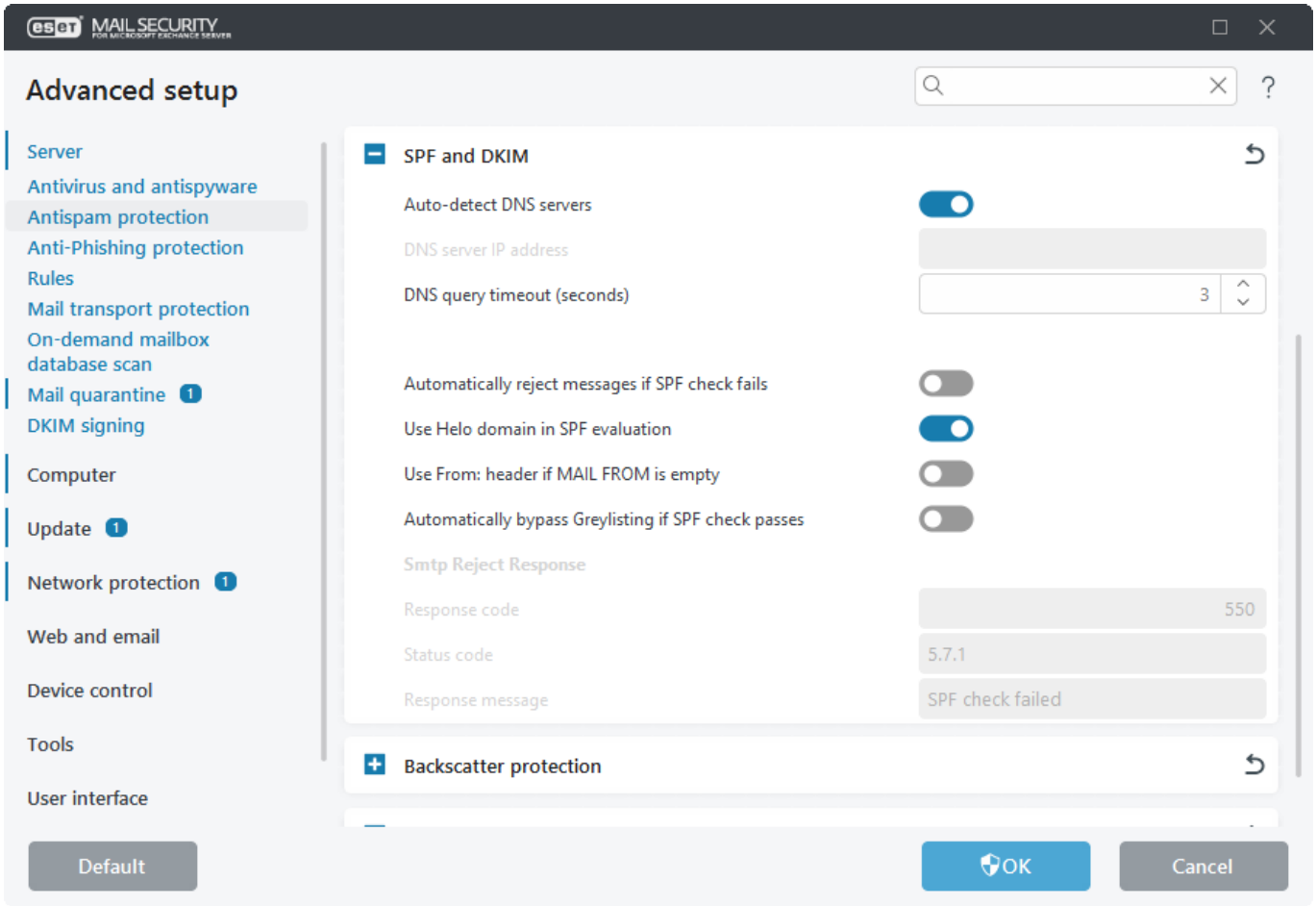
DKIM

Las organización lo usan para evitar la suplantación de mensajes de correo electrónico al agregar una firma digital a los mensajes salientes según el estándar DKIM. Esto implica usar una clave de dominio privado para cifrar los encabezados de correo saliente del dominio y agregar una versión pública de la clave a los registros DNS del dominio. ESET Mail Security puede luego recuperar la clave pública para descifrar encabezados entrantes y verificar que los mensajes realmente provienen de su dominio y que sus encabezados no han sufrido cambios en el camino.

> Exchange Server 2010 y sus versiones anteriores no son totalmente compatibles con DKIM, porque los encabezados incluidos en los mensajes entrantes firmados digitalmente pueden ser modificados durante la validación de DKIM.

DMARC

DMARC se basa en los mecanismos SPF y DKIM existentes. Puede usar reglas de protección de transporte de correo para evaluar los **resultados de DMARC** y **aplicar la acción de políticas DMARC**.



Detectar servidores DNS automáticamente

La detección automática usa la configuración del adaptador de red.

Dirección IP del servidor DNS

Si desea usar servidores DNS específicos para el SPF y DKIM, ingrese la dirección IP (en formato IPv4 o IPv6) del servidor DNS que desea usar.

Tiempo de espera de la consulta de DNS (en segundos)

Especifique un tiempo de espera para la respuesta DNS.

Rechazar mensajes automáticamente si falla la verificación de SPF

Si el resultado de la comprobación del SPF sea incorrecta al comienzo, se puede rechazar el mensaje de correo electrónico antes de la descarga.

La verificación SPF se realiza en la capa SMTP. Sin embargo, puede rechazarse automáticamente en la capa SMTP o durante la evaluación de reglas.
Los mensajes rechazados no se pueden registrar en el Registro de eventos cuando se usa el rechazo automático en la capa SMTP. Esto se debe a que el registro se realiza por acción de regla y el rechazo automático se realiza directamente en la capa SMTP, que sucede antes de la evaluación de la regla. Dado que los mensajes serán rechazados antes de que se evalúen las reglas, no hay información para registrar en el momento de la evaluación de la regla.
Puede registrar mensajes rechazados, pero solo si rechaza los mensajes por una acción de regla. Para rechazar los mensajes que no superaron el SPF, compruebe y registre dichos mensajes rechazados, deshabilite Rechazar **automáticamente los mensajes si falla la verificación de SPF** y cree la siguiente regla para la **Protección de transporte de correo**:
Condición
- Tipo: Resultado de SPF
- Operación: es
- Parámetro: Error

Acciones
- Tipo: Rechazar mensaje
- Tipo: Registrar eventos

Usar el dominio Helo en la evaluación de SPF

Esta característica usa el dominio HELO para la evaluación de SPF. Si no se especifica el dominio HELO, se usa el nombre de host del equipo.

Usar From: encabezado si MAIL FROM está vacío

El encabezado MAIL FROM puede estar vacío y también se puede falsificar fácilmente. Cuando esta opción está habilitada y MAIL FROM está vacío, se descarga el mensaje y, en cambio, se utiliza el encabezado From:.

Omitir automáticamente la lista gris si la verificación de SPF es correcta

No existe motivo para usar la lista gris para los mensajes que aprobaron la comprobación del SPF.

Respuesta de rechazo de SMTP

Puede especificar un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Puede ingresar un mensaje de respuesta con el siguiente formato:

Código de respuesta	Código de estado	Mensaje de respuesta
550	5.7.1	Comprobación del SPF incorrecta

Protección contra retrodispersión

La retrodispersión de spam son mensajes rebotados mal dirigidos enviados por servidores de correo y un efecto secundario no deseado del spam. Cuando el servidor de correo del destinatario rechaza un mensaje de spam, se envía un informe de no entrega (NDR), también conocido como mensaje rebotado, a un remitente supuesto (dirección de correo electrónico falsificada como remitente del mensaje de spam original), no al remitente real del spam. El propietario de la dirección de correo electrónico recibe un mensaje NDR, a pesar de no estar involucrado con el mensaje de spam original. Aquí es donde entra en juego **la protección de retrodispersión**. Puede evitar que los NDR spam se entreguen a las casillas de correo electrónico de los usuarios dentro de la organización mediante el uso de ESET Mail Security protección contra retrodispersión.

Cuando usted **Habilita el control de NDR**, debe especificar la **unidad de firma** (una cadena de al menos 8 caracteres, como una frase de contraseña. ESET Mail Security La protección contra dispersión `X-Eset-NDR: <hash>` en el encabezado de cada mensaje de correo electrónico de salida. La `<hash>` es una firma cifrada que además contiene la **unidad de firma** que ha especificado.

Si no se puede entregar un mensaje de correo electrónico legítimo, su servidor de correo generalmente recibe un NDR, que se verifica mediante ESET Mail Security al buscar la `X-Eset-NDR: <hash>` en los encabezados. Si `X-Eset-NDR:` está presente y la firma `<hash>` coincide, el NDR se envía al remitente del mensaje de correo electrónico legítimo para indicar que se ha producido un error en el envío del mensaje. Si `Eset-NDR:` no está presente o la firma `<hash>` es incorrecta, se identifica como una retrodispersión de spam y se rechaza el NDR.

Rechaza mensajes automáticamente si la comprobación del SPF es incorrecta

Si el resultado de la comprobación del SPF sea incorrecta al comienzo, se puede rechazar el mensaje de correo electrónico antes de la descarga.

Podrá ver la actividad de **Protección contra retrodispersión** en el registro de protección SMTP.

Protección contra la suplantación de identidad del remitente

La suplantación de remitentes de correo electrónico es habitual cuando un atacante falsifica el nombre o la dirección de correo electrónico del remitente para engañar al destinatario. Para el destinatario del correo electrónico, este tipo de correo electrónico de suplantación no puede distinguirse de uno auténtico, lo que supone un riesgo. Un tipo de suplantación de remitente se llama fraude CEO (el atacante suplanta al CEO).

Los empleados no cuestionarían los correos electrónicos de este tipo, lo que permitiría que el atacante tuviera éxito. Esto no es exclusivo del CEO. La suplantación de remitentes a menudo suplanta a cualquier remitente real, generalmente alguien de Active Directory de su organización. En tal sentido, un mensaje de correo electrónico suplantado parece muy convincente para un destinatario que no sospecha, lo que le permite ganar fácilmente confianza.

ESET Mail Security le proporciona protección contra la suplantación de remitentes de correo electrónico. La protección contra la suplantación de remitente verifica si la información del remitente es válida utilizando varios métodos.

La protección contra la suplantación de remitente busca el dominio contenido en el campo del encabezado del correo electrónico «Desde:» y el remitente del sobre y, a continuación, compara el dominio encontrado con las listas de dominio. Si el dominio Diferencia, el mensaje se considera válido (no suplantado) y otras capas de protección de ESET Mail Security lo procesan. Sin embargo, si el dominio coincide con un dominio de la lista, podría estar suplantado y requerir una verificación posterior.

En función de la configuración, se realiza una verificación posterior: una comprobación de SPF, la dirección IP del sobre se comprueba con las listas de IP o el mensaje se considera automáticamente como suplantado. Si se aprueba el resultado de la comprobación de SPF o la IP del sobre coincide con una IP de la lista, el mensaje será válido. De no ser así, está suplantado. Se inicia una acción con el mensaje suplantado.

Puede utilizar la protección contra la suplantación de remitente de dos maneras:

- Active **Protección contra suplantación de remitente,** configure sus ajustes y, si lo desea, especifique

dominios y listas de IP. La acción predeterminada con los mensajes de correo electrónico suplantados es **Poner mensaje en cuarentena.** Para cambiar la acción que se está haciendo, vaya a la configuración avanzada de Protección del transporte de correo.

- Usar reglas de protección del transporte de correo electrónico: **resultado SPF del remitente del encabezado** o **Remitente del sobre envolvente y de la condición del resultado de la comparación del encabezado De** con la acción que elija. Las reglas le ofrecen más opciones y combinaciones si desea lograr un comportamiento específico en relación con los mensajes de correo electrónico suplantados.

Cuando se utiliza la **Protección contra la suplantación de identidad del remitente** o se especifica el tipo de acción de una regla **Registrar en eventos**, todos los mensajes evaluados por la **Protección contra la suplantación de identidad del remitente** se registran en los Archivos de registro. Del mismo modo, puede encontrar mensajes de correo electrónico suplantados en Cuarentena de correo cuando se configura una acción como **Mensaje en cuarentena** en Protección del transporte de correo o se define en reglas.

Activar protección contra la suplantación de identidad del remitente

Active la protección contra la suplantación de remitente para evitar ataques de correo electrónico que intenten engañar a los destinatarios sobre el origen del mensaje (remitente suplantado).

Activar correos electrónicos entrantes con mi propio dominio en la dirección del remitente

Permita que se verifiquen los mensajes que contengan su propio dominio en el encabezado de correo electrónico "From:" o en el remitente del sobre (por lo que se sospecha que está siendo suplantado):

- **Solo cuando pasan la verificación de SPF**: se basa en que SPF esté habiltado. Si se aprueba el resultado de SPF, el mensaje se considera válido y se procesa para su entrega. Si el resultado de SPF falla, el mensaje se considera suplantado (tiene lugar una acción). De manera opciona, puede habilitar Rechazar mensajes automáticamente si falla la verificación de SPF.

- **Solo cuando la IP está en la lista de IP de infraestructura**: compara la dirección IP del sobre con las listas de IP (una lista de sus propias direcciones IP y la lista de IP ignoradas marcadas como **Es parte de la infraestructura interna**). Si la IP coincide, el mensaje es válido y se procesa para su entrega. Si la IP no coincide, el mensaje se considera suplantado y se realiza una acción.

- **Nunca**: si un mensaje entrante contiene su propio dominio en el encabezado de correo electrónico o en el remitente del sobre, se considerará automáticamente como suplantado sin verificarlo. Se inicia una acción con el mensaje; consulte Protección del transporte de correo para conocer las opciones de acción.

Cargar mis propios dominios automáticamente desde la lista de dominios aceptados

Se recomienda encarecidamente activar esta opción para mantener el máximo nivel de protección. De esta forma, la protección contra la suplantación del remitente que tiene lugar durante la evaluación tiene en cuenta los dominios y las direcciones IP de su infraestructura.

Lista de mis propios dominios

Estos dominios se consideran propios. Agregue los dominios que se utilizarán durante la evaluación, además de los dominios cargados automáticamente desde Active Directory. Los dominios del remitente se compararán con los dominios de estas listas. Si el dominio no coincide, el mensaje es válido. Si el dominio coincide, se realiza una verificación posterior de acuerdo con la opción **Activar correo electrónico entrante con mi propio dominio en la dirección del remitente**.

Lista de mis propias direcciones IP

Direcciones IP que se consideran creíbles. Agregue las direcciones IP que se utilizarán durante la evaluación, además de las direcciones IP de la lista de IP ignoradas marcadas como **Es parte de la infraestructura interna.** La dirección IP del sobre del remitente se compara con las direcciones IP de estas listas. Si la dirección IP del sobre coincide, el mensaje será válido. Si la IP no coincide, el mensaje se considera suplantado y se realiza una acción.

Protección Anti-Phishing

El phishing es un intento por obtener información confidencial tales como nombres de usuario, contraseñas, cuentas bancarias o detalles de tarjeta de crédito y mediante correo electrónico o páginas web ocultadas detrás de una entidad de confianza. Esta actividad en general se realiza con motivos maliciosos. Es una forma de ingeniería social (la manipulación de los usuarios para obtener información confidencial).

ESET Mail Security incluye protección anti-phishing que evita que los usuarios accedan a páginas web conocidas por phishing. En el caso de mensajes de correo electrónico que pudieran contener enlaces que conducen a páginas web con phishing, ESET Mail Security usa un analizador sofisticado que busca en el cuerpo y el asunto de los mensajes de correo electrónico entrantes para identificar dichos enlaces (URL) peligrosos.

Los enlaces se comparan con una base de datos de phishing. Si el resultado de la evaluación es positivo, el mensaje de correo electrónico se considera un mensaje de phishing y ESET Mail Security lo tratar según la configuración **Acción para adoptar con el mensaje de phishing** para cada capa de protección (Protección del transporte de correo electrónico, Protección de la base de datos del buzón de correo electrónico y Exploración de base de datos del buzón de correo a petición). También se ejecutan la acciones de la regla.

Estándares de formato de correo electrónico compatible:

- Texto plano:
- Solo HTML
- MIME
- MIME de parte múltiple (correo electrónico que incluye ambas partes, HTML y texto plano)

Entidades HTML compatibles:

Los mensajes de phishing podrían contener entidades HTML para ofuscar el motoro anti-phishing. La protección antiphishing también analiza y traduce símbolos HTML para encontrar y evaluar correctamente las URL ofuscadas.

Un único carácter se puede representar de formas diferentes. Por ejemplo, un período puede ser representado de las siguientes formas:

Las maneras en que los vínculos aparecen usualmente en el mensaje de correo electrónico para el usuario.	Valor	Enlaces ofuscados contenidos en el cuerpo del mensaje	Tipo
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	carácter
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	nombre de la entidad
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	número hexadecimal de la entidad

Las maneras en que los vínculos aparecen usualmente en el mensaje de correo electrónico para el usuario.	Valor	Enlaces ofuscados contenidos en el cuerpo del mensaje	Tipo
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	número decimal de la entidad

Para ver la actividad de protección de correo Anti-Phishing, consulte **Archivos de registro** > Registro de protección del servidor de correo. El registro contiene información sobre los mensajes de correo electrónico y sus enlaces de phishing.

Informar una página de phishing

Puede hacer clic en Informar para notificar a ESET sobre un sitio web malicioso o de phishing.

Reglas

Las Reglas le permiten definir manualmente las condiciones de filtrado de correo electrónico y asignar las acciones de correo electrónico filtrado. También puede definir diferentes condiciones y acciones individualmente para Protección del transporte de correo electrónico, Protección de la base de datos del buzón de correo electrónico y Exploración de base de datos del buzón de correo a petición. Esto es útil porque cada tipo de protección usa un enfoque ligeramente diferente al procesar mensajes, en especial la Protección del transporte de correo electrónico.

La disponibilidad de reglas para la Protección de la base de datos del buzón de correo electrónico, Exploración de base de datos del buzón de correo a petición y Protección del transporte de correo electrónico en su sistema depende de la versión de Microsoft Exchange Server que tenga instalada en el servidor con ESET Mail Security.

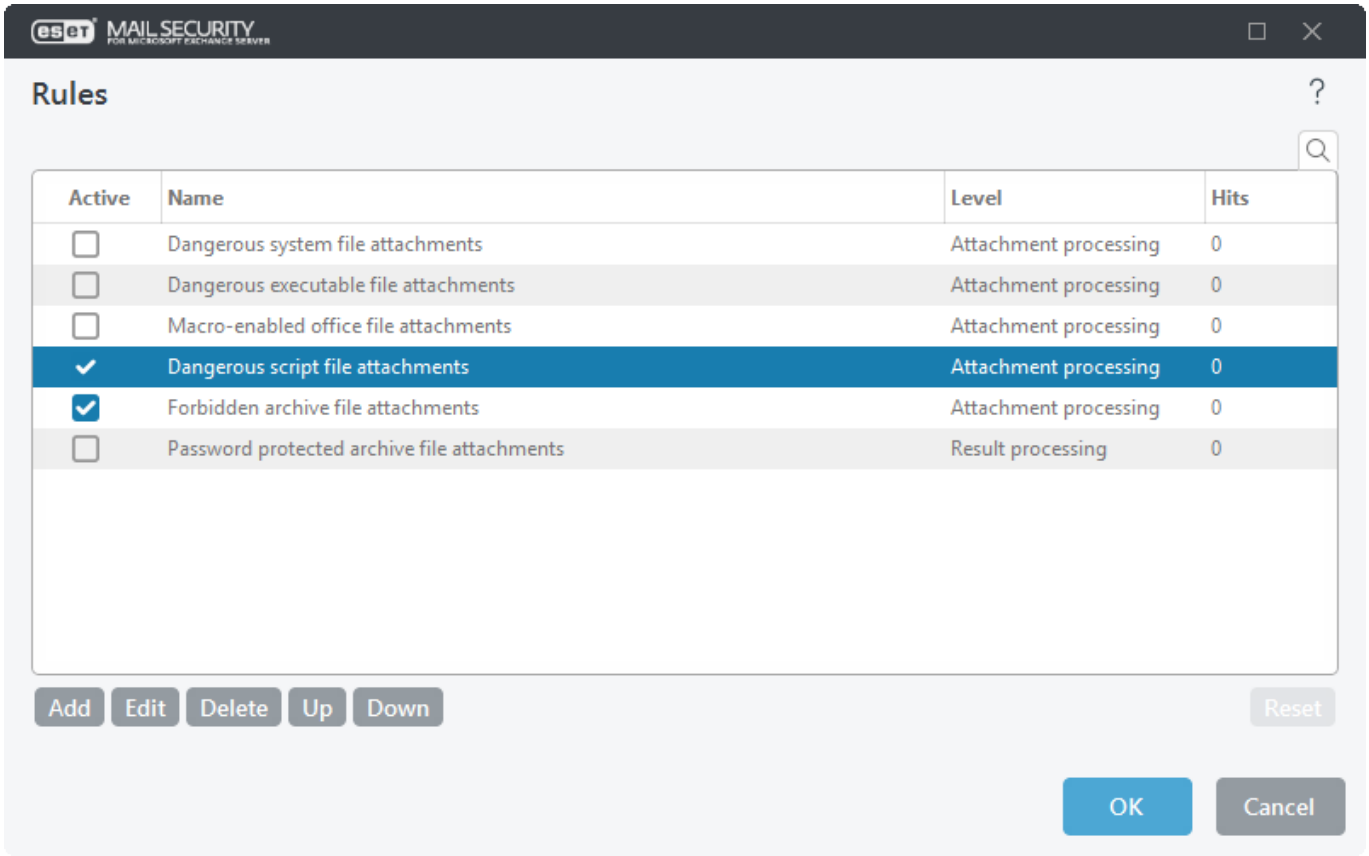
Las reglas incorrectamente definidas para la **Exploración de la base de datos de buzón de correo a petición** pueden causar cambios irreversibles en las bases de datos de buzones. Asegúrese siempre de tener la copia de seguridad más reciente de las bases de datos de su buzón de correo antes de ejecutar la exploración de base de datos del buzón de correo a petición con las reglas vigentes por primera vez. Le recomendamos encarecidamente que verifique que las reglas se ejecuten de acuerdo con sus expectativas. Para la verificación, defina reglas solo con la acción **Registrar en eventos** porque cualquier otra acción puede realizar cambios en sus bases de datos de buzones. Cuando esté satisfecho con la comprobación, podrá agregar acciones de reglas destructivas, como **Quitar archivo adjunto**.

Las reglas se clasifican en tres niveles y se evalúan en este orden:

- **Reglas de filtrado** (1): se evalúa antes de la exploración de antispam, antivirus y Anti-Phishing
- **Reglas de procesamiento de datos adjuntos** (2): se evalúa durante una exploración antivirus
- **Reglas de procesamiento de resultados** (3): se evalúa después de la exploración de antispam, antivirus y Anti-Phishing

Las reglas con el mismo nivel de evaluación se revisan en el orden que se muestra en la ventana de reglas. Solo puede cambiar el orden de las reglas del mismo nivel. Cuando tiene múltiples reglas de filtrado, puede cambiar el orden en el cual se aplican. No puede cambiar su orden al colocar reglas de **Procesamiento de adjuntos** antes de las reglas de **Filtrado**, los botones **Arriba**/**Abajo** no estarán disponibles. No puede mezclar las reglas de distintos **Niveles**.

La columna **Aciertos** muestra la cantidad de veces que se aplicó con éxito la regla. Al anular la selección de una casilla de verificación (a la izquierda de cada nombre de regla) desactiva la regla correspondiente hasta seleccionar otra vez la casilla de verificación.



Haga clic en **Restablecer** el contador para la regla seleccionada (la columna **Coincidencias**). Seleccione **Vista** para ver una configuración asignada desde la política ESET PROTECT.

> Normalmente, si se cumplen las condiciones de una regla, se detiene la evaluación de reglas para aplicar otras reglas con menor prioridad. Sin embargo, si es necesario, puede usar una Acción de regla especial denominada **Evaluar otras reglas** para permitir que continúe la evaluación.

Las reglas se verifican con respecto a un mensaje cuando se procesan mediante la Protección de transporte de correo, Protección de base de datos de buzón o Exploración de la base de datos del buzón de correo a petición. Cada capa de protección tiene un conjunto de reglas independiente.

Cuando las condiciones de las reglas de la Protección de la base de datos del buzón de correo electrónico o la Exploración de la base de datos del buzón de correo a petición coinciden, el contador de la regla puede incrementarse en dos o más puntos. Esto se debe a que estas capas de protección acceden al cuerpo y a los archivos adjuntos de un mensaje por separado, por lo que las reglas se aplican a cada parte de manera individual. Las reglas de la Protección de la base de datos del buzón de correo electrónico también se aplican durante la exploración del entorno (por ejemplo, cuando ESET Mail Security realiza una exploración del buzón de correo después de descargar un nuevo motor de detección), lo que puede aumentar el contador de la regla (coincidencias).

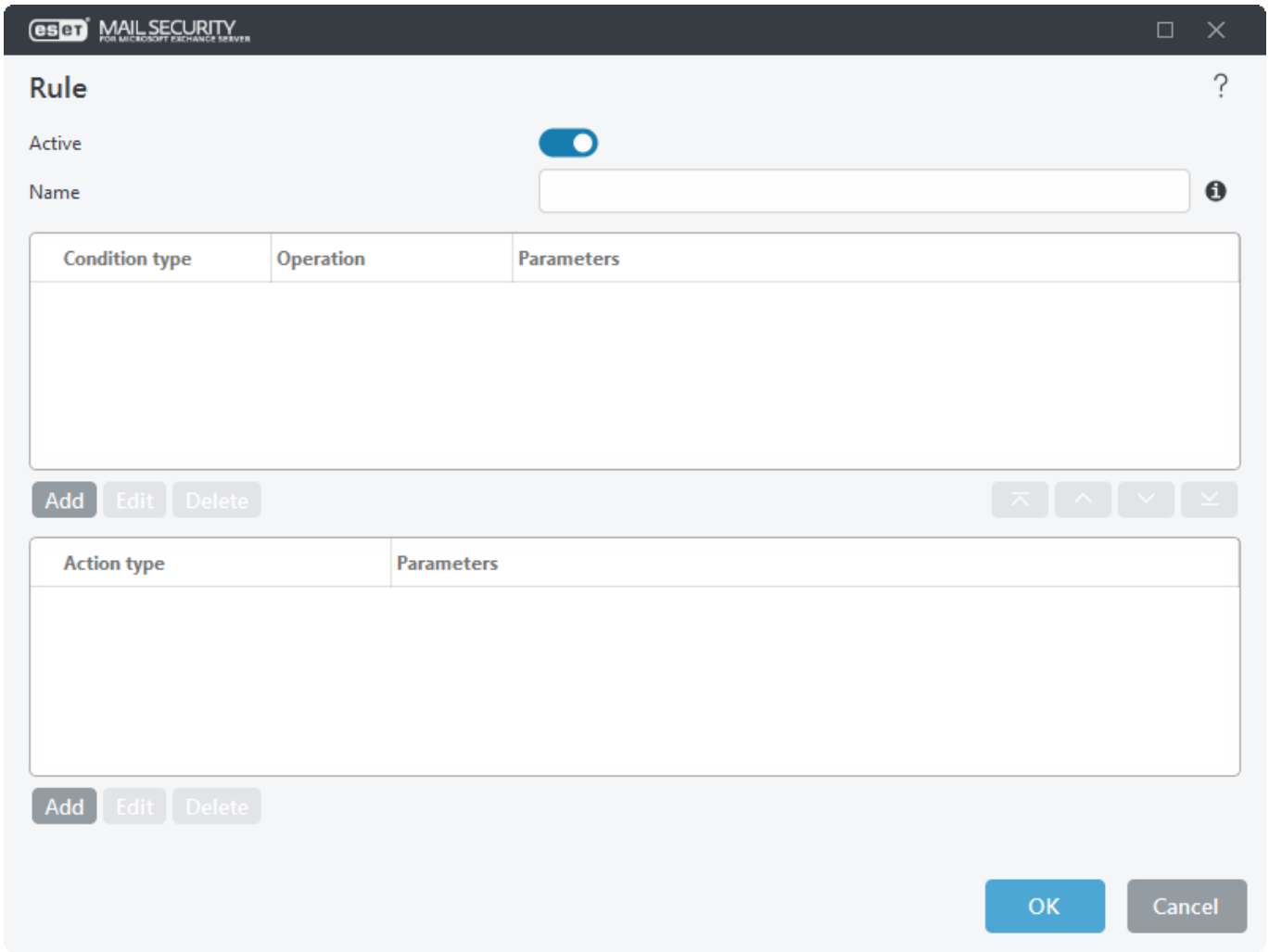
Asistente de reglas

1. Haga clic en **Añadir** (en el medio) y aparecerá una ventana de Condición de regla donde podrá seleccionar el tipo de condición, la operación y el valor. Defina primero las Condiciones, luego las Acciones.

Puedes definir múltiples condiciones. Si lo hace, se deben cumplir todas las condiciones para que se aplique la regla. Todas las condiciones se conectan mediante el operador lógico **AND** [Y]. Incluso si se cumple con la mayoría de las condiciones y solo uno no la cumple, el resultado de la evaluación de condiciones se considera *no cumplido* y no se puede adoptar la acción de la regla.

2. Haga clic en **Añadir** (en la parte inferior) para agregar una Acción de regla.

Puede agregar varias acciones para una misma regla.



3. Una vez que se definen las condiciones y las acciones, ingrese un **Nombre** para la regla (algo que le permita reconocer a la regla). El nombre se mostrará en la lista Reglas. Nombre es un campo obligatorio, si está resaltado en rojo, escriba el nombre de la regla en el cuadro de texto y haga clic en el botón **Aceptar** para crear la regla. El resaltado en rojo no desaparece ni siquiera si ha escrito el nombre de una regla; desaparece al hacer clic en **Aceptar**.

4. Si desea preparar reglas pero planea utilizarlas más tarde, puede hacer clic en el interruptor junto a **Activa** para desactivar la regla. Para activar la regla, seleccione la casilla de verificación junto a la regla que desea activar.

Si se agrega una nueva regla o se modifica una regla existente, se iniciará en forma automática una nueva exploración de los mensajes usando las reglas nuevas o modificadas.

Consulte Ejemplos de reglas para ver cómo puede usarlas.

Condición de regla

El asistente de condición de reglas le permite añadir condiciones para una regla. Seleccione el **Tipo** de condición y una **Operación** del menú desplegable. La lista de operaciones cambia en función del tipo de regla que seleccione. Y luego seleccione un **Parámetro**. Los campos del Parámetro cambiarán según el tipo de regla y la operación.

Por ejemplo, elija **El tamaño del adjunto** > **es mayor a** y en **Parámetro** especifique **10 MB**. Al usar estas configuraciones, cualquier archivo mayor que 10 MB será procesado mediante las acciones de regla que haya especificado. Por este motivo debe especificar la acción que se tomará cuando se active una regla determinada, si aún no lo hizo cuando configuró los parámetros para esa regla.

Si quiere importar su lista personalizada desde un archivo en lugar de agregar cada entrada de forma manual, haga clic con el botón secundario en la mitad de la ventana y seleccione **Importar** desde el menú contextual. A continuación, puede buscar el archivo (*.xml* o *.txt*, y con entradas delimitadas por nuevas líneas) que desea agregar a la lista. Asimismo, si necesita exportar su lista actual a un archivo, seleccione **Exportar** desde el menú contextual.

Alternativamente, puede especificar **Expresión regular**, seleccionar **Operación: coincide con una expresión regular** o **no coincide con una expresión regular**.

ESET Mail Security utiliza std::regex. Consulte la sintaxis de ECMAScript para construir expresiones regulares La sintaxis de expresión regular no distingue entre mayúsculas y minúsculas, incluidos los resultados de búsqueda.

Puedes definir múltiples condiciones. Si lo hace, deben cumplirse todas las condiciones para aplicar la regla. Todas las condiciones se conectan mediante el operador lógico **AND** [Y]. Incluso si se cumple con la mayoría de las condiciones, y solo una no se cumple, el resultado de la evaluación de condiciones se considera *no cumplido*, y no se puede ejecutar la acción de la regla.

Los siguientes tipos de condición están disponibles para la Protección de transporte de correo electrónico, Protección de la base de datos del buzón de correo electrónico y Exploración de la base de datos del buzón de correo a petición (no se mostrarán algunas de las opciones según las condiciones seleccionadas anteriormente):

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Asunto	✓	✓	✓	Se aplica a los mensajes que contengan o no una cadena específica (o una expresión regular) en el asunto.
Remitente	✓	✓	✓	Se aplica a los mensajes enviados por un remitente específico.
Remitente del sobre (remitente SMTP)	✓	⍰	⍰	MAIL FROM atributo envelope usado durante la conexión SMTP, también usado para la verificación SPF.
Dirección IP del remitente	✓	⍰	⍰	Se aplica a los mensajes enviados desde una dirección IP específica.

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Dominio del remitente del sobre/Dominio del remitente	✓	✓	✓	Se aplica a los mensajes de un remitente con un dominio específico en la dirección de correo electrónico.
Dominio del remitente SMTP	✓	⍰	⍰	Se aplica a los mensajes de un remitente con un dominio específico en la dirección de correo electrónico.
Desde encabezado - dirección	✓	⍰	⍰	"From:" valor contenido en los encabezados del mensaje. Esta es la dirección visible para el destinatario, pero no se hace ninguna comprobación que el sistema de envío esté autorizado a enviar mensajes en nombre de esa dirección. Se usa a menudo para engañar al remitente.
Desde encabezado - mostrar nombre	✓	⍰	⍰	"From:" valor contenido en los encabezados del mensaje. Esta es el nombre visible para el destinatario, pero no se hace ninguna comprobación que el sistema de envío esté autorizado a enviar mensajes en nombre de esa dirección. Se usa a menudo para engañar al remitente.
Destinatario	✓	✓	✓	Se aplica a los mensajes enviados a un destinatario específico.
Unidades organizativas del destinatario	✓	⍰	⍰	Se aplica a los mensajes enviados a un destinatario de una unidad organizativa específica.
Resultado de validación del destinatario	✓	⍰	⍰	Se aplica a los mensaje enviados a un destinatario validado en Active Directory.
Nombre del archivo adjunto	✓	✓	✓	Se aplica a los mensajes que contienen datos adjuntos con un nombre específico. Esto incluye los archivos incluidos en un archivo. **Evaluar solo para datos adjuntos de nivel superior**: cuando está activo, no se evaluarán los archivos dentro de un archivo. **Usar ruta completa para objetos dentro de datos adjuntos**: cuando está activo, se evaluará la ruta completa del objeto, no solo el nombre de archivo.
Tamaño de los datos adjuntos	✓	✓	✓	Se aplica a los mensajes que tengan datos adjuntos que no cumplan con un tamaño específico, que se encuentren dentro de un rango de tamaño específico o que superen un tamaño específico.

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Tipo de datos adjuntos	✓	✓	✓	Se aplica a los mensajes que tienen un tipo de archivo específico adjunto. Los tipos de archivo se clasifican en grupos para facilitar la selección. Puede seleccionar varios tipos de archivos o categorías completas. ESET Mail Security detecta el tipo de archivo real sin importar la extensión. Lo mismo se aplica al contenido de un archivo. **Evaluar solo para datos adjuntos de nivel superior**: cuando está activo, no se evaluarán los archivos dentro de un archivo. La condición de regla de **tipo de datos adjuntos** tiene una limitación conocida en la que el motor de detección ESET Mail Security no puede detectar archivos de texto extra pequeños de menos de 10 bytes de longitud en la codificación ASCII/ANSI.
Tamaño del mensaje	✓	⍰	⍰	Se aplica a los mensajes que tengan datos adjuntos que no cumplan con un tamaño específico, que se encuentren dentro de un rango de tamaño específico o que superen un tamaño específico.
Buzón de correo	⍰	✓	⍰	Se aplica a los mensajes ubicados en un buzón de correo específico.
Encabezados del mensaje	✓	✓	⍰	Se aplica a los mensajes que tienen datos específicos presentes en el encabezado del mensaje.
Cuerpo del mensaje	✓	⍰	✓	Se busca la frase específica en el cuerpo del mensaje. Puede usar la característica de etiquetas Strip HTML para quitar las etiquetas, los atributos y los valores de HTML, y conservar el texto solamente. Luego, se buscará en el cuerpo del texto.
Mensaje interno	✓	⍰	⍰	Se aplica según si el mensaje es interno o externo.
Mensaje saliente	✓	⍰	⍰	Se aplica a mensajes salientes.
Mensaje firmado	✓	⍰	⍰	Se aplica a mensajes firmados.
Mensaje cifrado	✓	⍰	⍰	Se aplica a mensajes encriptados.
Resultado de la exploración antispam	✓	⍰	⍰	Se aplica a los mensajes marcados como Ham o Spam.
Resultado de la exploración antivirus	✓	✓	✓	Se aplica a los mensajes marcados como malintencionados o no.
Resultado de la exploración anti-phishing	✓	⍰	✓	Se aplica a los mensajes que se evaluaron como phishing.
Tiempo de recepción	✓	✓	✓	Se aplica a los mensajes recibidos antes o después de una fecha específica o durante un rango de fechas específico.

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Contiene un archivo protegido por contraseña	✓	✓	⍰	Se aplica a los mensajes con datos adjuntos que están protegidos por contraseña.
Contiene un archivo dañado	✓	✓	⍰	Se aplica a los mensajes con archivos adjuntos dañados (lo más probable es que no se puedan abrir).
El adjunto es un archivo protegido con contraseña	⍰	⍰	✓	Se aplica a los datos adjuntos protegidos con contraseña.
El adjunto es un archivo dañado	⍰	⍰	✓	Se aplica a adjuntos que están dañados (la mayoría son imposibles de abrir).
Nombre de la carpeta	⍰	⍰	✓	Se aplica a los mensajes ubicados en un buzón de correo específico. Si la carpeta no existe, se creará. No aplica a carpetas públicas.
DKIM resultado	✓	⍰	⍰	Se aplica a los mensajes que aprobaron o no aprobaron la verificación de DKIM , de manera alternativa si no está disponible.
SPF resultado	✓	⍰	⍰	Se aplica a los mensajes que indican que el resultado de la evaluación de SPF es: • **Aprobado**: la dirección IP se encuentra autorizada para enviar desde el dominio (calificador SPF "+") • **Reprobado**: el registro SPF no contiene el servidor de envío o la dirección IP (calificador SPF "-") • **Falla de software**: la dirección IP puede estar autorizada o no para enviar desde el dominio (calificador SPF "~") • **Neutro**: significa que el propietario del dominio indicó en el registro SPF que no quiere que la dirección IP esté autorizada para enviar desde el dominio (calificador SPF "?") • **No disponible**: el resultado de SPF de None significa que el dominio no publicó registros o que no pudo determinarse ningún remitente verificable para la identidad específica. Lea RFC 4408 para obtener más información sobre SPF. Si usa el resultado de SPF, las listas blancas en Filtro y verificación no se tomarán en cuenta para las reglas.
DMARC resultado	✓	⍰	⍰	Se aplica a los mensajes que aprobaron o reprobaron la verificación de SPF, DKIM o ambas, de manera alternativa si no está disponible.
Permite anular registro DNS	✓	⍰	⍰	Se aplica a los mensajes con el dominio del remitente que tienen registro inverso DNS.

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
NDR resultado	✓	⍰	⍰	Se aplica a los mensajes que reprobaron la verificación de NDR.
resultado de SPF: encabezado De	✓	⍰	⍰	Se aplica a los mensajes que indican que el resultado de la evaluación de SPF es: • **Aprobado**: la dirección IP se encuentra autorizada para enviar desde el dominio (calificador SPF "+") • **Reprobado**: el registro SPF no contiene el servidor de envío o la dirección IP (calificador SPF "-") • **Falla de software**: la dirección IP puede estar autorizada o no para enviar desde el dominio (calificador SPF "~") • **Neutro**: significa que el propietario del dominio indicó en el registro SPF que no quiere que la dirección IP esté autorizada para enviar desde el dominio (calificador SPF "?") • **No disponible**: el resultado de SPF de None significa que el dominio no publicó registros o que no pudo determinarse ningún remitente verificable para la identidad específica. Lea RFC 4408 para obtener más información sobre SPF. Si utiliza los resultados de SPF, las listas blancas en Filtro y verificación no se tomarán en cuenta para las reglas.
Resultado de la comparación del remitente del sobre y del encabezado From	✓	⍰	⍰	Compara los dominios incluidos en el campo del encabezado de correo electrónico "From:" y el remitente del sobre con las listas de dominios.

Nombre de la condición	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Resultado de SPFHELO	✓	?	?	Se aplica a los mensajes que indican que el resultado de la evaluación de HELO es: • **Aprobado**: la dirección IP se encuentra autorizada para enviar desde el dominio (calificador SPF "+") • **Reprobado**: el registro SPF no contiene el servidor de envío o la dirección IP (calificador SPF "-") • **Falla de software**: la dirección IP puede estar autorizada o no para enviar desde el dominio (calificador SPF "~") • **Neutro**: significa que el propietario del dominio indicó en el registro SPF que no quiere que la dirección IP esté autorizada para enviar desde el dominio (calificador SPF "?") • **No disponible**: el resultado de SPF de None significa que el dominio no publicó registros o que no pudo determinarse ningún remitente verificable para la identidad específic Lea RFC 4408 para obtener más información sobre SPF. Si usa el resultado de SPF, las listas blancas en Filtro y verificación no se tomarán en cuenta para las reglas.

El tipo de condición tiene las siguientes **Operaciones**:

- **Cadena:** es, no es, contiene, no contiene, coincide con, no coincide con, está en, no está en, está en la lista, no está en la lista, coincide con la expresión regular, no coincide con la expresión regular
- **Número:** es menor a, es mayor a, se encuentra entre
- **Texto:** contiene, no contiene, coincide con, no coincide con
- **Fecha-Hora:** es menor a, es mayor a, se encuentra entre
- **Enum:** es, no es, está en, no está en

> Si el **Nombre del archivo adjunto** o **Tipo de datos adjuntos** es un archivo de Microsoft Office será tratado por ESET Mail Security como un archivo. Esto significa que se extrae su contenido y cada archivo contenido en el archivo de archivo de Office (por ejemplo, *.docx*, *.xlsx*, *.xltx*, *.pptx*, *.ppsx*, *.potx*, etc.) se analiza por separado.

Si desactiva **Protección antivirus** en el menú Configuración o **Configuración avanzada** (F5) > **Servidor** > **Antivirus y antispyware** en la capa de **Protección del transporte de correo electrónico y de la base de datos del buzón de correo electrónico**, afectará estas reglas condiciones:

- Nombre del archivo adjunto

- Tamaño de los datos adjuntos
- Tipo de datos adjuntos
- Resultado de la exploración antivirus
- El archivo adjunto está protegido por contraseña.
- El adjunto es un archivo dañado
- Contiene un archivo dañado
- Contiene un archivo protegido por contraseña

Acción de regla

Puede agregar acciones para mensajes y/o datos adjuntos que coincidan con las condiciones de la regla.

> ℹ Puede agregar varias acciones para una misma regla.

La lista de Acciones disponibles para la Protección del transporte de correo, Protección de la base de datos del buzón de correo y la Exploración de la base de datos de buzón de correo a petición (es posible que algunas de las opciones no se muestren según las condiciones seleccionadas):

Nombre de la acción	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Mensaje en cuarentena	✓	⍰	⍰	El mensaje no se entregará al destinatario y se moverá a la cuarentena de correo. Los usuarios sin permiso de administrador pueden liberar correos electrónicos puestos en cuarentena por esta regla (usando la interfaz web o informes de cuarentena).
Colocar el archivo adjunto en cuarentena	✓	✓	✓	Pone el archivo adjunto de correo electrónico en la cuarentena de archivos. El correo electrónico se entregará al destinatario con los datos adjuntos truncados a longitud cero.
Eliminar adjunto	✓	✓	✓	Elimina un archivo adjunto de mensaje. El mensaje se entregará al destinatario sin los datos adjuntos.
Rechazar mensaje	✓	⍰	⍰	Elimina el mensaje. El servidor del envío debe generar los correos electrónicos entrante recibidos mediante SMTP o NDR (Non-Delivery Report).
Eliminar el mensaje en silencio	✓	⍰	⍰	Quita un mensaje sin generar un NDR.
Definir el valor SCL	✓	⍰	⍰	Cambia o define un valor SCL específico.

Nombre de la acción	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Enviar notificación del evento a un Administrador	✓	✓	✓	Envía notificaciones de Evento a un destinatario específico en las Notificaciones de correo electrónico. Necesita habilitar la característica Enviar notificación de evento por correo electrónico. Entonces puede personalizar el formato de los mensajes de evento (use la información sobre herramientas para obtener las sugerencias) mientras crea la regla. Además, puede seleccionar el nivel de detalle para los mensajes de evento, aunque esto depende de la configuración de nivel de detalle mínima en la sección Notificaciones de correo electrónico.
Enviar notificación por correo electrónico				Envía notificaciones de correo electrónico a un destinatario específico en las Notificaciones de correo electrónico.
Omitir la exploración antispam	✓	?	?	El motor antispam no explorará el mensaje.
Omitir la exploración antivirus	✓	✓	✓	El motor antivirus no explorará el mensaje.
Omitir la exploración Anti-Phishing	✓	?	✓	La protección anti-phishing no analizará el mensaje.
Omitir la exploración ESET LiveGuard Advanced	✓	?	?	La protección ESET LiveGuard Advanced no validará el mensaje.
Evaluar otras reglas	✓	✓	✓	Permite la evaluación de otras reglas, habilita al usuario a definir varios grupos de condiciones y varias acciones a seguir, según las condiciones.

Nombre de la acción	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Registrar eventos	✓	✓	✓	Escribe la información acerca de la regla aplicada al registro de programa y define el formato de los mensajes de evento (use información sobre herramientas para obtener más sugerencias). Si configura el tipo de acción Eventos de registro para la protección de la base de datos del buzón de correo con el parámetro %IPAddress%, la columna Evento en los archivos de registro estará vacía para este evento particular. Esto se debe a que no hay dirección de IP en el nivel de protección de la base de datos del buzón de correo. Algunas opciones no están disponibles en todos los niveles de protección: %IPAddress%: ignorada por la exploración de base de datos del buzón de correo a petición y protección de base de datos del buzón de correo %Mailbox%: ignorado por la Protección del transporte de correo electrónico Las siguientes opciones aplican únicamente a las Reglas de procesamiento de datos adjuntos: %Attname% : ignorado por las Reglas de filtrado y Reglas de procesamiento de resultados %Attsize% : ignorado por las Reglas de filtrado y Reglas de procesamiento de resultados
Agregar campo de encabezado	✓	⍰	⍰	Agrega una cadena personalizada al encabezado del mensaje.
Añadir el prefijo del asunto	✓	⍰	⍰	Agrega un prefijo a un asunto.
Reemplazar adjunto con información sobre la acción	⍰	✓	✓	Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada.
Eliminar campos de encabezado	✓	⍰	⍰	Elimina campos del encabezado del mensaje según los parámetros específicos.
Eliminar mensaje	⍰	✓	✓	Elimina el mensaje infectado.
Mover mensaje a carpeta	⍰	⍰	✓	El mensaje se moverá a la carpeta específica.
Mover el mensaje a la papelera	⍰	⍰	✓	Coloca un mensaje de correo electrónico en la papelera en el lado del cliente de correo electrónico.

Nombre de la acción	Protección del transporte de correo electrónico	Protección de la base de datos de correo electrónico	Exploración de la base de datos del buzón de correo a petición	Descripción
Aplicar la política de DMARC	✓	?	?	Si se cumple con la condición del resultado DMARC, el mensaje de correo electrónico se gestiona según la política especificada en el registro DMARC DNS del dominio del remitente.

Si desactiva la opción **Protección antivirus** en el menú Configuración o **Configuración avanzada** (F5) > **Servidor** > **Antivirus y antispyware** en la **protección de transporte de correo electrónico**, afectará estas acciones de reglas.

- Colocar el archivo adjunto en cuarentena
- Eliminar adjunto

Ejemplos de reglas

Poner en cuarentena los mensajes que contienen Malware o datos adjuntos protegidos por contraseña, dañados o encriptados

Objetivo: Poner en cuarentena los mensajes que contienen Malware o datos adjuntos protegidos por contraseña, dañados o encriptados
Crear la siguiente regla para la **Protección del transporte de correo electrónico**:
Condición
- Tipo: Resultado de la exploración antivirus
- Operación: no es
- Parámetro: Limpiar

Acción
Tipo: Mensaje en cuarentena

Mover mensajes que fallaron la comprobación de SPF a una carpeta de correo no deseado

Objetivo: Mover mensajes que fallaron la comprobación de SPF a una carpeta de correo no deseado
Crear la siguiente regla para la **Protección del transporte de correo electrónico**:
Condición
- Tipo: Resultado de SPF
- Operación: es
- Parámetro: Error

Acción
- Tipo: Establecer el valor SCL
- Valor: 5

Establezca el valor de acuerdo al parámetro `SCLJunkThreshold` de `Get-OrganizationConfig` cmdlet de su servidor de Exchange. Para obtener más detalles, vea el artículo de Acciones de umbral de SCL.

Verificar mensaje de correo electrónico sospechoso de suplantación de remitente

Objetivo: Compruebe los mensajes de correo electrónico sospechosos de suplantación de remitente. Si el mensaje contiene su propio dominio en el encabezado de correo electrónico «Desde» o en el remitente del sobre, verifiquelo posteriormente con el resultado de SPF. Si el resultado de SPF es un mensaje neutro y en cuarentena, registre en eventos y notifique al administrador.

Condición

- Tipo: Resultado de la comparación del remitente del sobre y del encabezado From
- Operación: es
- Parámetro: Coincidencia
- Tipo: resultado de SPF: encabezado De
- Operación: es
- Parámetro: Neutro

Acción

Tipo: Poner mensaje en cuarentena, Registrar en eventos y Enviar notificación del evento al administrador

Eliminar mensajes de remitentes específicos

Objetivo: Eliminar mensajes de remitentes específicos

Crear la siguiente regla para la **Protección del transporte de correo electrónico**:

Condición

- Tipo: Remitente
- Operación: es / es uno de
- Parámetro: spammer1@domain.com, spammer2@domain.com

Acción

Tipo: **Eliminar el mensaje en silencio**

Lista de IP bloqueada

Objetivo: Mensaje de cuarentena desde una dirección IP en la lista de IP bloqueadas, notifique al administrador y registre el evento.

Detalles: Si llega un mensaje de correo electrónico desde una dirección IP de la lista de IP bloqueadas, <%PM%> pondrá en cuarentena el mensaje y se lo notificará por correo electrónico. A continuación, puede liberar el mensaje de la cuarentena o eliminarlo permanentemente. De lo contrario, <%PM%> omitiría el mensaje sin opción de realizar una acción.

Abrir **Protección del transporte de correo electrónico**

Condición

- Tipo: Dirección IP del remitente
- Operación: Está en la lista
- Lista: Lista de IP bloqueada

Acción

Tipo: Poner mensaje en cuarentena, Registrar en eventos y Enviar notificación del evento al administrador

Personalizar regla predefinida

Objetivo: Personalizar regla predefinida

Detalles: Permitir archivos adjuntos adjuntos en mensajes de direcciones IP especificadas (en el caso de sistemas internos, por ejemplo) al utilizar la regla de archivos adjuntos de archivo prohibidos

Abra el conjunto de reglas de la **Protección de transporte de correo**, seleccione **Archivos adjuntos prohibidos** u haga clic en **Editar**.

Condición

- Tipo: Dirección IP del remitente
- Operación: no es / no es ninguno
- Parámetro: 1.1.1.2, 1.1.1.50-1.1.1.99

Cuerpo del mensaje

Objetivo: Poner en cuarentena los mensajes que contienen ciertas líneas en el cuerpo del mensaje
Crear la siguiente regla para la **Protección del transporte de correo electrónico**:
Condición
- Tipo: Cuerpo del mensaje
- Operación: contiene / contiene uno de, haga clic en **Agregar** escriba la URL del sitio o parte de una URL

Acción
Tipo: Mensaje en cuarentena

Almacenar mensajes de receptores inexistentes

Objetivo: Almacenar mensajes de receptores inexistentes
Detalles: Si desea tener todos los mensajes en destinatarios inexistentes en cuarentena (independientemente de que estén marcados por la protección Antivirus o Antispam)
Condición
- Tipo: Resultado de validación del destinatario
- Operación: es
- Parámetro: Contiene destinatario inválido

Acción
Tipo: Mensaje en cuarentena

Protección del transporte de correo electrónico

Puede configurar acciones para las amenazas detectadas en la capa de transporte para cada módulo ESET Mail Security (Antivirus, Anti-phishing y Antispam) por separado.

Acciones a realizar si no es posible la limpieza:

- **Sin acción**: conservar los mensajes infectados que no pueden desinfectarse
- **Mensaje de cuarentena**: coloque los mensajes infectados en el buzón de cuarentena
- **Eliminar el mensaje**: eliminar el mensaje infectado
- **Abandonar mensaje en silencio:** elimina los mensajes sin enviar NDR (Informe de no entrega)

Si selecciona **Sin acción** y tiene el **Nivel de limpieza** definido como **Sin limpieza** en los parámetros de antivirus y antispyware ThreatSense, entonces el estado de protección cambiará a amarillo. Esto se debe a que es un riesgo de seguridad y no recomendamos que use esta combinación. Cambie alguna de las configuraciones para lograr la mejor protección.

Acción a seguir con un mensaje de phishing:

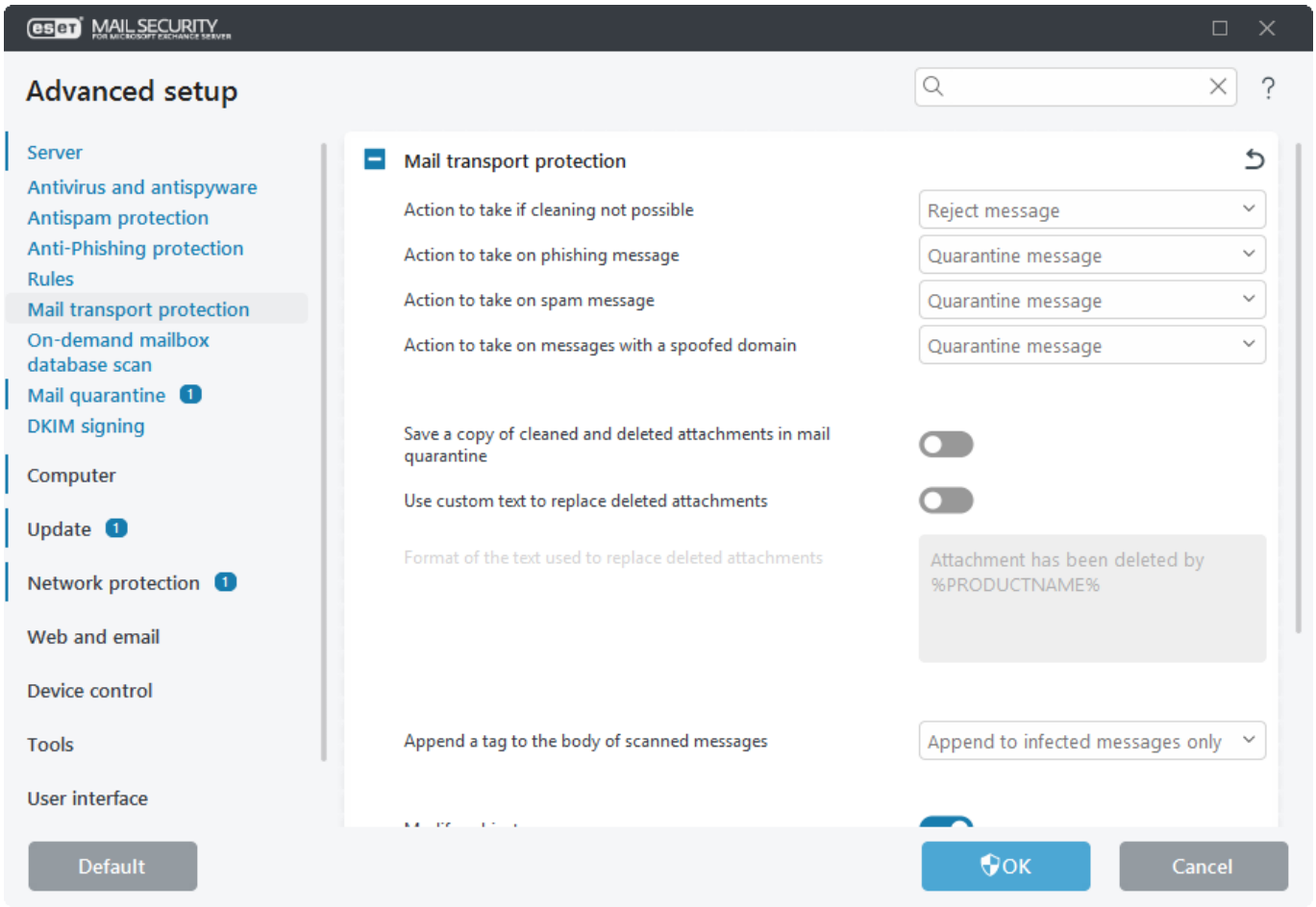
- **Sin acción**: conservar los mensajes
- **Mensaje de cuarentena**: colocar los mensajes marcados como phishing en el buzón de cuarentena
- **Rechazar mensaje**: rechazar los mensajes marcados como phishing
- **Abandonar mensaje en silencio:** elimina los mensajes sin enviar NDR (Informe de no entrega)

Acción a realizar en los mensajes spam:

- **Sin acción**: conservar los mensajes
- **Mensaje de cuarentena**: colocar los mensajes marcados como spam en el buzón de cuarentena
- **Rechazar mensaje**: rechazar los mensajes marcados como spam
- **Abandonar mensaje en silencio:** elimina los mensajes sin enviar NDR (Informe de no entrega)

Acción a realizar en mensajes con un dominio suplantado:

- **Sin acción**: conservar los mensajes
- **Poner el mensaje en cuarentena**: pone los mensajes marcados como suplantados en el buzón de correo de cuarentena
- **Rechazar mensaje**: rechazar los mensajes marcados como suplantados
- **Abandonar mensaje en silencio:** elimina los mensajes sin enviar NDR (Informe de no entrega)



Guardar una copia de los archivos adjuntos limpios y eliminados en la cuarentena de correo electrónico

Una copia del archivo adjunto original se almacenará en la cuarentena de correo.

Utilizar texto personalizado para sustituir los archivos adjuntos eliminados

Cuando esta opción está activada, puede especificar un texto personalizado que sustituya los archivos adjuntos

quitados.

Formato del texto utilizado para sustituir los archivos adjuntos eliminados

Reemplazar el adjunto con un archivo de texto que contiene información detallada sobre una acción tomada. Si ha habilitado la configuración anterior (**Usar texto personalizado**), puede modificar el texto predeterminado con sus detalles personalizados usando variables si lo desea.

Use variables al personalizar el texto que se usará como sustituto de los archivos adjuntos eliminados en un mensaje de correo electrónico.
%PRODUCTNAME%
%FILENAME%
%VIRUSNAME%
%DETECTIONNAME%
%FILESIZE%
%SENDERADDRESS%
%FROMADDRESS%
%DATETIME%
%FILENAME% Ha quitado el archivo adjunto%FILESIZE%, con el tamaño de %PRODUCTNAME%, debido a %DETECTIONNAME%.
El formato de texto personalizado tendrá la siguiente salida visible:
ESET Mail Security Ha quitado el archivo adjunto eicar_com.zip, con el tamaño de 184 B, debido al archivo Eicar test.

Respuesta de rechazo de SMTP

Puede especificar un **Código de respuesta**, un **Código de estado** y un **Mensaje de respuesta**, que defina la respuesta de rechazo temporal del SMTP enviada al servidor del SMTP si se rechaza un mensaje. Puede ingresar un mensaje de respuesta con el siguiente formato:

Código de respuesta	Código de estado	Mensaje de respuesta
250	2.5.0	Se aceptó y completó la acción solicitada para el correo
451	4.5.1	Se anuló la acción solicitada: error local de procesamiento
550	5.5.0	No se ejecutó la acción solicitada: buzón de correo no disponible
554	5.6.0	Contenido no válido

cuando configure las respuestas SMTP de rechazo, también puede utilizar variables del sistema.

Agregar notificación al cuerpo de los mensajes escaneados ofrece tres opciones:

- **No adjuntar a los mensajes**: no se agregará la información.
- **Solo adjuntar a los mensajes infectados**: solo afecta a los mensajes infectados.
- **Adjuntar a todos los mensajes** (no aplica a mensajes internos): se marcarán todos los mensajes.

Modificar asunto

Cuando esté habilitado, puede modificar las plantillas añadidas al asunto de mensajes infectados, spam o phishing.

Plantilla añadida al asunto de los mensajes infectados

ESET Mail Security añadirá una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes infectados** (el texto predeterminado por defecto es `[found threat %VIRUSNAME%]`). Esta modificación puede utilizarse para automatizar el filtrado de mensajes infectados al filtrar correos electrónicos que tengan un asunto específico, por ejemplo, al utilizar las reglas o de manera alternativa del lado del cliente (si el cliente de correo electrónico lo admite) para colocar dichos mensajes de correo electrónico en una carpeta aparte.

Plantilla añadida al asunto de los mensajes spam

ESET Mail Security añadirá una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes spam** (el texto predeterminado por defecto es `[SPAM]`). Esta modificación puede utilizarse para automatizar el filtrado de spam al filtrar correos electrónicos que tengan un asunto específico, por ejemplo, al utilizar las reglas o de manera alternativa del lado del cliente (si el cliente de correo electrónico lo admite) para colocar dichos mensajes de correo electrónico en una carpeta aparte.

Plantilla añadida al asunto de los mensajes de phishing

ESET Mail Security añadirá una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes phish** (el texto predeterminado por defecto es `[PHISH]`). Esta modificación puede utilizarse para automatizar el filtrado de spam al filtrar correos electrónicos que tengan un asunto específico, por ejemplo, al utilizar las reglas o de manera alternativa del lado del cliente (si el cliente de correo electrónico lo admite) para colocar dichos mensajes de correo electrónico en una carpeta aparte.

> i También puede usar las variables del sistema cuando edita texto, que se añadirá al asunto.

Configuración avanzada de transporte de correo

Puede personalizar la configuración de protección del transporte de correo electrónico.

Explorar también los mensajes recibidos de conexiones autenticadas o internas por

Puede seleccionar qué exploración realizar a mensajes desde fuentes autenticadas o servidores locales. Se recomienda explorar estos mensajes ya que esto aumenta la protección, y es necesario si usa el Microsoft SBS POP3 Connector integrado para obtener mensajes de correo electrónico desde servidores POP3 o servicios de correo externos (por ejemplo Gmail.com, Outlook.com, Yahoo.com, gmx.dem, etc.).

Elija un nivel de protección en el menú desplegable. Le recomendamos usar la **protección antivirus** (configuración predeterminada), en especial para las conexiones internas ya que es poco probable que los mensajes de phishing o spam se distribuirán mediante sus servidores locales. Sin embargo, puede aumentar la protección para Microsoft SBS POP3 Connector al seleccionar **Protección Antivirus y anti-phishing** o incluso **Protección antivirus, anti-phishing y antispam**.

> i Esta configuración enciende o apaga la Protección antispam para los usuarios autenticados y las conexiones internas. Los correos electrónicos de conexiones no autenticadas se exploran siempre, incluso si selecciona **No explorar**.

> Los mensajes internos de Outlook dentro de la organización se envían en formato TNEF (Transport Neutral Encapsulation Format). Antispam no admite TNEF. Por lo tanto, los correos electrónicos internos TNEF no se analizarán en busca de spam independientemente de la configuración **aAnalizatambién los mensajes recibidos de lasode conexiones autenticadas o internas por**.

Explorar los mensajes recibidos de conexiones autenticadas o internas por ESET LiveGuard Advanced

Cuando está habilitado, los mensajes recibidos por ESET LiveGuard Advanced de conexiones autenticadas o internas también se analizan. Esta configuración solo está disponible si cumple los requisitos ESET LiveGuard Advanced para obtener la licencia adecuada. La licencia ESET LiveGuard Advanced está administrada por ESET PROTECT, y la activación en sí debe realizarse desde ESET PROTECT usando una política.

Eliminar el encabezado SCL existente antes de la exploración

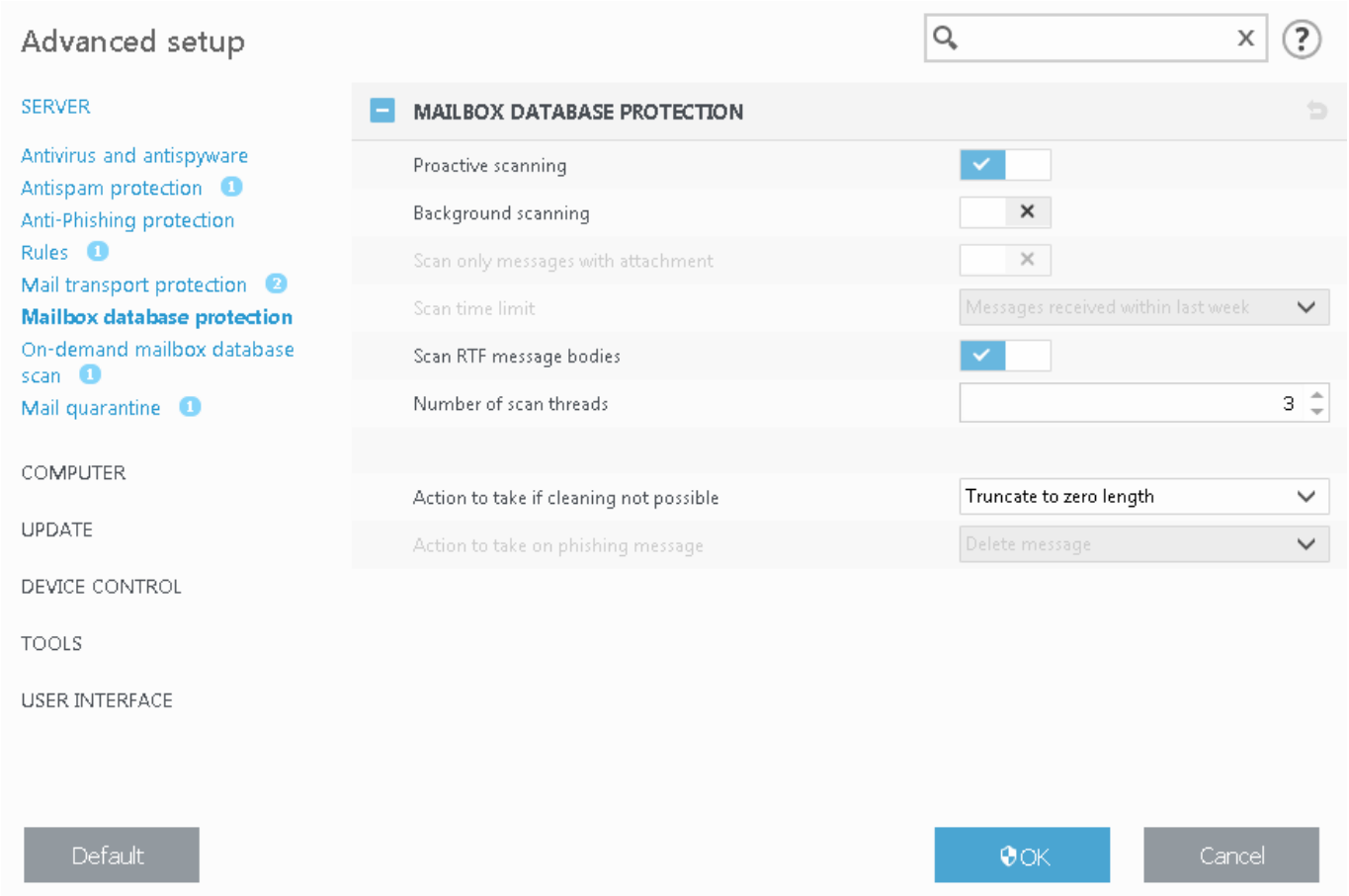
Esta opción está activada de forma predeterminada. Puede deshabilitarlo si se le pide que use el encabezado Nivel de confianza de spam (SCL) .

Escribir los resultados de la exploración en los encabezados de mensajes

Cuando está habilitado, los resultados de una exploración se escriben en los encabezados de los mensajes. Estos encabezados de mensajes comienzan con `X_ESET` lo que facilita reconocerlos (por ejemplo `X_EsetResult` o `X_ESET_Antispam`).

Protección de la base de datos de correo electrónico

Si la opción **Exploración proactiva** está habilitada, los nuevos mensajes entrantes se explorarán en el mismo orden en que fueron recibidos. Cuando esta opción está habilitada y un usuario abre un mensaje aún no explorado, dicho mensaje se explorará antes que los demás mensajes de la cola de espera.



Exploración del entorno

Permite que la exploración de todos los mensajes se ejecute en segundo plano (la exploración se ejecuta en la casilla de correo y la tienda de carpetas públicas, por ejemplo, la base de datos de Exchange). Microsoft Exchange Server decide si una exploración en segundo plano se ejecutará o no basándose en diversos factores, como la carga actual del sistema, la cantidad de usuarios activos, etc. Microsoft Exchange Server lleva un registro de los mensajes explorados y de la versión de la base de datos de firmas de virus utilizada.

Si abre un mensaje que no se exploró con la base de datos de firmas de virus más reciente, Microsoft Exchange Server envía el mensaje a ESET Mail Security para su exploración antes de que lo abra el cliente de correo electrónico. Puede elegir **Explorar solo los mensajes que contienen archivos adjuntos** y filtrarlos según el momento en que se recibieron, mediante las siguientes opciones de Límite de tiempo de la exploración:

- Todos los mensajes
- Mensajes recibidos en el último año
- Mensajes recibidos en los últimos 6 meses
- Mensajes recibidos en los últimos 3 meses
- Mensajes recibidos en el último mes
- Mensajes recibidos en la última semana

Como la exploración en segundo plano puede afectar la carga del sistema (la exploración se realiza en cada motor de detección), se recomienda programar las exploraciones fuera de las horas laborales. La exploración en segundo plano programada se puede configurar mediante la creación de una tarea especial en la sección de Tareas

programadas.

Cuando programa una tarea de exploración en segundo plano, puede especificar la hora de inicio, la cantidad de repeticiones y otros parámetros disponibles en las Tareas programadas. Luego de haber programado la tarea, ésta aparecerá en la lista de tareas programadas y será posible modificar sus parámetros, eliminarlas o desactivarla temporalmente.

Cantidad de subprocesos de exploración

La cantidad de subprocesos de exploración va desde el 1 al 21. Puede configurar la cantidad de subprocesos de análisis independientes que se utilizan a la vez. La mayor cantidad de subprocesos en máquinas de procesadores múltiples puede aumentar la tasa de exploración. Para un mejor rendimiento del programa, le recomendamos usar una cantidad igual de motores de exploración ThreatSense y subprocesos de exploración.

Explorar cuerpos de mensajes RTF

La opción activa la exploración de los cuerpos de mensajes RTF. El cuerpo de los mensajes RTF pueden contener virus de macro.

> i VSAPI no explora el cuerpo de los correos electrónicos cuyo texto no tiene formato.

Acciones a realizar si no es posible la limpieza:

- **Sin acción**: no se aplicarán cambios al mensaje.
- **Truncar el archivo a longitud cero:** el archivo adjunto se acortará a longitud cero.
- **Reemplazar el contenido con información sobre la acción:** el cuerpo original se reemplazará con la información de la acción. El contenido del archivo adjunto se reemplazará con la información de la acción.
- **Eliminar mensaje**: el mensaje se eliminará.

Acción a realizar en el mensaje de suplantación de identidad (phishing):

- **Sin acción**: no se aplicarán cambios al mensaje.
- **Eliminar mensaje**: el mensaje se eliminará.

> i las carpetas públicas se tratan de la misma manera que los buzones de correo. Esto implica que las carpetas públicas también son exploradas.

Exploración en segundo plano

Este tipo de tarea permite la exploración de la base de datos mediante VSAPI en segundo plano. Permite que Exchange Server ejecute una exploración en segundo plano si es necesario. La exploración se inicia el mismo Exchange Server, esto significa que Exchange Server decide si la exploración se ejecutará dentro del tiempo permitido.

Le recomendamos que permita que esta tarea se ejecute fuera de las horas picos cuando Exchange Server no esté ocupado, por ejemplo durante la noche. Esto se debe a que la exploración en segundo plano de la base de datos coloca cierta cantidad de carga en el sistema. Además, el periodo de tiempo no debe entrar en conflicto con cualquier copia de seguridad que pueda estar ejecutándose en Exchange Server para evitar problemas de

rendimiento o disponibilidad.

> La Protección de la base de datos del buzón de correo debe estar habilitada para que se ejecute la tarea del programador. Este tipo de protección solamente está disponible para Microsoft Exchange Server 2010 que funciona en el Servidor del buzón de correo.

Tiempo de espera (en horas)

Especifica cuántas horas tiene permitido Exchange Server para ejecutar la exploración en segundo plano de la base de datos desde la hora en que se ejecuta la tarea programada. Una vez que alcanza el tiempo de espera, se le indicará a Exchange que detenga la exploración en segundo plano.

Exploración de la base de datos del buzón de correo a petición

> Si ejecuta Microsoft Exchange Server 2010 puede elegir entre la Protección de la base de datos de correo electrónico y la **Exploración de la base de datos a petición**. Solamente un tipo de protección puede estar activo a la vez. Si decide usar la **Exploración de la base de datos del buzón de correo a petición** deberá deshabilitar la integración de **la Protección de la base de datos de correo electrónico** en la **Configuración avanzada** (**F5**) del Servidor. De lo contrario, la **Exploración de la base de datos del buzón de correo a petición** no estará disponible.

Dirección del host: nombre o dirección IP del servidor que ejecuta EWS (Exchange Web Services).

Nombre de usuario: especifica las credenciales de un usuario que tiene acceso adecuado a EWS.

Contraseña del usuario: haga clic en **Configurar** junto a la **Contraseña del usuario** e ingrese la contraseña para esta cuenta del usuario.

> Para explorar carpetas públicas, la cuenta del usuario que se usa para explorar la base de datos a petición debe tener un buzón de correo. De lo contrario, se mostrará *Failed to load public folders* en el registro de exploración de base de datos, junto con un mensaje más específico devuelto por Exchange.

Método de acceso al buzón: permite seleccionar el método preferido de acceso al buzón:

- **Suplantación** – La configuración más fácil y más rápida es el **rol ApplicationImpersonation** que se debe asignar a la cuenta de exploración.

Asignar el rol ApplicationImpersonation a un usuario

Si esta opción no está disponible, debe especificar un **nombre de usuario**. Haga clic en **Asignar** para asignar automáticamente el papel de aplicación/personificación al usuario seleccionado. Como alternativa, puede asignar manualmente el papel de aplicación/personificación a una cuenta de usuario. Se crea una nueva Directiva de límites EWS sin límites para la cuenta de usuario. Para obtener más información, consulte Detalles de la cuenta de la exploración de la base de datos.

- **Delegación** – Use este tipo de acceso si requiere derechos de acceso a casillas de correo individuales, pero puede proporcionar velocidades más rápidas al explorar grandes cantidades de datos.

Asignar acceso delegado a un usuario

Si esta opción no está disponible, debe especificar un **nombre de usuario**. Haga clic en **Asignar** para otorgar automáticamente al usuario seleccionado acceso pleno a todos los buzones de correo compartidos y usuarios. Se crea una nueva Directiva de límites EWS sin límites para la cuenta de usuario. Para obtener más información, consulte Detalles de la cuenta de la exploración de la base de datos.

Utilizar SSL

SSL debe estar habilitado si EWS está establecido en Requerir SSL en IIS. Si el SSL está habilitado, se debe importar el certificado de Exchange Server al sistema con ESET Mail Security (en caso de que los roles de Exchange Server estén en servidores diferentes). Las configuraciones para EWS pueden encontrarse en IIS en Sites/Default website/EWS/SSL Settings.

Deshabilite **Usar SSL** solo si tiene EWS configurado en IIS para no Solicitar SSL.

Ignorar el error del certificado del servidor – Si usa un certificado firmado, podrá ignorar el error del certificado del servidor.

Certificado de cliente: solo debe establecerse si EWS requiere un certificado de cliente. Haga clic en **Seleccionar** para seleccionar un certificado.

Acción para realizar cuando no es posible desinfectar: este campo de acción le permite bloquear el contenido infectado.

- **Sin acción**: no realizar ninguna acción con el contenido infectado del mensaje.
- **Mover el mensaje a la papelera**: no se admite para los elementos de la carpeta Pública; en cambio, se aplicará la acción Eliminar objeto.
- **Eliminar objeto**: elimina el contenido infectado del mensaje.
- **Eliminar mensaje**: eliminar el mensaje completo, incluyendo su contenido infectado.
- **Reemplazar objeto por información de acción**: quita un objeto e incluye información sobre el objeto que se quitó.

Acción a realizar en el mensaje de phishing:

- **Sin acción**: conservar el mensaje aunque esté marcado como phishing.
- **Mover el mensaje a la papelera**: no se admite para los elementos de la carpeta Pública; en cambio, se aplicará la acción Eliminar objeto.
- **Eliminar mensaje**: eliminar el mensaje completo, incluyendo su contenido infectado.

Cantidad de subprocesos

Puede especificar cuántas amenazas ESET Mail Security debe usar durante la exploración de base de datos. Cuanto mayor sea la cantidad, mayor será el rendimiento. Sin embargo, un aumento en el rendimiento usa más recursos. Ajuste esta configuración al valor deseado según sus requisitos. El valor predeterminado está establecido en 4 amenazas de escaneo.

Si configura la exploración de la base de datos del buzón de correo a petición para que utilice demasiadas amenazas, puede cargar demasiada información en su sistema, lo que podría hacer que otros procesos sean más lentos o incluso el sistema completo. Puede encontrar un mensaje de error que dice "*Demasiadas conexiones simultáneas abiertas*".

Microsoft 365

Solamente visible si tiene un entorno híbrido de Microsoft 365.

Cuenta de usuario para explorar una carpeta pública

Si desea explorar carpetas públicas, proporcione el nombre de la cuenta de usuario principal (no se necesita contraseña) para la suplantación. Asegúrese de que esta cuenta de usuario esté configurada para tener acceso a todas las carpetas públicas.

Exploración de la base de datos del buzón

Ejecutar una exploración completa de la base de datos de correo electrónico en entornos grandes puede provocar cargas de sistema no deseadas. Para evitar este problema, ejecute un análisis en bases de datos o buzones de correo específicos. Además, minimice el impacto del sistema del servidor mediante el filtrado de los objetivos de explración utilizando las marcas de tiempo del mensaje.

Las reglas incorrectamente definidas para la Exploración de la base de datos de buzón de correo a petición pueden causar cambios irreversibles en las bases de datos de buzones. Asegúrese siempre de tener la copia de seguridad más reciente de las bases de datos de su buzón de correo antes de ejecutar la exploración de la base de datos de buzón de correo a petición con las reglas vigentes por primera vez. Además, le recomendamos que verifique que las reglas se ejecuten de acuerdo con las expectativas.
Para la verificación, defina reglas solo con la acción Registrar en eventos porque cualquier otra acción puede realizar cambios en las bases de datos de su buzón. Una vez verificado, puede agregar acciones de reglas destructivas, como **Eliminar archivo adjunto**.

Los siguientes tipos de elementos se escanean tanto en **Carpetas públicas** como en **Casillas de correo** del usuario:

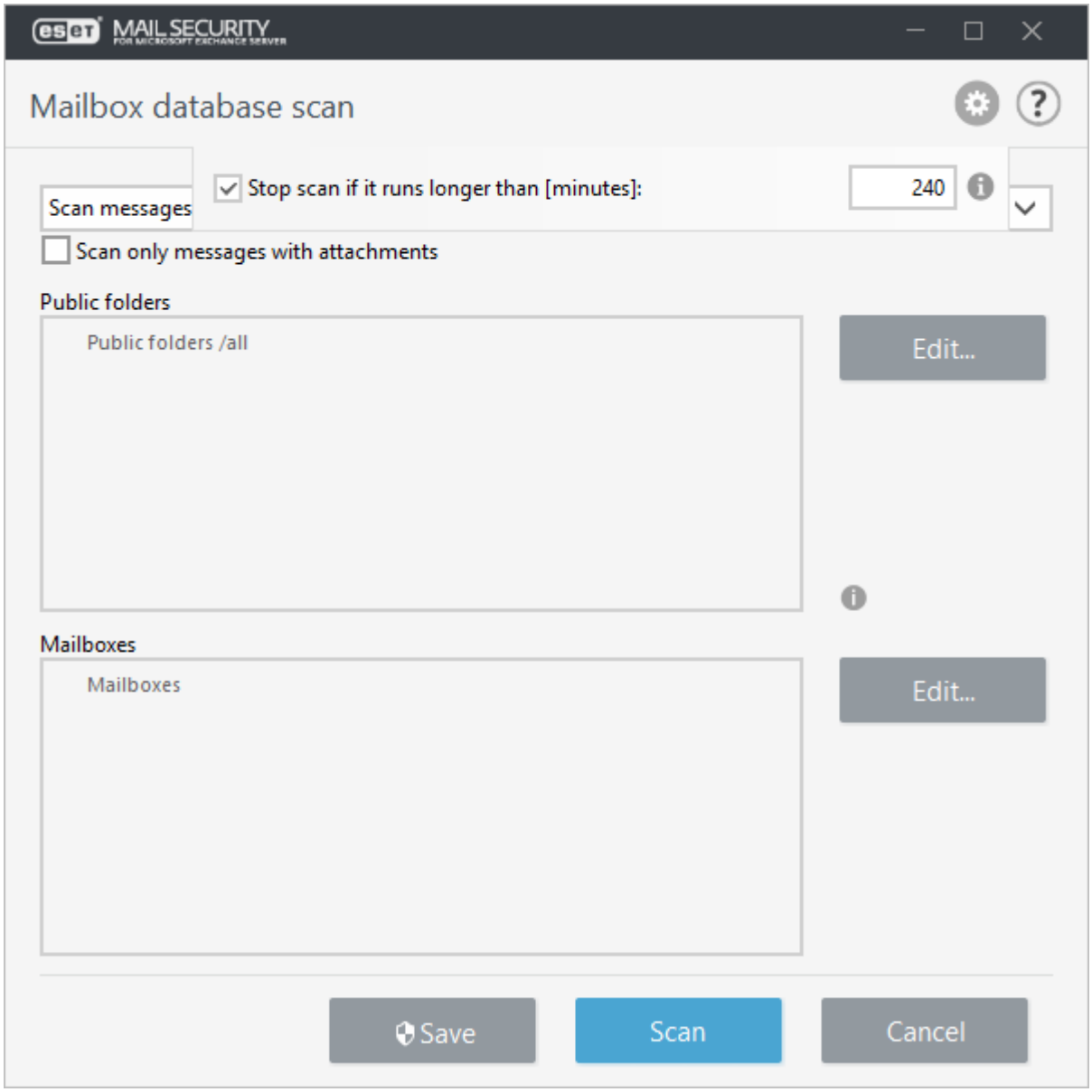
- Correo electrónico
- Publicar
- Elementos del calendario (reuniones/citas)
- Tareas
- Contactos
- Diario

Puede utilizar la lista desplegable para elegir qué mensajes explorar según la marca de tiempo. Por ejemplo, **Explorar mensajes modificados en la última semana**, también puede seleccionar **Explorar todos los mensajes** si es necesario.

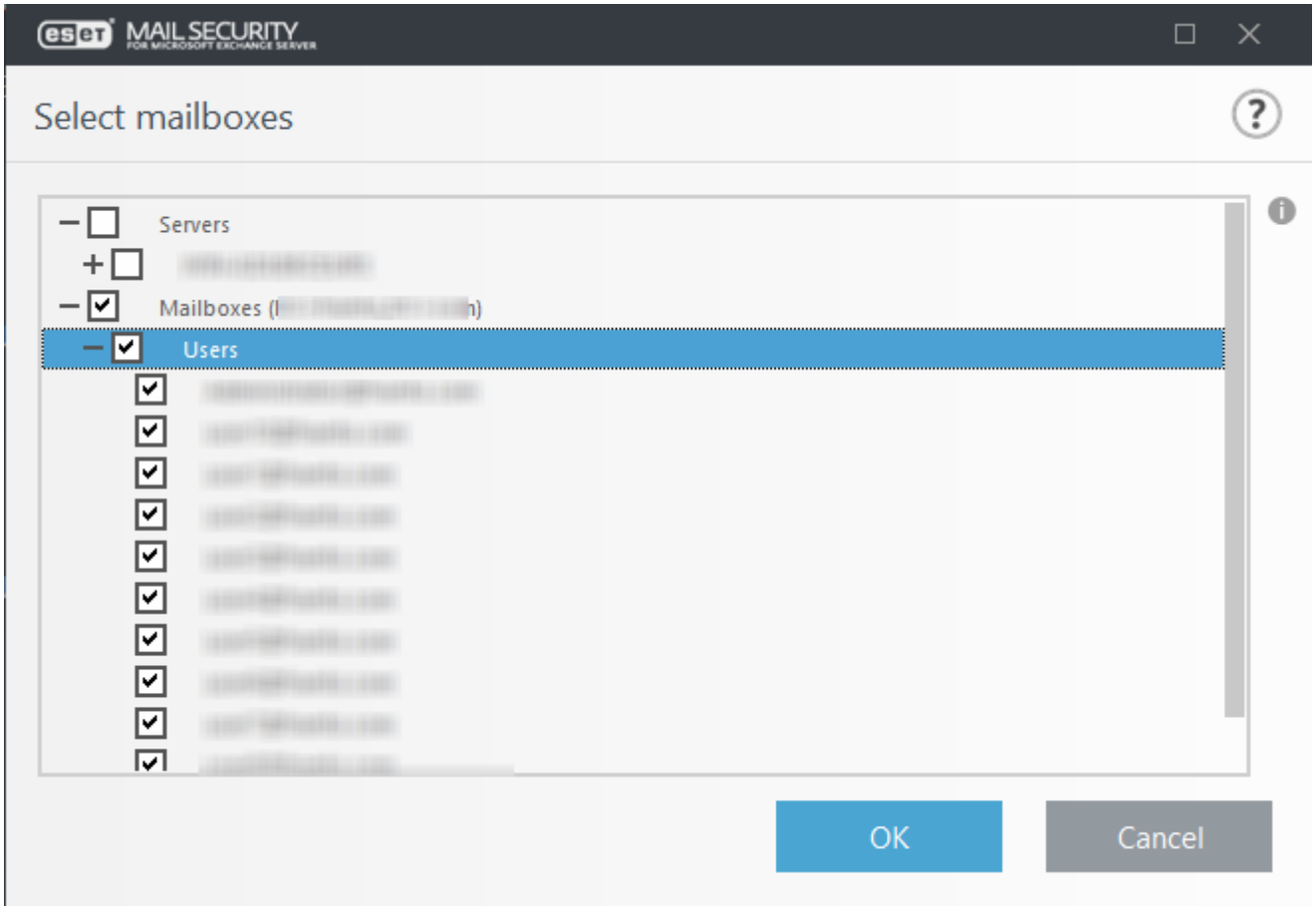
Para habilitar o deshabilitar la exploración del archivo adjunto del mensaje, seleccione la casilla de verificación junto a **Solo explorar mensajes con archivos adjuntos**. Haga clic en **Editar** para seleccionar la carpeta pública que

se explorará.

Haga clic en el ícono y modifique el intervalo para **Detener exploración si su duración es mayor a (minutos)** y cambie al tiempo que prefiera (entre 1 y 2880 minutos).



Seleccione las casillas de verificación junto a las Bases de datos y Casillas de correo del servidor que desee explorar. El Filtro le permite encontrar las Bases de datos y las Casillas de correo rápidamente, en especial si existe una gran cantidad de casillas de correo en su infraestructura de Exchange.



Haga clic en **Guardar** los objetivos de exploración y los parámetros en el perfil de exploración a petición. Ahora puede hacer clic en **Explorar**. En caso de que no haya especificado previamente los Detalles de la cuenta de exploración se abrirá una ventana emergente solicitando credenciales. De lo contrario, se iniciará la Exploración de la base de datos de buzón de correo a petición.

Si no ve el buzón del administrador integrado, compruebe que el atributo *UserPrincipalName* no esté vacío.

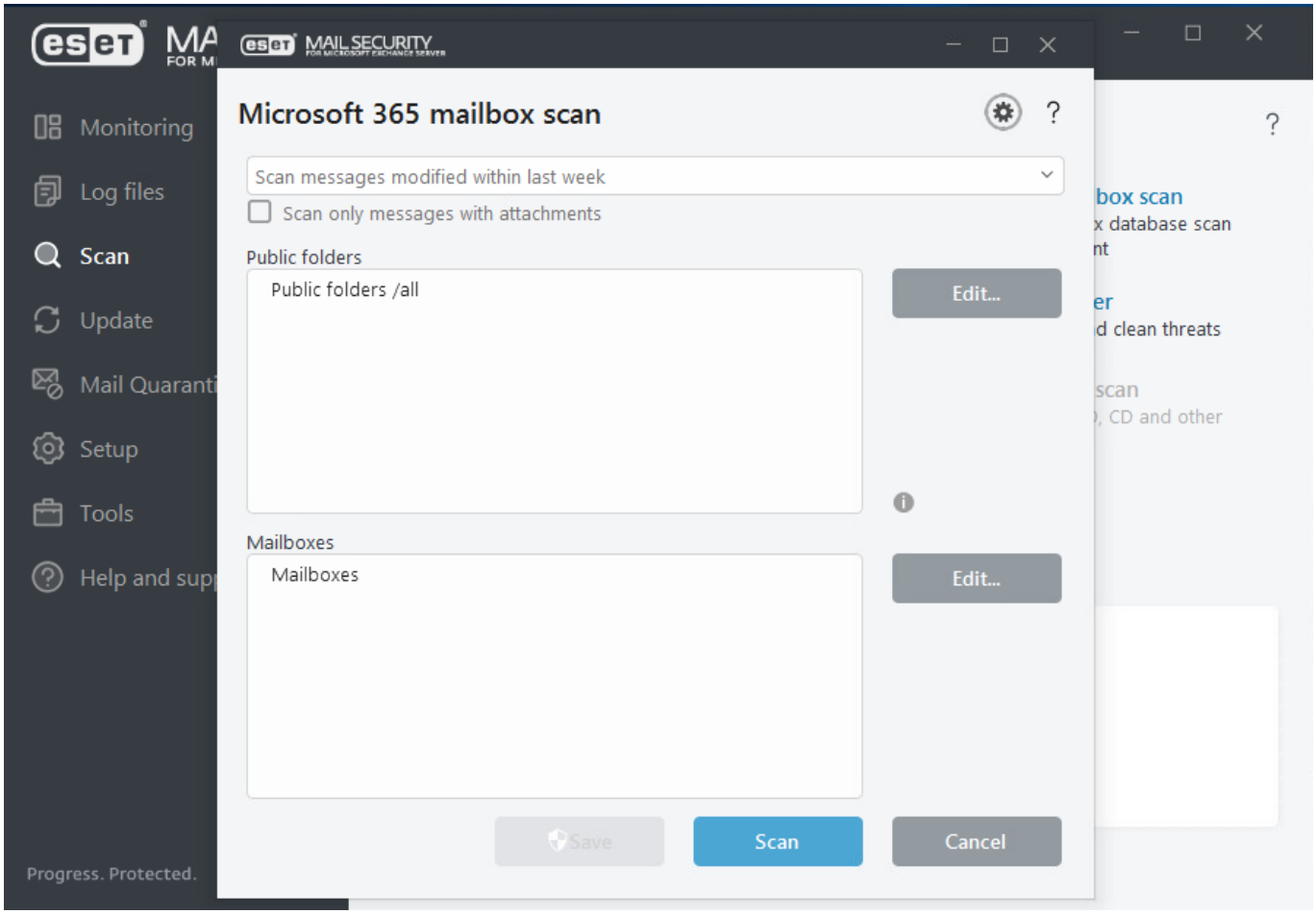
> Si ejecuta Microsoft Exchange Server 2010 puede elegir entre la Protección de la base de datos de correo electrónico y la Exploración de la base de datos del buzón de correo a petición, solo se puede activar un tipo de protección a la vez. Si decide usar la **Exploración de la base de datos del buzón de correo a petición** deberá deshabilitar la integración de **la Protección de la base de datos de correo electrónico** en la **Configuración avanzada del Servidor**. De lo contrario, la Exploración de la base de datos del buzón de correo a petición no estará disponible.

Exploración del buzón de Microsoft 365

ESET Mail Security provee funcionalidad de exploración para ambientes híbridos de Microsoft 365. Está disponible y visible en ESET Mail Security solo si tiene un ambiente híbrido de Exchange (in situ y nube). Ambas posibilidades de enrutamiento son compatibles, a través de **Exchange Online** u organización **in situ**. Para obtener más información, consulte Enrutamiento de transporte en implementaciones híbridas de Exchange.

Para activar esta función, registre el explorador ESET Mail Security.

Puede explorar las casillas de correo electrónico de Microsoft 365 y las carpetas públicas de la misma manera que lo haría con la exploración de la base de datos del buzón de correo electrónico a petición.



Ejecutar una exploración completa de la base de datos de correo electrónico en entornos grandes puede provocar cargas de sistema no deseadas. Para evitar este problema, ejecute un análisis en bases de datos o buzones de correo específicos. Para minimizar aún más el impacto del sistema, debe usar un filtro de tiempo en la parte superior de la ventana. Por ejemplo, en lugar de usar **Explorar todos los mensajes**, puede seleccionar **Explorar los mensajes modificados en la última semana**.

Le recomendamos configurar Microsoft 365. Presione la tecla **F5** y haga clic en **Servidor** > **exploración de base de datos del buzón de correo a petición**. Además, consulte los detalles de la cuenta de exploración de base de datos.

Para ver la actividad de exploración del buzón de correo de Office 365, consulte **Archivos de registro** > **Exploración de base de datos del buzón de correo**.

Elementos adicionales del buzón de correo

Las configuraciones del explorador de la base de datos del buzón de correo a petición le permiten habilitar o deshabilitar la exploración de otros tipos de elementos de la casilla de correo:

- Explorar calendario
- Explorar tareas
- Explorar contactos
- Explorar diario

> Si tiene problemas de rendimiento, puede deshabilitar la exploración de estos elementos. Las exploraciones tardarán más tiempo cuando estos elementos estén habilitados.

Servidor proxy

En caso de que utilice un servidor proxy entre Exchange Server con rol CAS y el Exchange Server donde está instalado ESET Mail Security, especifique los parámetros del servidor proxy. Esto es necesario porque ESET Mail Security se conecta con el API (EWS) mediante HTTP/HTTPS. De lo contrario, la casilla de correo de cuarentena y la cuarentena de Microsoft Exchange no funcionarán.

Servidor proxy

Ingrese la dirección IP o nombre del servidor proxy que desea utilizar.

Puerto

Ingrese el número de puerto del servidor proxy.

Nombre de usuario, Contraseña

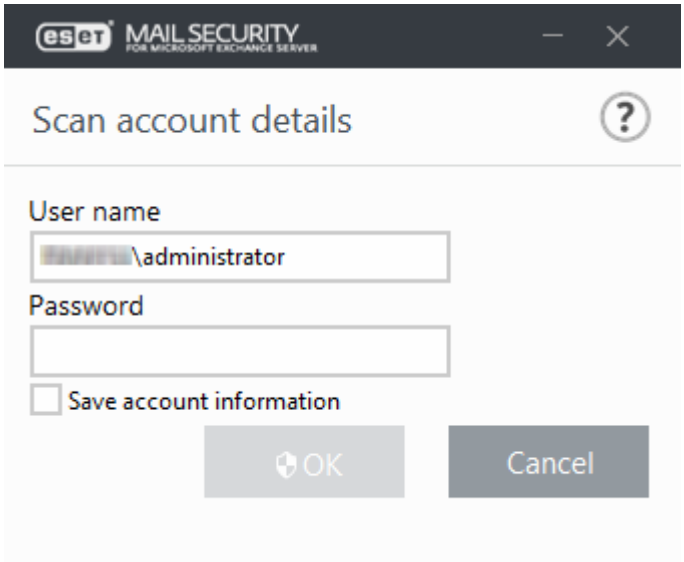
Ingrese las credenciales si su servidor proxy requiere autenticación.

Detalles de la cuenta de la exploración de la base de datos

Este cuadro de diálogo aparece si aún necesita especificar el nombre de usuario y la contraseña para la exploración de base de datos. Especifique las credenciales del usuario que tiene acceso a EWS (Servicios web de Exchange) en esta ventana y haga clic en **Aceptar**. También puede ir a **Configuración avanzada** > **Servidor** > Exploración de base de datos del buzón de correo a petición.

1. Ingrese el **Nombre de usuario**, haga clic en **Configurar**, ingrese la contraseña para esta cuenta de usuario y haga clic en **Aceptar**.

2. Haga clic en la casilla de verificación junto a **Guardar información de la cuenta** para guardar las configuraciones de la cuenta. De lo contrario, se le pedirá que ingrese la información de la cuenta cada vez que ejecute un análisis de la base de datos del buzón de correo a petición.



Si una cuenta de usuario no tiene el acceso adecuado a Exchange Web Services (EWS), puede seleccionar **Crear asignación de rol "Suplantación de aplicación"** para asignar este rol a la cuenta de usuario. Como alternativa, puede asignar manualmente el papel de **aplicación/personificación**.

> La cuenta de exploración debe tener el rol **Suplantación de aplicación** asignado para que el motor de exploración explore los buzones de correo de los usuarios dentro de las bases de datos de buzones de correo de Exchange. Si se ejecuta Exchange Server 2010 o superior, se crea una nueva Directiva de límites EWS sin límites para la cuenta de usuario.
> Asegúrese de configurar la Directiva de límite EWS para la cuenta de exploración y evitar varias solicitudes de operación de ESET Mail Security, que de otra manera podrían causar la expiración de las solicitudes. Consulte los artículos Procedimientos recomendados de EWS y Comprensión de las directivas de límite de cliente para obtener más información acerca de las Directivas de límite. Además, consulte el artículo Cambiar la configuración de límite de usuario para usuarios específicos para obtener más detalles y ejemplos.

Si desea asignar manualmente el **rol de Suplantación de aplicación** a una cuenta de usuario y crear una nueva Directiva de límite EWS para esta cuenta, puede usar los siguientes comandos (reemplazar `ESET-user` con un nombre de cuenta real en el sistema, también puede ajustar los límites para la directiva de límite EWS mediante el reemplazo de `$null` con números):

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

Esto puede demorar unos minutos en aplicarse.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -
EWSFastSearchTimeoutInSeconds $null -EWSMaxConcurrency $null -
EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
EWSPercentTimeInMailboxRPC $null

Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Exchange Server 2013, 2016 y 2019

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -
Role:ApplicationImpersonation -User ESET-user
```

Esto puede demorar unos minutos en aplicarse.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -
EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
```

```
Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-
ThrottlingPolicy
```

Tipos de cuarentena de correo

El administrador de Cuarentena de correo electrónico está disponible para los tres tipos de cuarentena:

- Cuarentena local
- Correo electrónico de cuarentena
- Cuarentena de Microsoft Exchange

Puede ver el contenido de Cuarentena de correo en el Administrador de cuarentena de correo. Además, puede ver la cuarentena local en la interfaz web de cuarentena de correo.

Almacenar mensajes de receptores inexistentes

Esta configuración se aplica a los mensajes marcados para ser puestos en cuarentena por la protección Antivirus, la protección Antispam o en base a Reglas. Cuando esta opción está habilitada, los mensajes que se enviaron a los destinatarios que no existen en el Active Directory se almacenan en el correo en cuarentena. Deshabilite esta característica si no desea conservar estos mensajes en el correo en cuarentena. Cuanto está deshabilitada, los mensajes para un destinatario desconocido se eliminarán silenciosamente.

Consulte ejemplo si desea tener todos los mensajes en destinatarios inexistentes en cuarentena.

Saltear la evaluación de reglas cuando se liberan correos electrónicos

Si desea liberar un mensaje de la cuarentena, las reglas no lo evaluarán. Es para evitar que el mensaje vuelva a la cuarentena y el mensaje liberado se entregue al destinatario de manera exitosa. Esta característica se usa solamente cuando el Administrador libera el mensaje. Si deshabilita esta característica o si un usuario que no es el Administrador libera un mensaje, las reglas evaluarán el mensaje.

> Si ejecuta un entorno en clúster y envía un mensaje de la cuarentena, los demás nodos de ESET Mail Security no volverán a poner el mensaje en cuarentena. Se consigue mediante la sincronización de las reglas entre los nodos del clúster.

Inicialización de firma de correo electrónico para entornos multiservidor

Le permite omitir la evaluación de las reglas al liberar correos electrónicos en un entorno con varios servidores. Ingrese el mismo valor de unidad (una cadena de caracteres, algo como una frase con contraseña) en todo el servidor en el que quiere establecer confianza.

Formatear para el sobre de archivos adjuntos

Cuando un mensaje de correo electrónico se libera de la cuarentena, se adjunta a un nuevo mensaje (sobre adjunto), que luego se entrega al destinatario. El destinatario recibe el mensaje original que se libera de la cuarentena de correo como un archivo adjunto. Puede usar el formato de sobre predefinido o modificarlo según sus requisitos con las variables disponibles.

Use ESET Cluster para almacenar todos los mensajes en cuarentena en un nodo

Si usa el clúster de ESET, esta opción está disponible. Le recomendamos utilizar esta función porque le permite mantener el almacenamiento de archivos en la cuarentena local en un solo lugar, el nodo maestro.

Nodo maestro

Especifique qué servidor es el nodo principal de su clúster de ESET. Luego, podrá acceder y administrar la Cuarentena local en el nodo maestro (puede usar el Administrador de cuarentena de correo desde la ventana principal del programa o la Interfaz web de la cuarentena de correo).

Cuarentena local

La cuarentena local utiliza el sistema de archivos local para almacenar los correos electrónicos en cuarentena y una base de datos de SQLite como índice. Los archivos de correo electrónico en cuarentena almacenados como también los archivos de la base de datos se cifran por motivos de seguridad. Estos archivos se ubican en C:\ProgramData\ESET\ESET Mail Security\MailQuarantine (en Windows Server 2012).

> i Si desea almacenar los archivos en cuarentena en un disco diferente, que no sea la unidad predeterminada C:, cambie la Carpeta de datos con su ruta preferida durante la instalación de ESET Mail Security.

Características de la cuarentena local:

- Los mensajes de SPAM y de correo electrónico en cuarentena se almacenarán en un sistema de archivos local, no en la base de datos del buzón de correo de Exchange.
- Cifra y comprime los archivos de correo electrónico en cuarentena almacenados localmente
- Interfaz web de cuarentena de correo: una alternativa al administrador de cuarentena de correo.
- Envía informes de cuarentena como una tarea programada a una dirección de correo electrónico especificada
- Elimina los archivos de correo electrónico en cuarentena de la ventana de cuarentena (después de 21 días en forma predeterminada), y los almacena en un sistema de archivos hasta que ocurre la eliminación automática después de una cantidad de días especificada
- Elimina automáticamente los archivos de correo electrónico antiguos (después de 3 días en forma predeterminada). Para obtener más información, consulte la configuración del almacenamiento de archivos
- Puede restablecer los archivos de correo electrónico en cuarentena eliminados mediante eShell (siempre que no hayan sido eliminados aún del sistema de archivos).
- Puede inspeccionar los mensajes de correo electrónico en cuarentena y decidir eliminar o liberar cualquiera de ellos. Para ver y administrar localmente los mensajes de correo electrónico en cuarentena, puede utilizar el Administrador de cuarentena de correo desde la ventana principal del programa o la interfaz web de la cuarentena de correo.

La desventaja de usar una cuarentena local es que, si ejecuta ESET Mail Security en múltiples servidores con el rol de servidor Transporte Hub, debe administrar la cuarentena local de cada servidor de manera separada. Cuantos más servidores de correo electrónico tiene, más cuarentenas debe administrar.

Almacenamiento de archivos

En esta sección puede modificar la configuración del almacenamiento de archivos que utiliza la cuarentena local.

Comprimir los archivos en cuarentena

Los archivos comprimidos en cuarentena ocupan menos espacio en disco, pero si decide no comprimir archivos, puede hacer clic en el botón de alternancia para deshabilitar la compresión.

Eliminar archivos antiguos tras (días)

Después de que los mensajes se retienen durante un número especificado de días, se eliminan de la ventana de cuarentena. Sin embargo, los archivos no se eliminarán del disco. Dado que los archivos no se eliminan del sistema de archivos, puede recuperarlos mediante eShell.

Eliminar archivos eliminados tras (en días)

Esta configuración elimina archivos del disco después de un número especificado de días y no puede recuperarlos después de que se hayan eliminado (a menos que tenga una solución de copia de seguridad del sistema de archivos).

Interfaz Web

La interfaz web de cuarentena de correo es una alternativa al Administrador de cuarentena de correo, no obstante, solo está disponible para la Cuarentena local.

La interfaz Web de la cuarentena no está disponible en un servidor con el rol de servidor de transporte perimetral porque no se puede acceder a Active Directory para la autenticación.

La interfaz web de cuarentena de correo le permite ver el estado de cuarentena del correo. También le permite administrar los objetos de correo electrónico en cuarentena. Se puede acceder a esta interfaz web mediante enlaces de los informes de cuarentena o al ingresar un enlace en el navegador web.

Para acceder a la interfaz web de la cuarentena de correo, debe autenticarse mediante credenciales de dominio. Edge autenticará automáticamente un usuario de dominio. Sin embargo, el certificado de la página web debe ser válido, el Inicio de sesión automático debe estar habilitado en Microsoft Internet Explorer, y debe agregar el sitio web de la interfaz web de Cuarentena de correos a los sitios de Intranet local.

Cualquier usuario de Active Directory puede tener acceso a la interfaz web de cuarentena de correo, pero solo verá los elementos en cuarentena enviados a su dirección de correo electrónico (incluidos los alias del usuario). El Administrador puede ver todos los elementos en cuarentena de todos los destinatarios.

ESET Mail Security no está utilizando IIS para ejecutar la interfaz web de la Cuarentena de correos. En cambio, usa servidor HTTP API, que incluye soporte SSL para permitir el intercambio de datos en conexiones HTTP seguras.

Url Web

Esta es la dirección URL donde está disponible la interfaz web de Cuarentena de correos. De forma predeterminada, es el FQDN del servidor con `/quarantine` (por ejemplo, `mailserver.company.com/quarantine`). Puede especificar su propio directorio virtual en lugar del `/quarantine` predeterminado. Puede cambiar la url de la Web en cualquier momento al editar el valor.

El valor web debe especificarse sin un esquema (HTTP, HTTPS) o número de puerto, solo use el formulario fqdn/virtualdirectory. También puede usar comodines en lugar de FQDN.

Después de modificar la dirección URL Web, no puede volver a la predeterminada haciendo clic en el icono de reversión. Quite la entrada y deje el cuadro de texto en blanco. Reinicie el servidor. Cuando se inicia ESET Mail Security y detecta que la url de la Web está vacía, completará automáticamente este campo con el valor predeterminado `fqdn/quarantine`.

> ESET Mail Security es compatible con url de la Web en cuatro formas diferentes:
> Comodín fuerte (+/quarantine)
> Explícito (mydomain.com/quarantine)
> Comodín débil vinculado con IP (192.168.0.0/quarantine)
> Comodín débil (*/quarantine)
> Para más información, consulte la sección **Categorías especificadoras del host** del artículo Cadenas de UrlPrefix.

Lenguaje de informes y Web

Esta característica le permite establecer el idioma de la interfaz web de cuarentena de correo y los informes de cuarentena.

Puerto HTTPS

El puerto HTTPS se usa para la interfaz web. El número de puerto predeterminado es 443.

Puerto HTTP

Puerto HTTP: se usa para liberar correos de cuarentena mediante informes de correos.

> Si no tiene el certificado SSL instalado en IIS, configure la vinculación del puerto HTTPS. Si cambia el número de puerto a HTTPS o HTTP, asegúrese de agregar el correspondiente enlace al puerto en IIS.

Registrar acciones de liberación a sucesos

Cuando se liberan elementos desde la cuarentena de correo, esta acción se escribe en los archivos de registro.

Habilitar administradores predeterminados

De manera predeterminada, los miembros del grupo de administradores tienen acceso de administrador a la interfaz web de la cuarentena de correo. El acceso de administrador no tiene restricciones y le permite al Administrador ver todos los elementos en cuarentena de todos los destinatarios. Si deshabilita esta opción, solo los usuarios enumerados en Derechos de acceso adicionales (consulte a continuación) pueden acceder a la interfaz web de Cuarentena de correos.

Derechos de acceso adicionales

Esta característica permite a los usuarios administrar la cuarentena de correo de otros usuarios. Puede crear administradores de cuarentena concediendo a un usuario (o grupo) acceso adicional a la interfaz web de cuarentena de correo de otro usuario (o de todos los miembros del grupo) para administrar los elementos en cuarentena.

1. Haga clic en **Editar** para abrir la ventana de derechos de acceso adicionales y haga clic en **Agregar**.

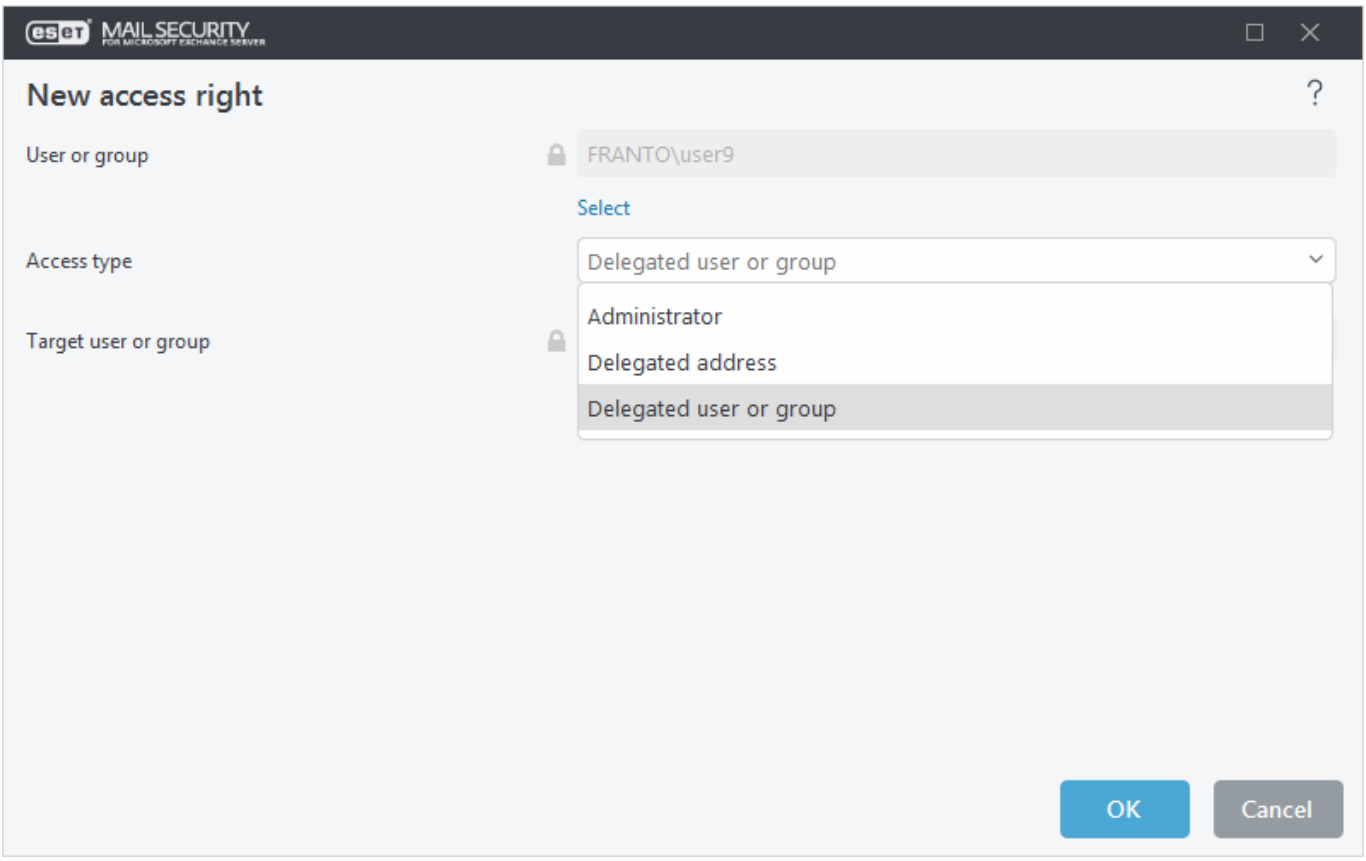
2. Haga clic en **Seleccionar** y use el selector de objetos de Active Directory para elegir un usuario o un grupo cuyos miembros tendrán acceso a la cuarentena de correo.

3. Seleccione el **Tipo de acceso** en el menú desplegable:

   - **Administrador:** el usuario tendrá acceso de administrador a la Interfaz web de cuarentena de correo.

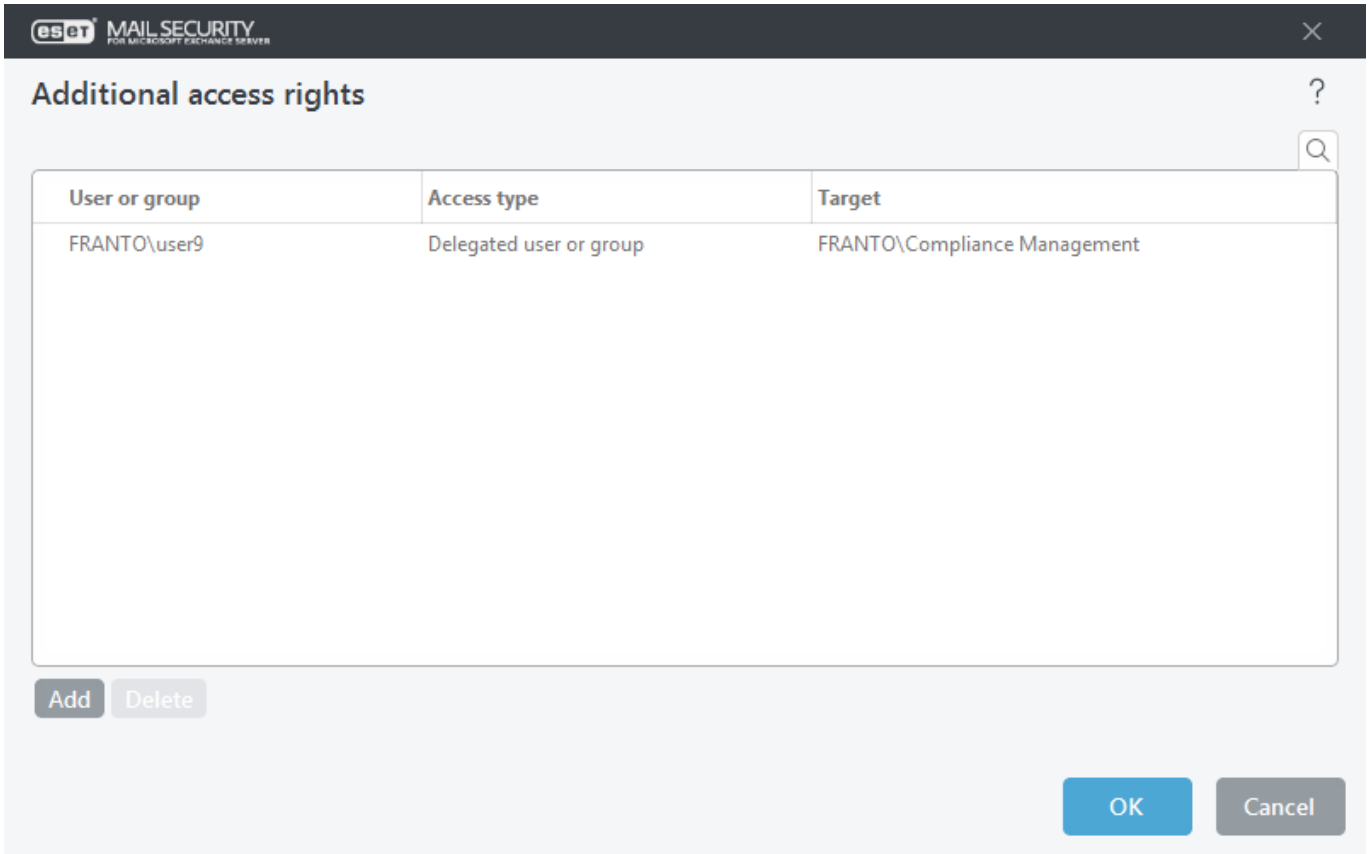
   - **Acceso delegado**: el usuario (delegado) puede ver y administrar los mensajes en cuarentena de otro destinatario. Especifique la Dirección del destinatario ingresando la dirección de correo electrónico para un usuario, cuyos mensajes en cuarentena los administrará un delegado. Si un usuario tiene un alias en el Active Directory, puede agregar derechos de acceso adicionales para cada alias si lo desea.

   - **Usuario o grupo delegado**: igual que Acceso delegado, y el usuario también puede usar el selector de objetos de Active Directory para elegir un usuario o un grupo cuya cuarentena de miembros se administrará.

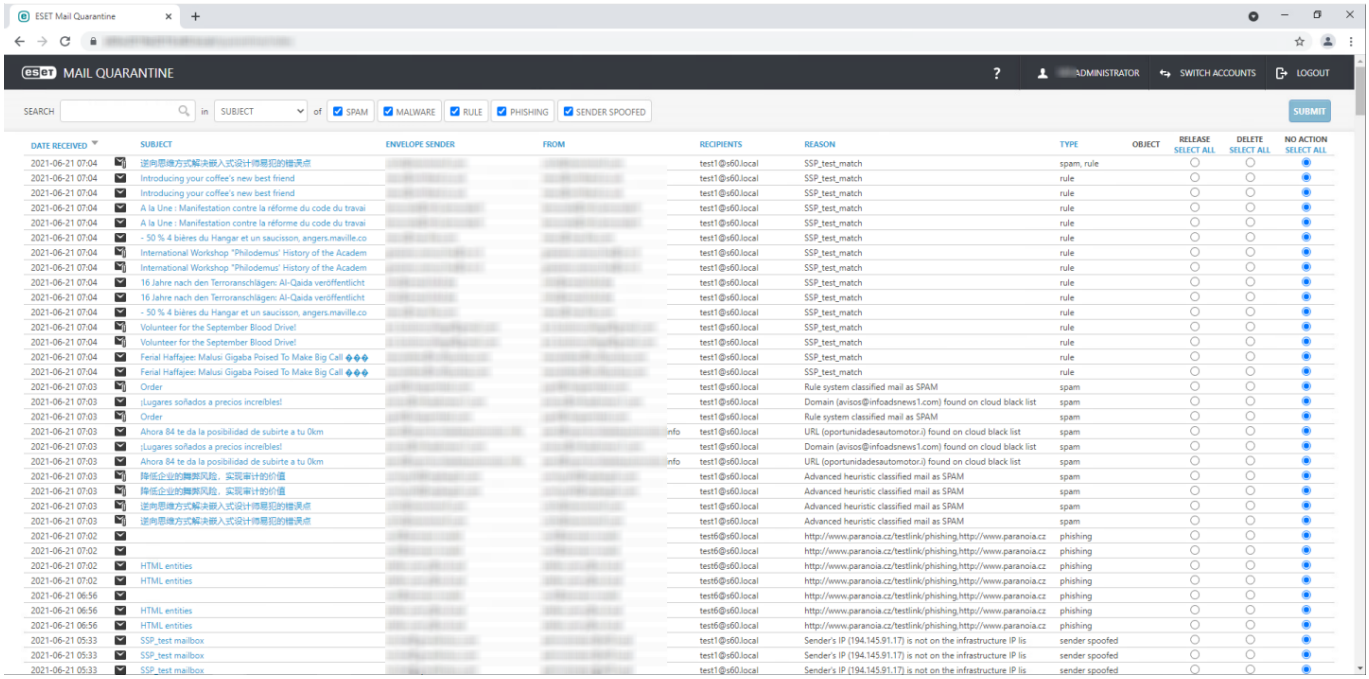


4. Haga clic en **Seleccionar** y elija un **usuario o grupo de destino**. Use el selector de objetos de Active Directory para elegir un usuario o un grupo cuya cuarentena de miembros será administrada por el delegado seleccionado en el paso 2.

Un ejemplo de usuarios a los que se les concedieron derechos de acceso adicionales a la interfaz web de la Cuarentena de correo:



Para acceder a la interfaz Web de cuarentena de correo, abra el navegador Web y utilice la URL especificada en **Configuración avanzada** (**F5**) > **Servidor** > **Cuarentena de correo** > **Interfaz Web** > **URL Web**.



Liberar

Esta función libera los correos electrónicos a sus destinatarios originales mediante el directorio de reproducción nueva y los elimina de la cuarentena. Haga clic en **Enviar** para confirmar la acción.

> Cuando se libera un correo de cuarentena, ESET Mail Security ignora el encabezado To: MIME porque se puede alterar fácilmente. En cambio, usa la información del destinatario original del comando `RCPT TO:` adquirida durante la conexión de SMTP. De esta manera, se garantiza que el destinatario correcto del correo reciba el mensaje liberado de cuarentena.

> Si ejecuta un entorno en clúster y envía un mensaje de la cuarentena, los demás nodos de ESET Mail Security no volverán a poner el mensaje en cuarentena. Se consigue mediante la sincronización de las reglas entre los nodos del clúster.

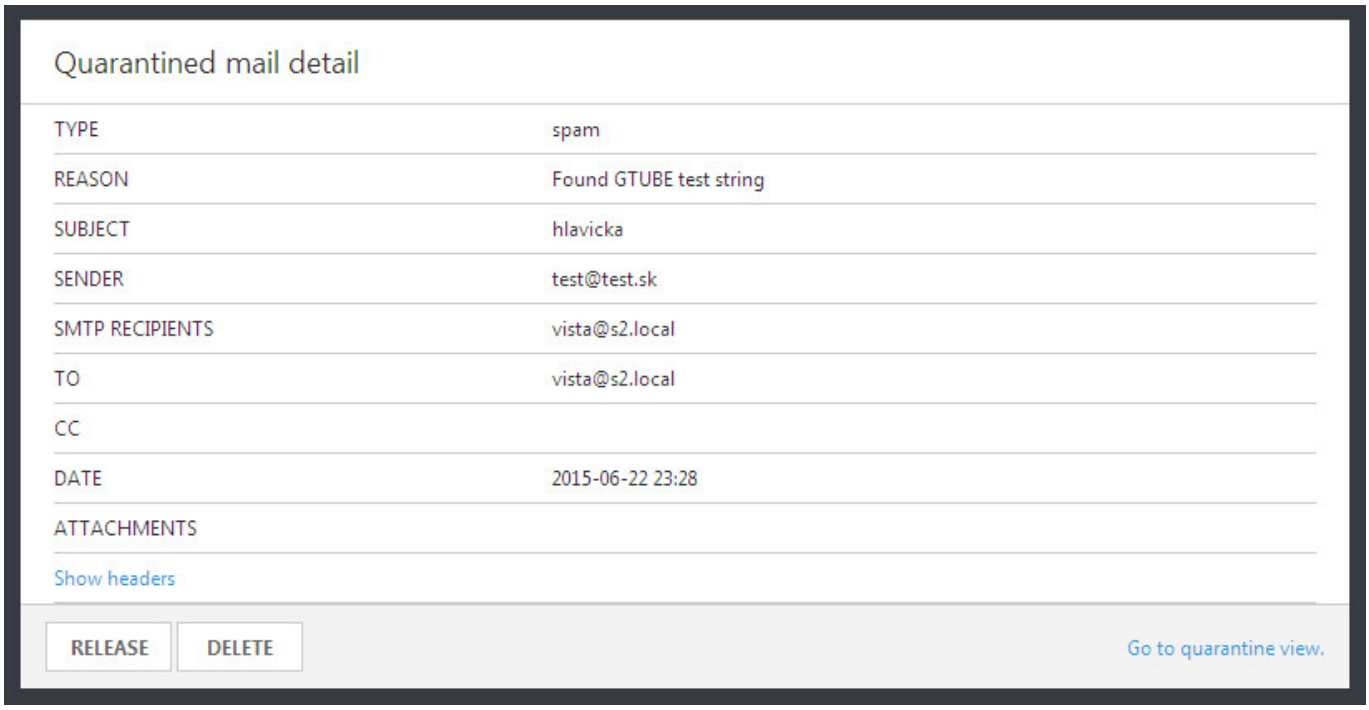
Liberar a

Si no desea liberar un correo electrónico a todos los destinatarios, use esta opción para seleccionar destinatarios específicos que recibirán el correo electrónico liberado. Esta opción solo está disponible para mensajes con varios destinatarios.

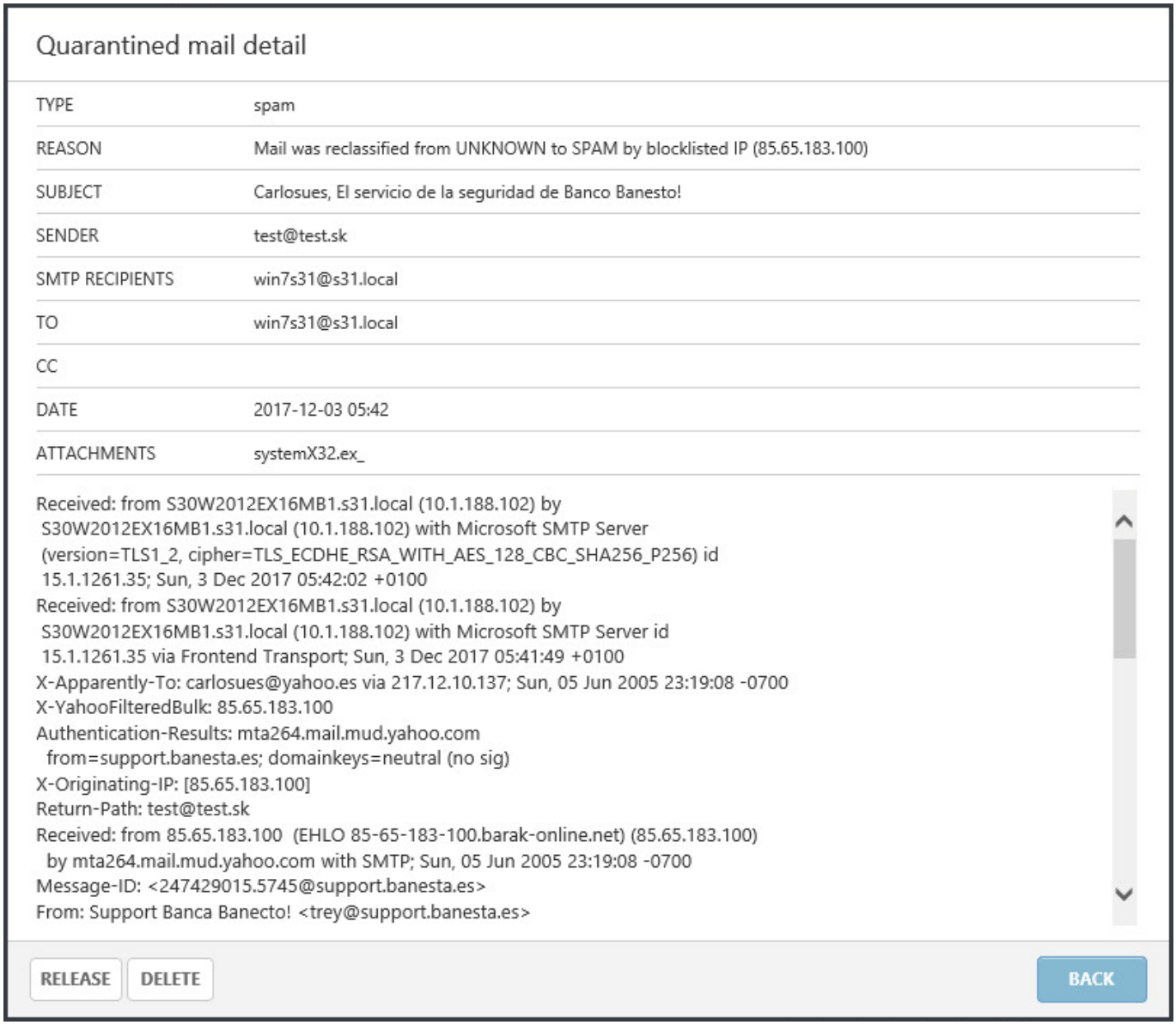
Eliminar

Esta característica elimina elementos de la cuarentena. Haga clic en **Enviar** para confirmar la acción.

Cuando haga clic en **Asunto**, se abrirá una ventana emergente con detalles acerca de los correos electrónicos en cuarentena, como el Tipo, Motivo, Emisor, Fecha, Adjuntos, etc.



Haga clic en **Mostrar encabezados** para revisar el encabezado del correo electrónico en cuarentena.



Si lo desea, haga clic en **Liberar** o **Eliminar** para realizar una acción sobre un mensaje de correo electrónico en cuarentena.

> Debe cerrar la ventana del navegador para salir por completo de la interfaz web de cuarentena de correos. De lo contrario, haga clic en **Ir a vista de cuarentena** para regresar a la pantalla anterior.

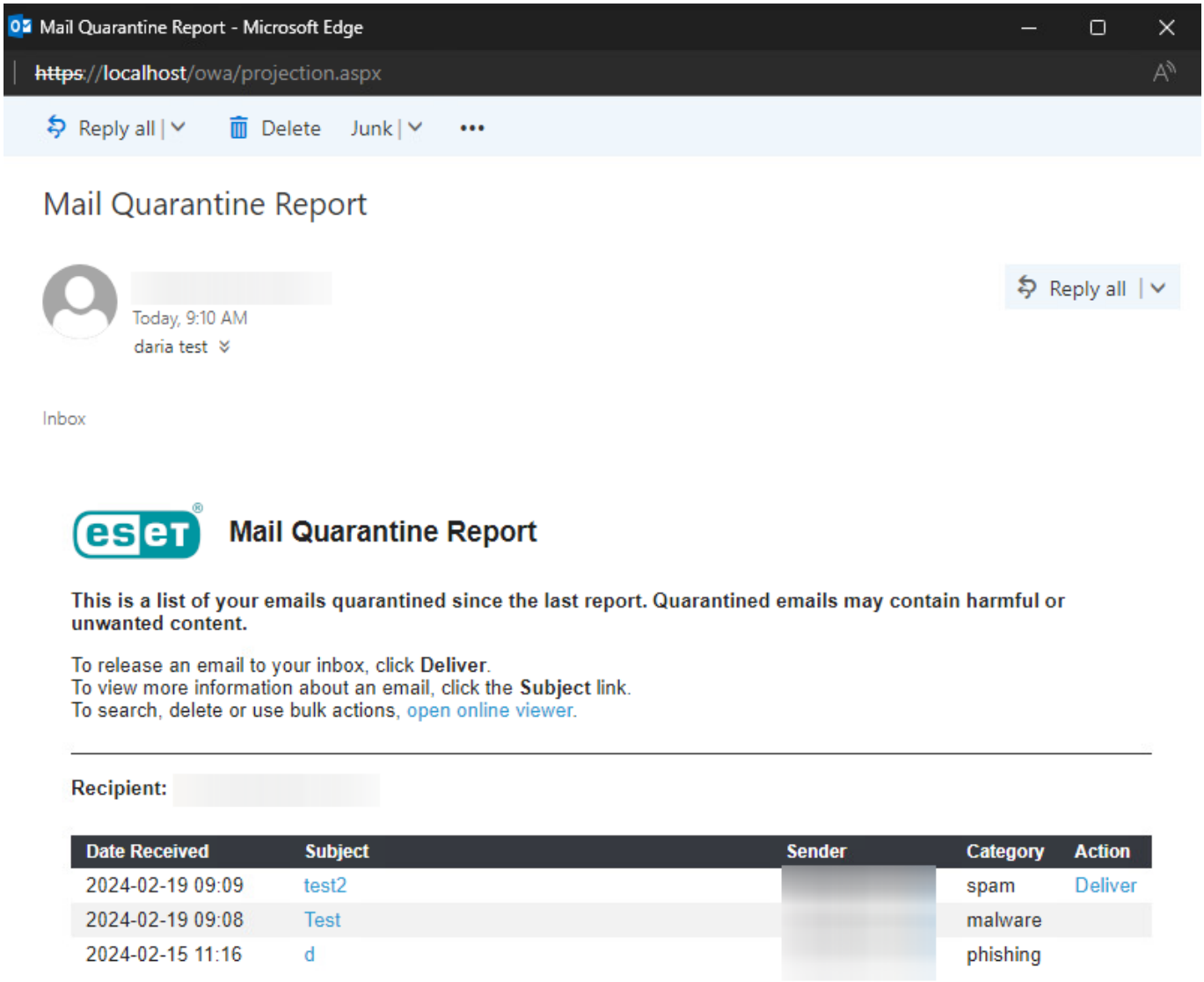
> Si tiene problemas para acceder a la Interfaz web de cuarentena de correo desde su navegador o recibe el error HTTP Error 403.4 - Forbidden o similar, controle para ver qué Tipo de cuarentena tiene seleccionado y asegurarse de que sea una **Cuarentena local** y que la opción **Habilitar interfaz web** esté habilitada.

Enviar informes de cuarentena de correo - tarea programada

Los informes de cuarentena de correo son mensajes de correo electrónico de notificación enviados a usuarios y administradores seleccionados para informarles sobre los mensajes de correo electrónico puestos en cuarentena por ESET Mail Security. Los informes contienen vínculos que les permiten a ustedes, además de los usuarios que reciben los informes de cuarentena de correo, eliminar o liberar (enviar) un mensaje de correo electrónico falso positivo (FP) directamente. La entrega de determinados mensajes filtrados por reglas o colocados en cuarentena de correo por protección antivirus no está permitida para los usuarios regulares.

Para empezar a enviar informes de cuarentena, cree una tarea programada (Herramientas > Tareas programadas > Agregar tarea) y seleccione el tipo de tarea Enviar informes de cuarentena de correo electrónico o Enviar informes de administrador de la cuarentena de correo electrónico. Al seleccionar destinatarios, los buzones de correo vinculados se incluyen en la lista de buzones de correo disponibles.

La tarea Enviar informes de cuarentena de correo/Enviar informes de cuarentena de correo envía un informe de Cuarentena de correo a través del correo electrónico según la tarea programada especificada. Este es un ejemplo del informe de cuarentena de correo de usuario:



El informe de cuarentena de correo contiene un enlace a la interfaz de la Web de cuarentena de correo del usuario (abrir el visualizador en línea).

> La tarea Enviar informes de cuarentena de correo electrónico está disponible solo cuando se utiliza la **Cuarentena local**. No podrá usarlo con el buzón de cuarentena y la cuarentena de MS Exchange.

Dirección del remitente

Especifica una dirección de correo electrónico que se mostrará como remitente del informe de cuarentena de correo.

Cuenta máx. de registros en el informe

Puede limitar la cantidad de entradas en un informe. El recuento predeterminado es 50.

URL Web

Esta URL se incluirá en el informe de cuarentena de correo para que el destinatario pueda hacer clic simplemente en el enlace para acceder a la interfaz web de la cuarentena de correo.

Destinatarios

Seleccione los usuarios que recibirán los informes de cuarentena de correo. Haga clic en **Editar** para seleccionar los buzones de correo para destinatarios específicos (los buzones de correo vinculados también son compatibles).

> El informe de Cuarentena de correo se enviará solo si hay mensajes en cuarentena. Si la cuarentena está vacía o no hay nuevos elementos desde el último informe, el informe no se enviará. Cuando se envíe el informe de cuarentena de correo, solo contendrá los elementos recién agregados desde el último informe (no todo el contenido de cuarentena).

> Objetivo: Cree una tarea programada para enviar los informes de cuarentena de correo regularmente a usted mismo como administrador o para informar a los usuarios de sus mensajes de spam actualmente almacenados en la cuarentena de correo.
> Navegue hasta **Herramientas** > **Tareas programadas** > **Agregar tarea** y abra el asistente.
> Escriba el **nombre de la tarea** y seleccione el **tipo de tarea** en el menú desplegable.
> **Envíe informes de administrador de cuarentena de correo** (el informe contendrá solo mensajes de spam del usuarios en particular) o **Envíe informes de administrador de cuarentena de correo** (el informe contendrá todos los mensajes, toda la cuarentena), haga clic en **Siguiente**.
> Seleccione una de las siguientes opciones para definir cuando desea ejecutar la tarea. Por ejemplo, **semanalmente** a las **10.00.00 AM** el **viernes**.
> Especifique la **dirección del remitente** (administrator@mydomain.com).
> Haga clic en **Editar** para agregar **Destinatarios** de la lista. Seleccione las casillas de correo electrónico del usuario que recibirán los informes de cuarentena de correo.

Interfaz web de la Cuarentena de correos del usuario

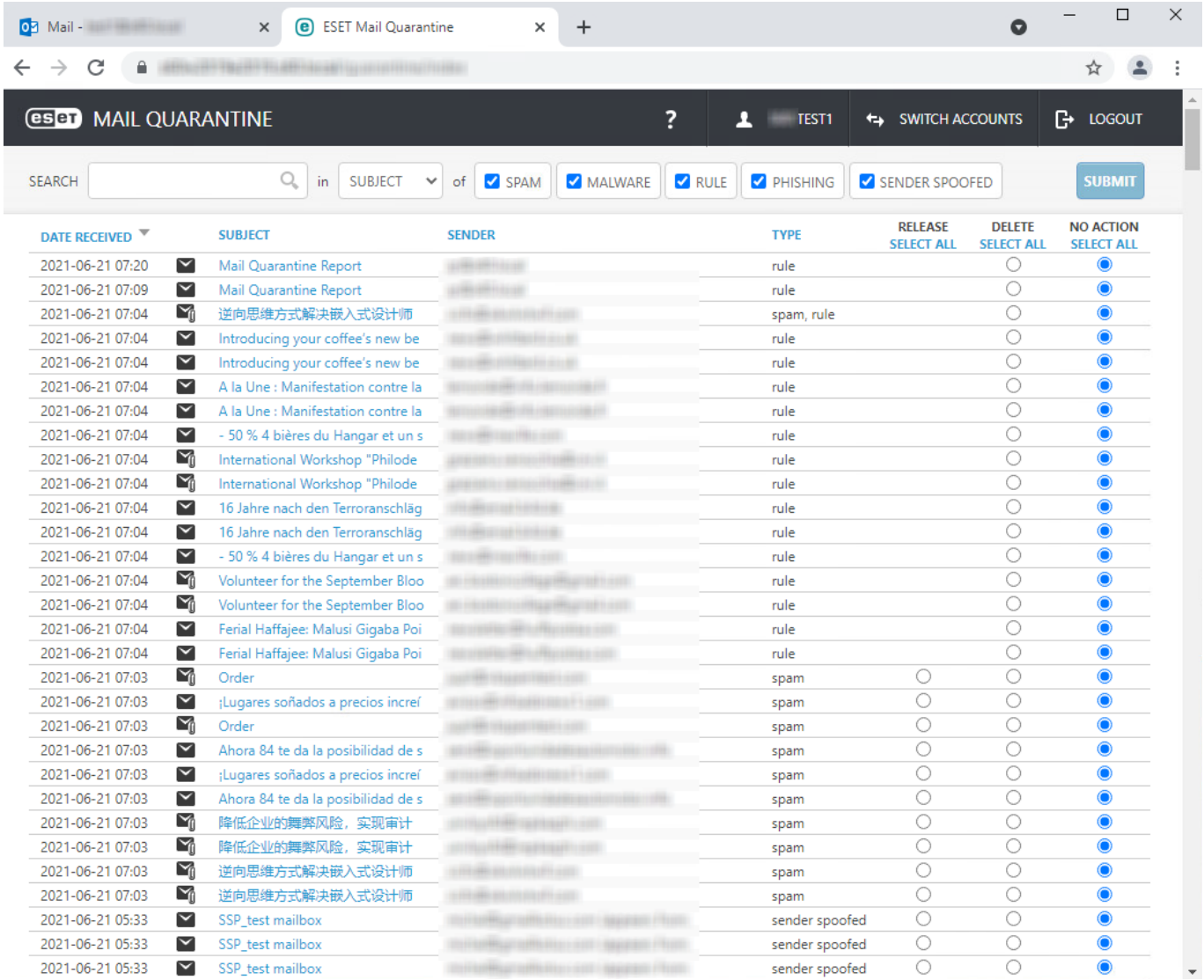
Se le ha otorgado acceso a una interfaz web donde podrá administrar los mensajes en cuarentena como spam, remitente suplantado o phishing, y los mensajes filtrados por las reglas establecidas por el administrador. Normalmente, solo podrá ver los mensajes enviados a su dirección de correo electrónico y puestos en cuarentena. Sin embargo, si ha sido delegado para manejar los mensajes puestos en cuarentena de otros usuarios, también verá los mensajes de esos usuarios. Puede distinguir los mensajes por destinatarios. Use la función de búsqueda para filtrar mensajes por destinatario, por ejemplo.

Puede elegir una acción para realizar con uno o varios mensajes, tales como **liberar**, **eliminar** o **sin acción**. La disponibilidad de acciones depende del nivel de acceso y la configuración de las reglas, por ejemplo, posiblemente no pueda liberar o eliminar determinados tipos de mensajes.

Si se le ha asignado acceso de administrador, verá todos los mensajes en cuarentena para todos los usuarios y podrá realizar cualquier acción.

Manejo de sus mensajes en cuarentena.

La interfaz web de cuarentena de correo le permite ver el contenido que se ha puesto en cuarentena. Si tiene acceso delegado o incluso es administrador, también verá otros mensajes en cuarentena.



Puede cambiar la cantidad de entradas por página (tamaño de la página) en el extremo inferior izquierdo de la ventana.

Si hay demasiados mensajes, use la función Búsqueda en la barra superior para buscar un correo electrónico particular o para filtrar el contenido por Asunto, Remitente o Destinatario (el Destinatario solo está disponible para los usuarios con acceso delegado o administrador). Además, puede usar las casillas de verificación para mostrar solo mensajes de un determinado tipo (**spam**, **malware**, **regla**, **phishing** y **remitente suplantado**).

Para liberar (entregar) un mensaje puesto en cuarentena como resultado de un falso positivo durante una clasificación, use los botones de opción a la derecha y seleccione **Liberar**. Para eliminar un mensaje, seleccione la acción **Eliminar**.

Puede seleccionar varios mensajes con la acción apropiada al mismo tiempo. Después de completar su selección, haga clic en **Enviar**.

Los mensajes marcados para liberar se entregan en su buzón de correo o al buzón de correo de su destinatario original si ha delegado el acceso y está liberando mensajes para otros usuarios. Los mensajes marcados para eliminar se quitan de la cuarentena permanentemente.

> i Ambas acciones, **Liberar** y **Eliminar**, son irreversibles cuando hace clic en **Enviar**.

La vista se actualiza automáticamente cuando hace clic en Enviar, pero puede actualizar la vista manualmente mediante el botón actualizar en el navegador web o puede presionar la tecla **F5** en el teclado.

> i Solo se pueden liberar los mensajes de spam y falsificados por el remitente. No se permite la liberación de mensajes de tipo de regla, phishing y malware. Si necesita liberar ese mensaje, pida ayuda al administrador.

No necesita eliminar regularmente los mensajes en cuarentena; se eliminan automáticamente después de un período de tiempo especificado por el administrador.

> i Debe cerrar la ventana del navegador web para salir por completo de la interfaz web de cuarentena de correo. De lo contrario, haga clic en Ir a vista de cuarentena para regresar a la pantalla anterior.

Buzón de correo de cuarentena y cuarentena de Microsoft Exchange

Si decide no utilizar la cuarentena local tiene dos opciones, la Cuarentena de casilla de correo o la Cuarentena de MS Exchange. Cualquiera que sea la opción que elija, deberá crear un usuario dedicado con casilla de correo (por ejemplo main_quarantine@company.com) la cual luego se utilizará para almacenar mensajes de correo electrónico en cuarentena. Este usuario y este buzón de correo además serán utilizados por el Administrador de cuarentena de correo para ver y administrar los elementos de la cuarentena. Deberá especificar los detalles de cuenta de este usuario en la Configuración del administrador de cuarentena.

> i La ventaja del Buzón de correo en cuarentena/Cuarentena de Microsoft Exchange con respecto a la Cuarentena local es que los objetos en cuarentena de correo se administran en un lugar sin importar la cantidad de servidores con rol de servidor de Transporte Hub. A diferencia de la cuarentena local, el Buzón de correo en cuarentena/Cuarentena de Microsoft Exchange, los mensajes de SPAM y de correo electrónico en cuarentena se almacenan en la base de datos del buzón de correo de Exchange. Cualquiera con acceso a la Casilla de correo de cuarentena puede gestionar los correos electrónicos en cuarenta.

Al comparar el Buzón de correo de cuarentena y la cuarentena de MS Exchange, ambas opciones usan un buzón de correo electrónico dedicado como mecanismo subyacente para almacenar los mensajes en cuarentena, pero difieren ligeramente en la forma en que se envían los mensajes de correo electrónico al buzón de correo. Buzón de correo de cuarentena vs. cuarentena de MS Exchange:

Correo electrónico de cuarentena

ESET Mail Security crea un correo electrónico de envoltorio separado con información adicional y los correos electrónicos originales como dato adjunto y lo envía al buzón de entrada.

Especifica la dirección del mensaje de cuarentena (por ejemplo main_quarantine@company.com).

No recomendamos que use la cuenta de usuario de Administrador como casilla de correo de cuarentena.

Cuarentena de MS Exchange

El servidor de Microsoft Exchange es responsable de enviar el correo electrónico al buzón del correo. El buzón de correo debe estar configurado como Cuarentena a nivel de organización en el Directorio Activo (por el comando PowerShell indicado a continuación).

En forma predeterminada, la cuarentena interna de Microsoft Exchange Server no está activada. A menos que esté activada, abra la Consola de Administración de Exchange y escriba el siguiente comando (reemplazar `Name@domain.com` por una dirección real de su casilla de correo dedicada): `Set-ContentFilterConfig -QuarantineMailbox name@domain.com`

ESET Mail Security usa el sistema de cuarentena de Microsoft Exchange (esto aplica a Microsoft Exchange Server 2010 y posteriores) En este caso, el mecanismo interno de Exchange se usa para almacenar mensajes potencialmente infectados y SPAM.

Configuración de la administración de cuarentena

Dirección del host

Aparecerá de manera automática si su Exchange Server con rol de servidor de acceso de cliente (CAS) está localmente presente. De manera alternativa, si el rol de CAS no está presente en el mismo servidor con ESET Mail Security instalado pero puede encontrarse dentro de Active Directory (AD), la dirección del host aparecerá de manera automática. Si no aparece, puede ingresar el nombre del host de manera manual. La detección automática no funcionará con el rol del servidor Transporte Edge. No se admite la dirección IP, debe utilizar el nombre de host del servidor CAS.

Nombre de usuario

Cuenta de usuario de cuarentena dedicada que creó para almacenar los mensajes en cuarentena (o una cuenta que tiene acceso a esta casilla de correo mediante la delegación de acceso). En el rol del servidor Transporte Edge que no forma parte del dominio, resulta necesario utilizar toda la dirección de correo electrónico (por ejemplo *main_quarantine@company.com*).

Contraseña

Escriba la contraseña de su cuenta en cuarentena.

Utilizar SSL

Debe estar habilitado si Servicios web de Exchange (EWS) está configurado para **Solicitar SSL** en IIS. Si el SSL está habilitado, se debe importar el certificado de Exchange Server al sistema con ESET Mail Security (en caso de que los roles de Exchange Server estén en servidores diferentes). Las configuraciones para EWS se pueden encontrar en IIS en Sites/Default web site/EWS/SSL Settings.

Solo desactive **Usar SSL** cuando Servicios web de Exchange (EWS) está configurado en IIS para no requerir SSL.

Ignorar los errores del certificado del servidor

Ignora los siguientes estados: self-signed, wrong name in certificate, wrong usage, expired.

Servidor proxy

En caso de que utilice un servidor proxy entre Exchange Server con rol CAS y el Exchange Server donde está instalado ESET Mail Security, especifique los parámetros del servidor proxy. Esto es necesario porque ESET Mail Security se conecta con el API (EWS) mediante HTTP/HTTPS. De lo contrario, la casilla de correo de cuarentena y la cuarentena de Microsoft Exchange no funcionarán.

Servidor proxy

Ingrese la dirección IP o nombre del servidor proxy que desea utilizar.

Puerto

Ingrese el número de puerto del servidor proxy.

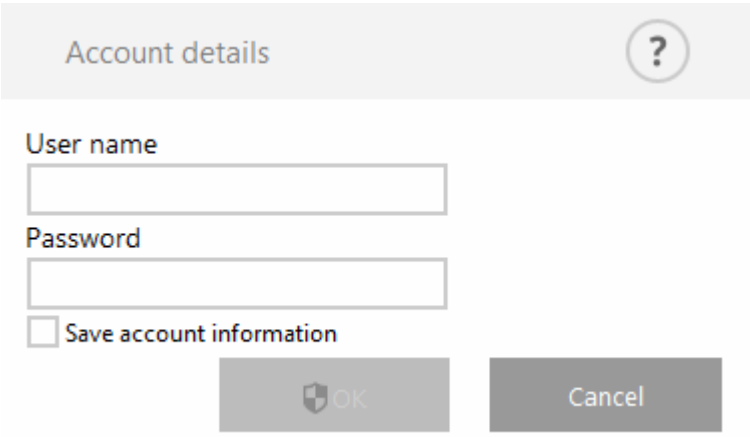
Nombre de usuario, Contraseña

Ingrese las credenciales si su servidor proxy requiere autenticación.

Detalles de la cuenta del administrador de la cuarentena

Esta ventana de diálogo se mostrará si no ha especificado los detalles de la cuenta (nombre de usuario y contraseña) en Administrador de cuarentena. Especifique las credenciales para un usuario con acceso a la Casilla de correo de cuarentena y haga clic en **Aceptar**. De manera alternativa, presione **F5** para acceder a la **Configuración avanzada** y navegar al **Servidor** > **Cuarentena de correo** > Configuraciones del administrador de cuarentena.

Ingrese el **Nombre de usuario** y la **Contraseña** para su casilla de correo de cuarentena.



Haga clic en la casilla de verificación junto a **para guardar información de la cuenta** y guardar las configuraciones de la cuenta para uso futuro cuando acceda al administrador de cuarentena.

Firma DKIM

La firma Correo identificado con clave de dominio (DKIM) es un método para proteger los mensajes de correo electrónico salientes y facilitar la comprobación. Este método ofrece a los servidores de correo receptores una forma precisa de distinguir los mensajes genuinos del spam.

La autenticación DKIM funciona de la siguiente forma:

- Los encabezados de mensajes de correo electrónico salientes están firmados con la clave privada DKIM.
- El servidor de correo receptor comprueba el registro DKIM de DNS que contiene una clave pública.
- Si la firma con la clave privada en los encabezados del mensaje coincide con la clave pública del registro DKIM de DNS, el correo electrónico se considerará genuino y se entregará a los destinatarios.
- Si la firma y la clave pública no coinciden, lo que sucede con el mensaje de correo electrónico depende de la configuración del servidor de correo receptor (puede tener reglas específicas, por ejemplo, ESET Mail Security usa la condición de regla de resultado DKIM para este propósito)

Para utilizar la característica de firma DKIM de ESET Mail Security, asegúrese de tener el registro DKIM de DNS configurado para su dominio. Para obtener más información sobre la creación de un registro DKIM, consulte el artículo ¿Qué es el registro DKIM y cómo crearlo?. En el artículo, también se incluye un ejemplo de un registro DKIM. También puede probar utilizar un generador de DKIM en línea para generar claves privadas y públicas de DKIM.

Cuando haya terminado, le sugerimos que use DKIM Record Checker o MXToolBox para verificar la presencia de la clave DKIM pública y que la sintaxis se haya implementado correctamente.

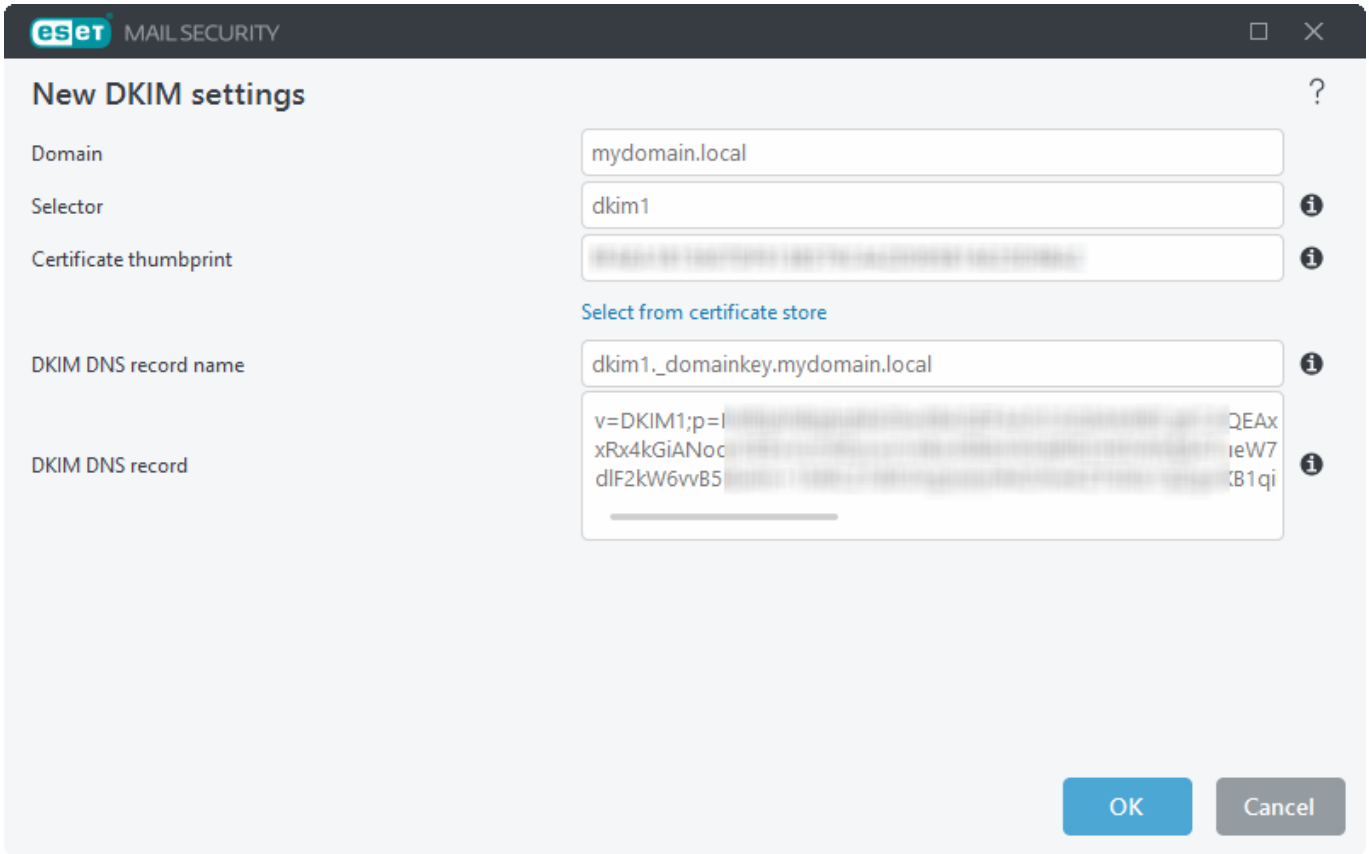
Configure la firma DKIM en ESET Mail Security; para ello, especifique los dominios DKIM y una lista de los encabezados de correo electrónico que desea firmar. La firma DKIM se agrega a los encabezados de mensajes seleccionados. Cada firma DKIM contiene información que los servidores de correo pueden usar para verificar la autenticidad de un mensaje de correo electrónico a medida que lo pasan al destino final. Si utiliza varios dominios para los mensajes salientes, puede configurar la firma DKIM para cada dominio por separado.

> Habilite la **firma DKIM** en **Servidor** > Integración en la **Configuración avanzada**. Para la configuración de la prioridad del agente, le recomendamos que mantenga la prioridad del agente ESET DKIM en el último lugar, en la parte inferior, para asegurarse de que los encabezados estén firmados por última vez después de cualquier modificación en los encabezados realizada por agentes anteriores.

Dominios DKIM

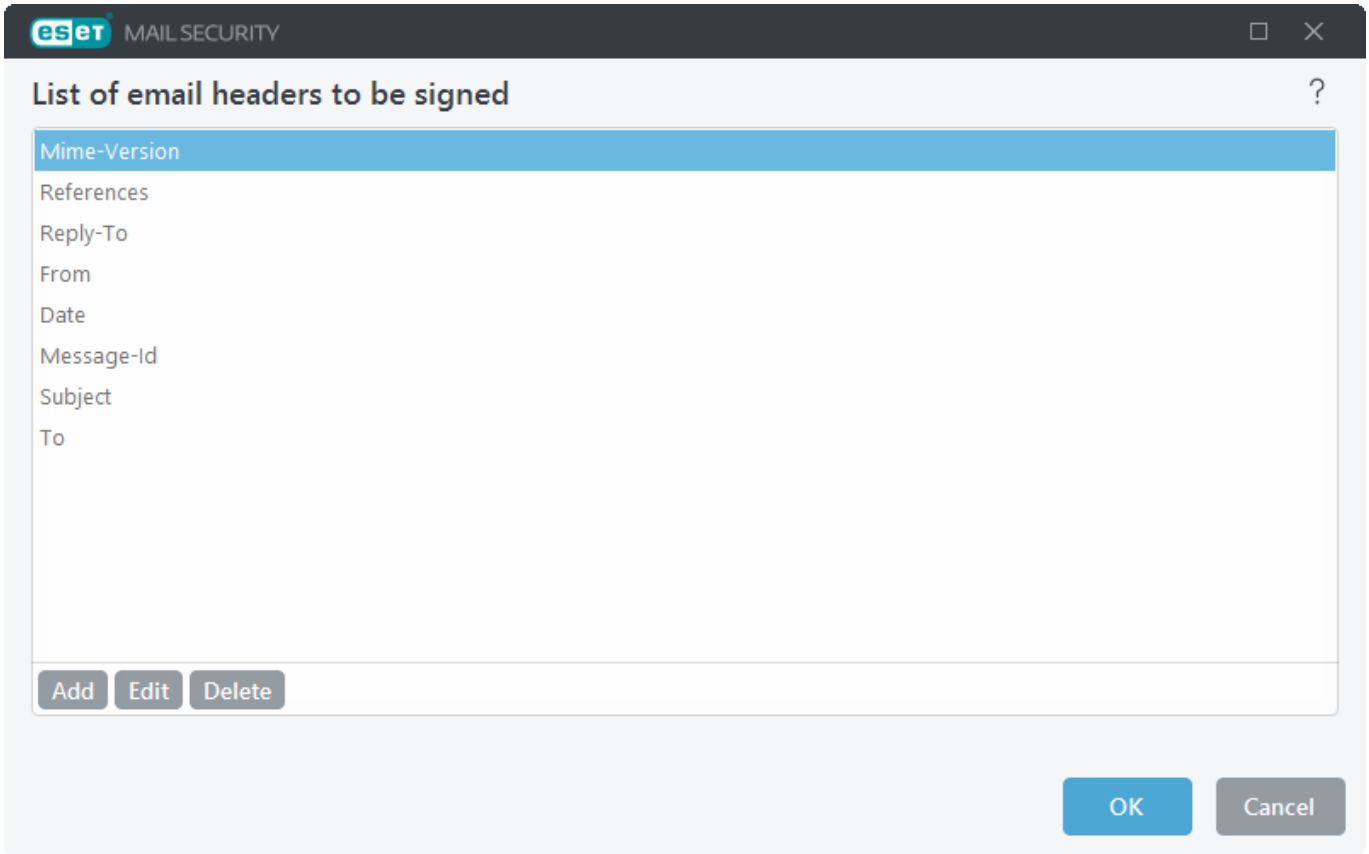
Defina la configuración de cada dominio para la firma DKIM. Haga clic en **Editar** para abrir la ventana de dominios DKIM. Haga clic en **Agregar** para crear una **nueva configuración de DKIM** o Editar para modificar las existentes.

- **Dominio**: escriba el dominio (por ejemplo, *domainname.local*)
- **Selector**: especifique un selector para un atributo de firma DKIM; a continuación, se registra en el campo de encabezado Firma DKIM
- **Certificado del cliente:** haga clic en **Seleccionar** y elija el certificado de cliente utilizado para la firma DKIM.



Lista de encabezados de correo electrónico a firmar

Haga clic en **Editar** para abrir la ventana Lista de encabezados de correo electrónico que se firmarán. Haga clic en **Agregar** para agregar nuevos encabezados o **Editar** para modificar los encabezados existentes en la lista.



Prueba Antivirus

Para verificar que la protección en tiempo real se encuentra activa y es capaz de detectar virus, use un archivo de prueba de eicar.com. Este es un archivo inofensivo detectable por todos los programas antivirus creados por la empresa EICAR (Instituto Europeo para la Investigación de los Antivirus Informáticos).

Para probar la funcionalidad del antivirus, cree un archivo de texto que contenga esta cadena de caracteres:

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

Para obtener más información y descargar archivos de prueba, visite https://www.eicar.org/download-anti-malware-testfile/

Prueba antispam

Mediante una cadena de prueba GTUBE (prueba genérica para correo electrónico masivo no solicitado), puede comprobar si la ESET Mail Security característica Antispam detecta los mensajes de spam entrantes.

Para probar la funcionalidad antispam, envíe un correo electrónico con la siguiente cadena de 68 bytes en el cuerpo del mensaje:

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

Utilice la cadena tal como está (una línea, sin espacios en blanco o saltos de línea). Usted puede descargar el mensaje de correo electrónico más adecuado en el formato RFC-822.

Prueba anti-phishing

Para probar la funcionalidad anti-phishing, envíe un correo electrónico con el siguiente enlace (URL) en el cuerpo del mensaje o en el asunto:

https://www.amtso.org/check-desktop-phishing-page/

Para ver la actividad de protección de correo Anti-Phishing, consulte **Archivos de registro** > Registro de protección del servidor de correo. Contendrá información sobre los mensajes de correo electrónico y los enlaces de phishing encontrados.

Configuración general

Puede configurar los parámetros y opciones generales según sus necesidades. El menú de la izquierda incluye las siguientes categorías:

Computer

Active o desactive la detección de aplicaciones potencialmente no deseadas, inseguras, sospechosas, y la protección anti-stealth. Especifique las exclusiones de procesos o archivos y carpetas. Configure la protección del sistema de archivos en tiempo real, ThreatSense los parámetros, la protección basada en la nube (ESET

LiveGrid®), las detecciones de malware (Exploración del equipo a petición y otras opciones de exploración), la exploración de Hyper-V y HIPS.

Actualización

Configure las opciones de actualización tales como perfiles, antigüedad del motor de detección, instantáneas para reversión de módulo, tipo de actualización, servidor de actualización personalizado, servidor de conexión y proxy, mirror de actualización, acceso a archivos de actualización, servidor HTTP, detalles de cuenta de usuario para la conexión de red, etc.

Protección de red

Administrar la protección de red: redes conocidas, zonas, protección contra ataques a la red (IDS), protección contra ataques por fuerza bruta y protección contra botnets.

Internet y correo electrónico

Habilita la configuración del Filtrado de protocolos y las exclusiones (Aplicaciones excluidas y direcciones IP), opciones de filtrado de protocolo SSL/TLS, protección del cliente de correo electrónico (integración, protocolos de correo electrónico, alertas y notificaciones), protección del acceso a la web (Protocolos web HTTP/HTTPS y administración de direcciones URL) y protección antiphishing del cliente de correo electrónico.

Control del dispositivo

Le permite la integración y configuración de reglas y grupos de control de dispositivos.

Configuración de herramientas

Permite personalizar las herramientas, como ESET CMD, ESET RMM, Proveedor WMI, ESET PROTECT, objetivos para explorar, notificaciones sobre actualización de Windows, archivos de registro, servidor proxy, notificaciones por correo electrónico, diagnósticos, clúster, etc.

Notificaciones

Configure las notificaciones que se mostrarán en el escritorio o se enviarán por correo electrónico para estados de la aplicación, notificaciones en el escritorio, alertas interactivas y reenvíos.

Interfaz de usuario

Configure la ventana principal del programa, información sobre la licencia, protección por contraseña, política de ejecución de eShell y mucho más.

Computer

El motor de detección brinda protección contra ataques maliciosos del sistema mediante la exploración de archivos, correos electrónicos y comunicaciones de red. Si se detecta un objeto clasificado como malware, se dará lugar a la corrección. El motor de detección puede primero bloquearlo para eliminarlo y, luego, desinfectarlo, eliminarlo o enviarlo a cuarentena.

Protección en tiempo real y con aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que permite mejorar la detección en función del aprendizaje automático. Lea más sobre este tipo de

protección en el glosario . Puede configurar Niveles de informes y protecciones de las siguientes categorías:

Malware

Un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su equipo. Sin embargo, el término "virus" suele usarse en forma errónea. "Malware" (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Lea más sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente no deseadas (PUAs)

Una aplicación potencialmente no deseada es un software cuyo objetivo no es necesariamente malicioso; sin embargo, puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades que el usuario no aprueba o no espera, o tener otros objetivos no deseados.

Esta categoría incluye: software de visualización de publicidad, descarga de envoltorios, distintas barras de herramientas de navegadores, software con comportamiento engañoso, bundleware, trackware, etc. Lea más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente sospechosas

Es un software comprimido con empaquetadores o protectores frecuentemente usados para evitar la ingeniaría inversa o para ofuscar el contenido de un ejecutable (por ejemplo, para ocultar la presencia de malware) mediante métodos propietarios de compresión o cifrado.

Esta categoría incluye: todas las aplicaciones desconocidas comprimidas con empaquetadores o protectores utilizadas frecuentemente para comprimir malware.

Aplicaciones potencialmente no seguras

Esta clasificación se proporciona para el software comercial legítimo que pudiera usarse indebidamente con fines maliciosos. Una aplicación potencialmente no segura hace referencia al software comercial legítimo que se puede usar inadecuadamente para fines malintencionados.

Esta categoría incluye: herramientas de descifrado, generadores de claves de licencia, herramientas de piratería informática, herramientas de control o acceso remoto, aplicaciones para adivinar contraseñas y los registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). Esta opción se encuentra deshabilitada en forma predeterminada.
Lea más información sobre estos tipos de aplicaciones en el glosario.

Lea lo siguiente antes de modificar un umbral (o nivel) de categoría Informar o Protección:

Informar

El motor de detección y el componente de aprendizaje automático se ocupan de realizar los informes. Puede definir el umbral de informes que mejor se adapte a su entorno y necesidades. No hay una única configuración correcta. Por lo tanto, recomendamos que monitoree el comportamiento dentro de su entorno y decida si hay una configuración de informes más apropiada.
Los informes no ejercen ningún tipo de acción sobre los objetos, ya que transmiten la información a una capa de protección correspondiente, y la capa de protección realiza las tareas pertinentes.

Intenso	**Se han configurado los informes con máxima confidencialidad. Se informan más detecciones. Si bien el ajuste Intenso parecería ser el más seguro, a menudo también puede ser demasiado confidencial, lo que puede resultar contraproducente.** El ajuste Intenso puede identificar de manera falsa objetos como maliciosos y se iniciará una acción respecto de dichos objetos (según los ajustes de Protección).
Balanceado	Este ajuste es un equilibrio óptimo entre el rendimiento y la precisión de las tasas de detección y el número de objetos que se reportan falsamente.
Cauteloso	Informes que se configuran para minimizar la cantidad de objetos identificados en forma errónea al mismo tiempo que se mantiene un nivel suficiente de protección. Los objetos se informan únicamente cuando la probabilidad es evidente y concuerda con el comportamiento de un malware.
Desactivado	Informes no activos. No se hallaron, reportaron ni limpiaron detecciones. No pueden desactivarse los informes sobre malware. Por lo tanto, el ajuste Desactivado no se encuentra habilitado para el malware.

Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.

Protección

Cuando un objeto se informa en función de la configuración mencionada y de los resultados del aprendizaje automático, se bloquea y se inicia una acción (limpiado, quitado o movido a cuarentena).

Intenso	**Las detecciones informadas de nivel agresivo (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).**
Balanceado	Las detecciones reportadas de nivel balanceado (o más bajo) se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Cauteloso	Las detecciones reportadas de nivel cauteloso se bloquean, y se inicia la corrección automática (por ejemplo, la desinfección).
Desactivado	Los informes no están activos, no se encontraron, informaron ni limpiaron detecciones. No pueden desactivarse los informes sobre malware. Por lo tanto, la configuración Apagado no se encuentra habilitada para el malware.

Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.

De manera predeterminada, las configuraciones de protección del aprendizaje automático antes mencionado rigen también para la exploración del equipo a demanda. De ser necesario, puede configurar los ajustes **Protección de acuerdo a las necesidades y con aprendizaje automático** por separado. Haga clic en el ícono del interruptor para deshabilitar **Uso de configuraciones de protección en tiempo real** y continúe con la configuración.

Detección de aprendizaje automático

El motor de detección brinda protección contra ataques maliciosos del sistema mediante la exploración de archivos, correos electrónicos y comunicaciones de red. Si se detecta un objeto clasificado como malware, se dará lugar a la corrección. El motor de detección puede primero bloquearlo para eliminarlo y, luego, desinfectarlo, eliminarlo o enviarlo a cuarentena.

Protección en tiempo real y con aprendizaje automático

El aprendizaje automático avanzado ahora forma parte del motor de detección como una capa de protección avanzada, lo que permite mejorar la detección en función del aprendizaje automático. Lea más sobre este tipo de protección en el glosario . Puede configurar Niveles de informes y protecciones de las siguientes categorías:

Malware

Un virus informático es un código malicioso que puede agregarse al principio o al final de archivos existentes en su equipo. Sin embargo, el término "virus" suele usarse en forma errónea. "Malware" (software malicioso) es un término más preciso. La detección de malware se realiza mediante la combinación del módulo del motor de detección con el componente de aprendizaje automático. Lea más sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente no deseadas (PUAs)

Una aplicación potencialmente no deseada es un software cuyo objetivo no es necesariamente malicioso; sin embargo, puede instalar software adicional no deseado, cambiar el comportamiento del dispositivo digital, realizar actividades que el usuario no aprueba o no espera, o tener otros objetivos no deseados.

Esta categoría incluye: software de visualización de publicidad, descarga de envoltorios, distintas barras de herramientas de navegadores, software con comportamiento engañoso, bundleware, trackware, etc. Lea más información sobre estos tipos de aplicaciones en el glosario.

Aplicaciones potencialmente sospechosas

Es un software comprimido con empaquetadores o protectores frecuentemente usados para evitar la ingeniaría inversa o para ofuscar el contenido de un ejecutable (por ejemplo, para ocultar la presencia de malware) mediante métodos propietarios de compresión o cifrado.

Esta categoría incluye: todas las aplicaciones desconocidas comprimidas con empaquetadores o protectores utilizadas frecuentemente para comprimir malware.

Aplicaciones potencialmente no seguras

Esta clasificación se proporciona para el software comercial legítimo que pudiera usarse indebidamente con fines maliciosos. Una aplicación potencialmente no segura hace referencia al software comercial legítimo que se puede usar inadecuadamente para fines malintencionados.

Esta categoría incluye: herramientas de descifrado, generadores de claves de licencia, herramientas de piratería informática, herramientas de control o acceso remoto, aplicaciones para adivinar contraseñas y los registradores de pulsaciones (programas que registran cada tecla pulsada por el usuario). Esta opción se encuentra deshabilitada en forma predeterminada.
Lea más información sobre estos tipos de aplicaciones en el glosario.

Lea lo siguiente antes de modificar un umbral (o nivel) de categoría Informar o Protección:

^ Informar

El motor de detección y el componente de aprendizaje automático se ocupan de realizar los informes. Puede definir el umbral de informes que mejor se adapte a su entorno y necesidades. No hay una única configuración correcta. Por lo tanto, recomendamos que monitoree el comportamiento dentro de su entorno y decida si hay una configuración de informes más apropiada.
Los informes no ejercen ningún tipo de acción sobre los objetos, ya que transmiten la información a una capa de protección correspondiente, y la capa de protección realiza las tareas pertinentes.

Intenso	**Se han configurado los informes con máxima confidencialidad. Se informan más detecciones. Si bien el ajuste Intenso parecería ser el más seguro, a menudo también puede ser demasiado confidencial, lo que puede resultar contraproducente.** El ajuste Intenso puede identificar de manera falsa objetos como maliciosos y se iniciará una acción respecto de dichos objetos (según los ajustes de Protección).
Balanceado	Este ajuste es un equilibrio óptimo entre el rendimiento y la precisión de las tasas de detección y el número de objetos que se reportan falsamente.
Cauteloso	Informes que se configuran para minimizar la cantidad de objetos identificados en forma errónea al mismo tiempo que se mantiene un nivel suficiente de protección. Los objetos se informan únicamente cuando la probabilidad es evidente y concuerda con el comportamiento de un malware.
Desactivado	Informes no activos. No se hallaron, reportaron ni limpiaron detecciones. No pueden desactivarse los informes sobre malware. Por lo tanto, el ajuste Desactivado no se encuentra habilitado para el malware.

Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.

Protección para transporte de correo y aprendizaje automatizado

Informar
Llevado a cabo por el motor de detección y el componente de aprendizaje automático. Los informes no ejercen ningún tipo de acción sobre los objetos (esto se lleva a cabo en la capa de protección correspondiente).
Protección
Configure los parámetros en la sección Protección del transporte de correo electrónico para afectar el tipo de acción que se inicia en relación con los objetos informados. También puede configurar una regla personalizada:

Ejemplo de instalación de Núcleo:
Objetivo: Poner en cuarentena los mensajes que contienen Malware o datos adjuntos protegidos por contraseña, dañados o encriptados
Crear la siguiente regla para la **Protección del transporte de correo electrónico**:
Condición
Tipo: **Resultado de la exploración antivirus**
Operación: **es**
Parámetro: **Infectado - no limpiado**
Acción
Tipo: **Mensaje en cuarentena**

Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.
Configurar la protección del aprendizaje automático mediante el uso de eShell. El nombre de contexto en eShell es **MLP**. Abra eShell en el modo interactivo y vaya a MLP:

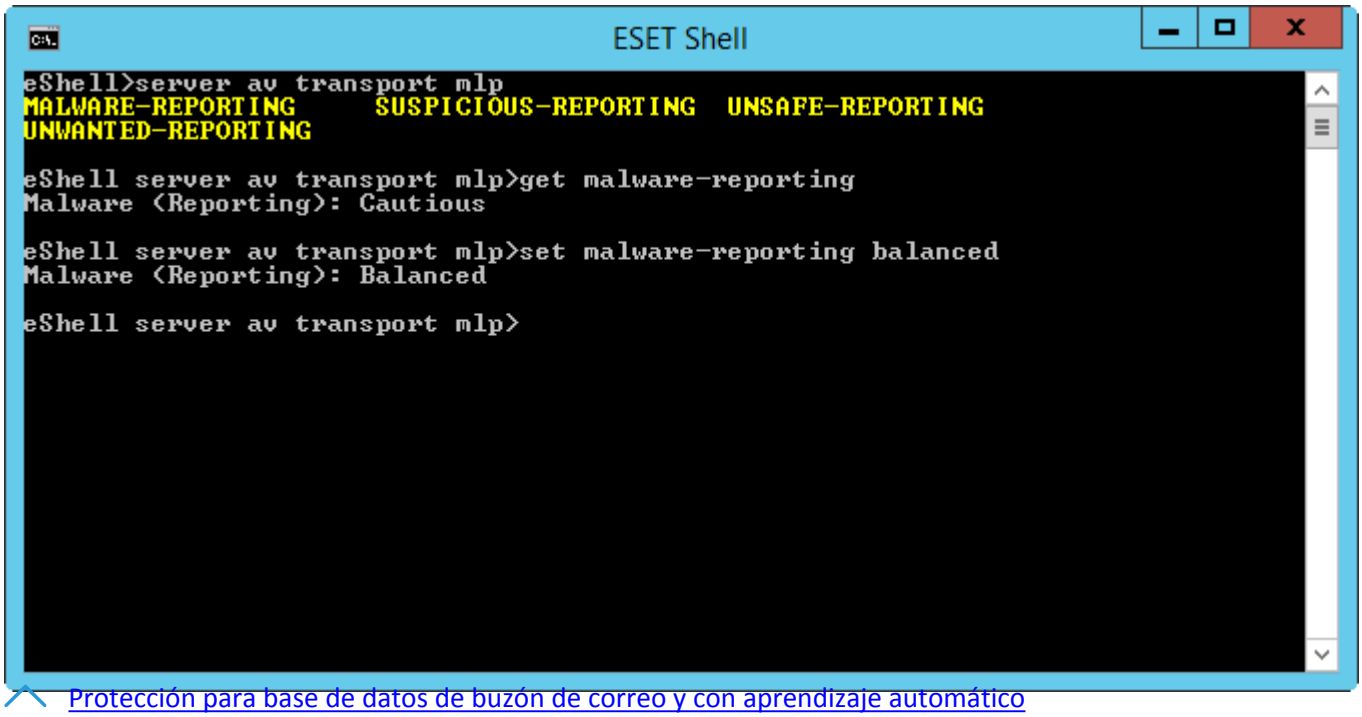
```
server av transport mlp
```

Vea cuál es la configuración actual de informes para aplicaciones sospechosas:

```
get suspicious-reporting
```

Si quiere un informe menos estricto, cambie la configuración a Cauteloso:

```
set suspicious-reporting cautious
```



Protección para base de datos de buzón de correo y con aprendizaje automático

Informar
Llevado a cabo por el motor de detección y el componente de aprendizaje automático. Los informes no ejercen ningún tipo de acción sobre los objetos (esto se lleva a cabo en la capa de protección correspondiente).
Protección
Configure los parámetros en la sección Protección para base de datos de buzón de correo para afectar el tipo de acción que se inicia en relación con los objetos informados.
Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.
Configurar la protección del aprendizaje automático mediante el uso de eShell. El nombre de contexto en eShell es **MLP**. Abra eShell en el modo interactivo y vaya a MLP:
```
server av database mlp
```

Vea cuál es la configuración actual de informes para aplicaciones sospechosas:
```
get suspicious-reporting
```

Si quiere un informe menos estricto, cambie la configuración a Cauteloso:
```
set suspicious-reporting cautious
```

Exploración de la base de datos del buzón de correo a petición y protección con aprendizaje automático

Informar
Llevado a cabo por el motor de detección y el componente de aprendizaje automático. Los informes no ejercen ningún tipo de acción sobre los objetos (esto se lleva a cabo en la capa de protección correspondiente).
Protección
Configure los parámetros en la sección Exploración de la base de datos del buzón de correo a petición para afectar el tipo de acción que se inicia en relación con los objetos informados.
Si desea Revertir las configuraciones de esta sección a sus valores predeterminados, haga clic en la flecha "Giro en U", ubicada junto al encabezado de la sección. Cualquier cambio que haya realizado en esta sección se perderá.
Configurar la protección del aprendizaje automático mediante el uso de eShell. El nombre de contexto en eShell es **MLP**. Abra eShell en el modo interactivo y vaya a MLP:
```
server av on-demand mlp
```

Vea cuál es la configuración actual de informes para aplicaciones sospechosas:
```
get suspicious-reporting
```

Si quiere un informe menos estricto, cambie la configuración a Cauteloso:
```
set suspicious-reporting cautious
```

Exclusiones

Las exclusiones le permiten excluir archivos y carpetas de la exploración. Para asegurarse de que todos los objetos se exploren en busca de amenazas, recomendamos únicamente crear las exclusiones cuando sea absolutamente necesario. Las situaciones donde es posible que necesite excluir un objeto pueden incluir la exploración de las entradas de una base de datos grande que podría reducir la velocidad de su servidor durante una exploración o software que entra en conflicto con la exploración (por ejemplo, un programa de creación de copias de seguridad).

No debe confundirse con extensiones excluidas, exclusiones de procesos o filtro de exclusiones.

una amenaza dentro de un archivo no se detectará por el módulo de protección del sistema de archivos en tiempo real o módulo de exploración del equipo si dicho archivo cumple con los criterios para la exclusión de la exploración.

Seleccione el tipo de exclusiones y haga clic en **Editar** para agregar una nueva o modificar una existente:

- Exclusiones de rendimiento: excluya archivos y carpetas de la exploración.
- Exclusiones de la detección: excluya objetos de la exploración mediante el uso de criterios específicos, como ruta, hash de archivo o nombre de detección.

Exclusiones de rendimiento

Esta función le permite excluir archivos y carpetas de la exploración. Las exclusiones de rendimiento resultan útiles para excluir exploraciones a nivel del archivo de aplicaciones clave para la misión o cuando la exploración produce un comportamiento anormal del sistema o reduce el rendimiento.

Ruta

No incluye la ruta específica (archivo o directorio) para este equipo. No use caracteres globales o asterisco (*) en el medio de la ruta. Para obtener más información, consulte el siguiente Artículo de base de conocimiento .

Para excluir contenidos de una carpeta, no se olvide de agregar el asterisco (*) al final de la ruta (*C:\Tools**).
C:\Tools no se excluirá porque, desde la perspectiva del explorador, las *Herramientas* también pueden ser el nombre de un archivo.

Comentario

Agregue un comentario opcional para reconocer de manera sencilla la exclusión más adelante.

Exclusiones de ruta que usan un asterisco:
C:\Tools* -la ruta debe terminar con una barra invertida (\) y un asterisco (*) para indicar que es una carpeta y todo el contenido de la carpeta (archivos y subcarpetas) se excluirá
C:\Tools*.* - el mismo comportamiento que C:\Tools*, lo que significa que funciona repetidamente
C:\Tools*.dat - excluirá los archivos dat en la carpeta de Herramientas
C:\Tools\sg.dat - excluirá este archivo específico ubicado en la ruta exacta

Para excluir todos los archivos de una carpeta, escriba la ruta de la carpeta y utilice la máscara *.*. Para excluir únicamente los archivos doc, utilice la máscara *.doc.
Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o se desconocen).

Use variables del sistema como %PROGRAMFILES% para definir las exclusiones de la exploración.
Para excluir la carpeta Archivos de programa mediante el uso de la variable del sistema, utilice la ruta %PROGRAMFILES%\ (asegúrese de agregar la barra invertida al final de la ruta al agregar a las exclusiones)
Para excluir todos los archivos en un subdirectorio %HOMEDRIVE%, utilice la ruta %HOMEDRIVE%\Excluded_Directory*.*
Las siguientes variables pueden utilizarse en el formato de exclusión de ruta:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Las variables de sistema específicas del usuario (como %TEMP% o %USERPROFILE%) o las variables del entorno (como %PATH%) no son compatibles.

Exclusiones de detección

Este es otro método para excluir objetos de la exploración mediante el uso del nombre, la ruta o el hash de detección. Las exclusiones de la detección no excluyen archivos y carpetas de la exploración como las Exclusiones de rendimiento. Las exclusiones de la detección excluyen objetos solo cuando el motor de detección los detecta y existe una regla pertinente en la lista de exclusiones.

La manera más sencilla de crear una exclusión basada en la detección es por medio de una detección existente en la sección **Archivos de registro** > Detecciones. Haga clic con el botón secundario en un registro (detección) y, luego, en **Crear exclusión**. De esta manera, se abrirá el asistente de exclusiones con criterios predefinidos.

Para crear manualmente una exclusión de detección, haga clic en **Editar** > **Agregar** (o **Editar** cuando se modifica una exclusión existente) y especifique uno o más de los siguientes criterios (pueden combinarse):

Ruta

No incluye la ruta específica (archivo o directorio). Puede buscar un archivo o una ubicación específicos, o bien, ingresar la secuencia manualmente. No use caracteres globales o asterisco (*) en el medio de la ruta. Para obtener más información, consulte el siguiente Artículo de base de conocimiento .

Para excluir contenidos de una carpeta, no se olvide de agregar el asterisco (*) al final de la ruta (C:\Tools*).
C:\Tools no se excluirá porque, desde la perspectiva del explorador, las *Herramientas* también pueden ser el nombre de un archivo.

Hash

Excluye un archivo basado en un hash especificado (SHA1), sin importar el tipo de archivo, la ubicación, el nombre o la extensión.

Nombre de detección

Ingrese un nombre de detección (amenaza) válido. El hecho de crear una exclusión basada en el nombre de la detección puede representar un riesgo para la seguridad. Recomendamos combinar el nombre de la detección con la ruta. Este criterio de exclusión puede usarse únicamente para ciertos tipos de detecciones.

Comentario

Agregue un **comentario** opcional para reconocer de manera sencilla la exclusión más adelante.

ESET PROTECT incluye la administración de exclusiones de detección para crear exclusiones de detección y aplicarlas a más grupos/equipos.

Puede usar caracteres globales para abarcar un grupo de archivos. Un signo de interrogación (*?*) representa un carácter único variable, mientras que un asterisco (*) representa una cadena variable de cero o más caracteres.

Exclusiones de ruta que usan un asterisco:
C:\Tools* -la ruta debe terminar con una barra invertida (\) y un asterisco (*) para indicar que es una carpeta y todo el contenido de la carpeta (archivos y subcarpetas) se excluirá
C:\Tools*.* - el mismo comportamiento que C:\Tools*, lo que significa que funciona repetidamente
C:\Tools*.dat - excluirá los archivos dat en la carpeta de Herramientas
C:\Tools\sg.dat - excluirá este archivo específico ubicado en la ruta exacta

Para excluir una amenaza, ingrese el nombre de detección válido con el siguiente formato:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

Para excluir todos los archivos de una carpeta, escriba la ruta de la carpeta y utilice la máscara *.*. Para excluir únicamente los archivos doc, utilice la máscara *.doc
Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato:
D????.exe (los signos de interrogación sustituyen a los caracteres que faltan o se desconocen).

Use variables del sistema como *%PROGRAMFILES%* para definir las exclusiones de la exploración.
Para excluir la carpeta Archivos de programa mediante el uso de la variable del sistema, utilice la ruta %PROGRAMFILES%\ (asegúrese de agregar la barra invertida al final de la ruta al agregar a las exclusiones)
Para excluir todos los archivos en un subdirectorio %HOMEDRIVE%, utilice la ruta %HOMEDRIVE%\Excluded_Directory*.*
Las siguientes variables pueden utilizarse en el formato de exclusión de ruta:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Las variables de sistema específicas del usuario (como %TEMP% o %USERPROFILE%) o las variables del entorno (como %PATH%) no son compatibles.

Crear asistente de exclusión

La exclusión recomendada se selecciona previamente en función del tipo de detección. Sin embargo, puede especificar aún más los criterios de exclusión para las detecciones. Haga clic en **Modificar criterios**:

- **Archivos exactos**: excluya cada uno de los archivos según su hash SHA-1.
- **Detección**: especifique el nombre de la detección para excluir cada uno de los archivos que contengan dicha exclusión.
- **Ruta + Detección**: especifique el nombre y la ruta de la detección (incluido el nombre de archivo) para excluir cada archivo con una detección situada en la ubicación específica.

Agregue un **comentario** opcional para reconocer de manera sencilla la exclusión más adelante.

Opciones avanzadas

Tecnología Anti-Stealth

Un sofisticado sistema que detecta programas peligrosos como rootkits que se pueden ocultar del sistema operativo. Estos tipos de programas suelen ser indetectables mediante las técnicas estándar.

AMSI

Permita que la Interfaz de exploración antimalware (AMSI) de Microsoft realice la exploración de scripts de Powershell ejecutados por Windows Script Host.

Exclusiones automáticas

Los desarrolladores de aplicaciones y sistemas operativos para servidores recomiendan excluir de la exploración de malware grupos críticos de archivos operativos y carpetas para la mayoría de sus productos. Las exploraciones de malware pueden tener un efecto negativo en el rendimiento de un servidor, que pueden generar conflictos e, incluso, impedir la ejecución de algunas aplicaciones en el servidor. Las exclusiones ayudan a minimizar el riesgo de conflictos potenciales y a incrementar el rendimiento general del servidor mientras se ejecuta un programa anti-malware. Consulte la lista completa de los archivos excluidos desde la exploración de productos de servidor ESET.

La función de exclusiones automáticas se habilita después de activar ESET Mail Security con una licencia válida y realizar la actualización inicial para incluir los módulos más recientes.

> Las exclusiones automáticas de los archivos de base de datos de Microsoft SQL Server funcionan para la ubicación predeterminada. Si tiene bases de datos de Microsoft SQL Server en ubicaciones distintas (diferentes de las predeterminadas), tiene dos opciones. Agregar manualmente las exclusiones o excluir automáticamente los archivos de la base de datos. Para la exclusión automática, ESET Mail Security debe tener acceso de lectura a la instancia de Microsoft SQL Server para detectar las rutas de acceso que se usan para los archivos de base de datos. Si ESET Mail Security muestra un mensaje de error de derechos insuficientes, resuélvalo y conceda a la cuenta NO_AUTHORITY\SYSTEM el permiso **Ver cualquier permiso** de definición a cada instancia de Microsoft SQL Server que ejecute en el servidor con ESET Mail Security. Para obtener más información, consulte el artículo de la base de conocimiento sobre cómo agregar permisos para obtener ubicaciones de datos de base de datos para generar exclusiones automáticas para Microsoft SQL Server.

ESET Mail Security identifica las aplicaciones críticas del servidor y los archivos críticos del sistema operativo, y los agrega automáticamente a la lista de Exclusiones. Todas las exclusiones automáticas están habilitadas de forma predeterminada. Puede habilitar o deshabilitar cada aplicación del servidor con un clic en la barra deslizante con el siguiente resultado:

- Cuando se habilita, se agregará cualquiera de sus carpetas o archivos críticos a la lista de archivos excluidos de la exploración. Cada vez que se reinicia el servidor, el sistema realiza una verificación automática de exclusiones y restaura cualquier exclusión que pueda haber sido eliminada de la lista (por ejemplo, cuando se instaló una nueva aplicación para el servidor). Esta configuración garantiza que siempre se apliquen las exclusiones automáticas recomendadas.

- Cuando se deshabilita, se eliminan de la lista los archivos y las carpetas excluidos automáticamente. Las exclusiones definidas por el usuario que se ingresaron de forma manual no se verán afectadas.

Las exclusiones automáticas para servidores de Exchange se basan en las recomendaciones de Microsoft. ESET Mail Security se aplica en "Directorio/Carpeta de exclusiones " solamente ("Exclusiones de proceso" y "Exclusiones de extensión de nombre de archivo" no se aplican). Lea los siguientes artículos de la base de conocimiento de Microsoft para obtener más información:

Actualización sobre las exclusiones del antivirus de Exchange Server

Recomendaciones de exploración de virus para computadoras Enterprise que actualmente ejecutan versiones compatibles de Windows.

Exploración de antivirus a nivel de archivo en Exchange 2010

Software antivirus en el sistema operativo en Exchange Servers (Exchange 2013)

Ejecución de software antivirus de Windows en servidores de Exchange 2016

> Además, existen exclusiones de archivos en bases de datos Exchange para bases de datos activas y pasivas en DAG (Grupo de disponibilidad de base de datos) alojadas en un servidor local. La lista de exclusiones automáticas se actualiza cada 30 minutos. Si se crea un nuevo archivo de base de datos de Exchange, se excluirá automáticamente independientemente de su estado, ya sea activo o pasivo.

Para identificar y generar exclusiones automáticas, ESET Mail Security utiliza la aplicación dedicada eAutoExclusions.exe, ubicada en la carpeta de instalación. Usted no necesita hacer nada, pero puede usar la línea de comandos para enumerar las aplicaciones del servidor detectadas en su sistema si ejecuta eAutoExclusions.exe -servers. Para la sintaxis completa, utilice `eAutoExclusions.exe -?`.

Detección de una infiltración

Las infiltraciones pueden llegar al sistema desde diversos puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Conducta estándar

Como ejemplo general de la forma en que ESET Mail Security maneja las infiltraciones, estas se pueden detectar mediante:

- Protección del sistema de archivos en tiempo real
- Protección del acceso a la Web
- Protección del cliente de correo electrónico
- Exploración del equipo a petición

Cada uno usa el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Una ventana de notificación se muestra en el área de notificaciones en la esquina inferior derecha de la pantalla. Para obtener más información sobre los niveles de desinfección y conducta, consulte Desinfección.

Desinfección y eliminación

Si no hay ninguna acción predefinida para la protección del sistema de archivos en tiempo real, el programa le pedirá que seleccione una opción en una ventana de alerta. Por lo general están disponibles las opciones **No infectados**, **Eliminar** y **Sin acción**. No se recomienda seleccionar **Sin acción**, ya que esto dejará los archivos infectados sin desinfectar. La excepción a este consejo es cuando usted está seguro de que un archivo es inofensivo y fue detectado por error.

Aplique la opción de desinfección si un virus atacó un archivo y le adjuntó códigos maliciosos. Si este es el caso, intente limpiar el archivo infectado para restaurarlo a su estado original antes de limpiarlo. Si el archivo está compuesto exclusivamente por códigos maliciosos, será eliminado.

Si un archivo infectado está “bloqueado” u otro proceso del sistema lo está usando, por lo general se elimina cuando es liberado (normalmente luego del reinicio del sistema).

Varias amenazas

Si algún archivo infectado no se desinfectó durante la exploración del equipo (o el Nivel de desinfección estaba configurado en **Sin desinfección**), se muestra una ventana de alerta que le solicitará seleccionar las acciones para dichos archivos.

Seleccione una acción individualmente para cada amenaza de la lista o puede usar **Seleccione una acción para todas las amenazas de la lista** y seleccionar una acción para aplicar a todas las amenazas de la lista, y después haga clic en **Finalizar**.

Eliminación de archivos en archivos comprimidos

En el modo de desinfección predeterminado, se eliminará el archivo comprimido completo solo si todos los archivos que lo componen están infectados. En otras palabras, los archivos comprimidos no se eliminan si

también contienen archivos inofensivos no infectados.

Tenga precaución al realizar una exploración con Desinfección estricta: si la Desinfección estricta está habilitada, un archivo se eliminará si al menos contiene un archivo infectado, sin importar el estado de los demás archivos que lo componen.

Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos del sistema relacionados con el antivirus. Se exploran todos los archivos en busca de códigos maliciosos cuando se abren, se crean o se ejecutan en el equipo. De manera predeterminada, la protección del sistema de archivos en tiempo real se activa junto con el inicio del sistema y ofrece análisis ininterrumpido.

En casos especiales (por ejemplo, si existe un conflicto con otro explorador en tiempo real), se puede deshabilitar la protección en tiempo real quitando **Iniciar automáticamente la protección del sistema de archivos en tiempo real** en **Configuración avanzada** (**F5**) de **Protección del sistema de archivos en tiempo real** > **Básico**.

ESET Mail Security es compatible con equipos que usan el agente Azure File Sync con la nube por niveles activada. ESET Mail Security reconoce archivos con el atributo *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Medios para explorar

En forma predeterminada, todos los tipos de medios se exploran en busca de amenazas potenciales:

- **Unidades locales**: controla todos los discos rígidos del sistema.
- **Medios extraíbles**: controla los CD/DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.
- **Unidades de red**: explora todas las unidades asignadas.

Recomendamos que use la configuración predeterminada y solo modificarla en los casos específicos, por ejemplo, si al explorar ciertos medios, se ralentizan significativamente las transferencias de archivos.

Explorar al

En forma predeterminada, se exploran todos los archivos cuando se abren, se crean o se ejecutan. Se recomienda mantener estas configuraciones predeterminadas, ya que proveen el máximo nivel de protección en tiempo real del equipo:

- **Abrir el archivo**: la exploración se realiza cuando se abren los archivos o se accede a estos.
- **Crear el archivo**: la exploración se realiza cuando se crean o se modifican los archivos.
- **Ejecutar el archivo**: se realiza la exploración cuando se ejecutan los archivos.
- **Acceder a medios extraíbles**: se realiza la exploración cuando se accede al almacenamiento extraíble. Cuando los medios extraíbles que contienen un sector de inicio se insertan en el dispositivo, el sector de inicio se explora de inmediato. Esta opción no permite la exploración de archivos de medios extraíbles. La exploración de archivos de medios extraíbles se encuentra ubicada en **Medios para explorar** > **Medios extraíbles**. Para que el sector de inicio de los medios extraíbles funcione correctamente, conserve Sectores de inicio/UEFI habilitados en los parámetros de ThreatSense.

Exclusiones de procesos

Le permiten excluir procesos específicos. Por ejemplo, los procesos de la solución de copias de respaldo, todas las operaciones de archivos atribuidas a dichos procesos excluidos se ignoran y se consideran seguras, minimizando de esta manera la interferencia con los procesos de copia de respaldo.

ThreatSense parámetros

La protección del sistema de archivos en tiempo real verifica todos los tipos de medios y se acciona por diversos eventos del sistema, como acceder a un archivo. La protección del sistema de archivos en tiempo real se puede configurar para manejar los archivos creados recientemente de un modo diferente a los archivos ya existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para controlar más de cerca a los archivos creados recientemente.

Para asegurar el mínimo impacto en el sistema al usar la protección en tiempo real, los archivos que ya se exploraron no se vuelven a explorar reiteradamente (a menos que se hayan modificado). Los archivos se vuelven a explorar de inmediato luego de cada actualización de la base de datos del motor de detección. Este comportamiento se controla mediante el uso de la **Optimización inteligente**. Si se deshabilita la **Optimización inteligente**, se exploran todos los archivos cada vez que se accede a ellos.

Para modificar esta configuración, presione **F5** para abrir **Configuración avanzada** y expandir **Computer** > **Protección del sistema de archivos en tiempo real**. Haga clic en **ThreatSense parámetros de** > **Otros** y seleccione o anule la selección de **Habilitar la optimización inteligente**.

Parámetros ThreatSense adicionales

Puede modificar las opciones detalladas de los parámetros **adicionales ThreatSense de los archivos creados y modificados recientemente** o los parámetros **adicionales ThreatSense de los archivos ejecutados**.

ThreatSense parámetros

ThreatSense es una tecnología conformada por muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también brinda protección durante las primeras horas de propagación de una nueva amenaza. usa una combinación de la exploración del código, la emulación del código, las firmas genéricas y las firmas de virus que funcionan conjuntamente para mejorar en forma significativa la seguridad del sistema. El motor de exploración cuenta con la capacidad de controlar varios flujos de datos simultáneamente, lo que maximiza la eficiencia y la tasa de detección. La tecnología ThreatSense también elimina con éxito los rootkits.

> i para más detalles sobre la verificación de archivos de inicio, consulte Exploración de arranque.

Las opciones de configuración del motor ThreatSense permiten especificar varios parámetros de exploración:

- los tipos de archivos y las extensiones que se van a explorar;
- La combinación de diversos métodos de detección.
- Los niveles de desinfección, etc.

Para ingresar a la ventana de configuración, haga clic en**ThreatSense Configuración de los parámetros del motor** en la ventana de **Configuración avanzada** (**F5**) de cualquier módulo que use la tecnología ThreatSense (ver abajo).

Diferentes escenarios de seguridad pueden requerir distintas configuraciones. Por ese motivo, ThreatSense puede configurarse en forma individual para cada uno de los siguientes módulos de protección:

- Protección del transporte de correo electrónico
- Protección de la base de datos del buzón de correo a petición
- Protección de la base de datos de correo electrónico
- Exploración Hyper-V
- Protección del sistema de archivos en tiempo real
- Exploración de malware
- Exploración en estado inactivo
- Exploración al inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del acceso a la Web

Los parámetros de ThreatSense están sumamente optimizados para cada módulo y su modificación puede afectar el funcionamiento del sistema en forma significativa. Por ejemplo, la modificación de los parámetros para que siempre se exploren los empaquetadores de tiempo de ejecución, o la habilitación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían ralentizar el sistema (normalmente, solo los nuevos archivos creados se exploran con estos métodos). En consecuencia, es recomendable mantener los parámetros predeterminados de ThreatSense sin modificaciones en todos los módulos excepto para la exploración del equipo.

Objetos para explorar

Esta sección le permite definir qué componentes y archivos del equipo se explorarán en busca de infiltraciones.

Memoria operativa

Explora en busca de amenazas que atacan la memoria operativa del sistema.

Sectores de inicio/UEFI

Explora los sectores de inicio para detectar la presencia de virus en el MBR (Master Boot Record). En caso de una máquina virtual de Hyper-V, el MBR de su disco se explora en el modo solo lectura.

Base de datos WMI

Explora toda la base de datos de WMI en busca de referencias a archivos infectados o malware incrustados como datos.

Registro del sistema

Explora todo el registro del sistema, todas las claves y las subclaves en busca de referencias a archivos infectados o malware incrustados como datos.

Archivos de correo electrónico

El programa es compatible con las siguientes extensiones: DBX (Outlook Express) y EML.

Archivos

El programa es compatible con las siguientes extensiones: *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE*, entre muchas otras.

Archivos comprimidos de autoextracción

Los archivos comprimidos de autoextracción (SFX) son archivos comprimidos que no necesitan ningún programa de extracción especializado para descomprimirse.

Empaquetadores de tiempo de ejecución

Después de su ejecución, los empaquetadores de tiempo de ejecución (a diferencia de los tipos de archivos comprimidos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el explorador puede reconocer varios tipos de empaquetadores adicionales mediante el uso de la emulación del código.

> En el caso de la protección de la base de datos del buzón de mensajes, los archivos de correo electrónico como datos adjuntos (por ejemplo *.eml files*) se exploran independientemente de la configuración bajo **Objetos para explorar**. Esto se debe a que el Servidor de Exchange analiza los datos adjuntos .eml antes de enviarlo a ESET Mail Security para que lo explore. El complemento VSAPI obtiene los archivos extraídos de los datos adjuntos del .eml en lugar de recibir el archivo .eml original.

Opciones de exploración

Seleccione los métodos usados al explorar el sistema en busca de infiltraciones. Se encuentran disponibles las siguientes opciones:

Heurística

La heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La ventaja principal de esta tecnología radica en su capacidad de identificar software malicioso que antes no existía o que no era reconocido por el motor de detección anterior.

Heurística avanzada/ADN inteligentes

La heurística avanzada está compuesta por un algoritmo heurístico exclusivo, desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos que fueron creados con lenguajes de programación de última generación. El uso de la heurística avanzada incrementa significativamente la capacidad de detección de amenazas de los productos de ESET. Las firmas tienen la capacidad de detectar e identificar los virus en forma confiable. Mediante el uso del sistema de actualizaciones automáticas, las nuevas firmas están disponibles en el transcurso de unas pocas horas tras el descubrimiento de una amenaza. La desventaja de las firmas es que solo detectan los virus que ya conocen (o las versiones ligeramente modificadas de estos virus).

Limpieza

La configuración de limpieza determina el comportamiento del explorador durante la limpieza de archivos infectados. La protección en tiempo real y otros módulos de protección tienen los siguientes niveles de corrección (es decir, limpieza).

Reparar siempre la detección

Intentar corregir la detección durante la limpieza de objetos sin la intervención del usuario. Los archivos del sistema son una excepción. Estos objetos se dejan en su ubicación original si no se puede corregir la detección.

Reparar detección si es seguro. Caso contrario, conservar

Intentar corregir la detección durante la limpieza de objetos sin la intervención del usuario. Si no se puede corregir una detección de archivos o archivos comprimidos del sistema (con archivos limpios e infectados), el objeto informado se conserva en su ubicación original.

Reparar detección si es seguro. Caso contrario, consultar

Intentar corregir la detección durante la limpieza de objetos. En algunos casos, si ESET Mail Security no puede realizar una acción automática, se le pedirá que elija una acción (quitar o ignorar). Esta configuración se recomienda en la mayoría de los casos.

Preguntar siempre al usuario final

ESET Mail Security no realizará ninguna acción automática. Se le pedirá que elija una acción.

Exclusiones

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Una extensión define el tipo de archivo y su contenido. Esta sección de la configuración de los parámetros de ThreatSense permite definir los tipos de archivos a excluir de la exploración.

Otros

Cuando se configuran los valores de los parámetros del motor ThreatSense para una exploración del equipo a petición, las siguientes opciones en la sección **Otros** también están disponibles:

Explorar secuencias de datos alternativas (ADS)

Las secuencias de datos alternativas usadas por el sistema de archivos NTFS constituyen asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración. Muchas infiltraciones intentan evitar la detección camuflándose como secuencias de datos alternativas.

Ejecutar exploraciones en segundo plano con baja prioridad

Cada secuencia de exploración consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para los recursos del sistema, es posible activar la exploración en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.

Registrar todos los objetos

Si se selecciona esta opción, el archivo de registro mostrará todos los archivos explorados, incluso los que no estén infectados.

Habilitar la optimización inteligente

Cuando la opción para habilitar la optimización inteligente está seleccionada, se usa la configuración favorable para garantizar el nivel de exploración más eficiente, al mismo tiempo que mantiene la mayor velocidad de exploración. Los diversos módulos de protección realizan exploraciones en forma inteligente; para ello emplean distintos métodos de exploración y los aplican a tipos de archivos específicos. Si se deshabilita la Optimización inteligente, solo se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos específicos al realizar una exploración.

Preservar el último acceso con su fecha y hora

Seleccione esta opción para preservar la hora de acceso original a los archivos explorados en vez de actualizarla (por ejemplo, para usarlos con sistemas que realizan copias de seguridad de datos).

Límites

La sección Límites permite especificar el tamaño máximo de los objetos y los niveles de los archivos comprimidos anidados que se explorarán:

Configuración predeterminada del objeto

Habilitar para utilizar la configuración predeterminada (sin límites). ESET Mail Security ignorará la configuración personalizada.

Tamaño máximo del objeto

Define el tamaño máximo de los objetos que se van a explorar. El módulo de protección determinado explorará solamente los objetos con un tamaño inferior al especificado. Los únicos que deberían modificar esta opción son los usuarios avanzados que tengan motivos específicos para excluir objetos de mayor tamaño de la exploración. Valor predeterminado: ilimitado.

Tiempo máximo de exploración para el objeto (seg.)

Define el valor máximo de tiempo para explorar un objeto. Si en esta opción se ingresó un valor definido por el usuario, el módulo de protección detendrá la exploración de un objeto cuando haya transcurrido dicho tiempo, sin importar si finalizó la exploración. Valor predeterminado: ilimitado.

Configuración de la exploración de archivos comprimidos

Para modificar la configuración de la exploración del archivo, anule la selección de **Configuración predeterminada para la exploración de archivos comprimidos**.

Nivel de anidado de archivos comprimidos

Especifica la profundidad máxima de la exploración de archivos comprimidos. Valor predeterminado: 10. Para objetos detectados por la protección de transporte del buzón de correo, el nivel de anidado real es +1 porque un archivo adjunto en un correo electrónico se considera de primer nivel.

> ✓ Si tiene el nivel de anidado configurado en 3, un archivo con un nivel de anidado 3 solo se examinará en una capa de transporte hasta su nivel 2 real. Por lo tanto, si desea que la protección de transporte de buzón de correo lo analice hasta el nivel 3, configure el valor de **nivel de anidado de archivo** a 4.

Tamaño máximo del archivo incluido en el archivo comprimido

Esta opción permite especificar el tamaño máximo de los archivos incluidos en archivos comprimidos (al extraerlos) que se explorarán. Valor predeterminado: ilimitado.

> i no se recomienda cambiar los valores predeterminados; en circunstancias normales, no existe ninguna razón para modificarlos.

Parámetros ThreatSense adicionales

Parámetros adicionales ThreatSense para archivos creados o modificados recientemente

La probabilidad de infección de los nuevos archivos creados o en los modificados es mayor al compararla con la correspondiente a los archivos existentes. Por ese motivo, el programa verifica esos archivos con parámetros adicionales de exploración. Junto con los métodos comunes de exploración basados en firmas, se utiliza la heurística avanzada, que puede detectar las nuevas amenazas antes del lanzamiento de la actualización del módulo. Además de los nuevos archivos creados, la exploración se realiza en los archivos de autoextracción (.sfx) y los empaquetadores de tiempo de ejecución (archivos ejecutables comprimidos internamente).

En forma predeterminada, los archivos comprimidos se exploran hasta el décimo nivel de anidado y se verifican independientemente de su tamaño real. Para modificar la configuración de la exploración de los archivos comprimidos, desactive **Configuración predeterminada para la exploración de archivos comprimidos**.

Parámetros adicionales ThreatSense para los archivos ejecutados

En forma predeterminada, la Heurística avanzada se utiliza cuando se ejecutan los archivos. Cuando está habilitada, recomendamos firmemente mantener la Optimización inteligente y ESET LiveGrid® habilitados para mitigar el impacto en el rendimiento del sistema.

Extensiones de archivos que no se analizarán

Una extensión es la parte delimitada por un punto en el nombre de un archivo. Esa extensión define el tipo de archivo. Normalmente, se analizan todos los archivos. Sin embargo, si desea excluir archivos con una extensión específica, la configuración de parámetros de ThreatSense le permite excluir los archivos que no desea analizar según su extensión. La exclusión puede ser útil si el análisis de ciertos tipos de archivos impide que una aplicación se ejecute correctamente.

Para añadir una nueva extensión a la lista, haga clic en **Agregar**. Escriba la extensión en el campo de texto (por ejemplo tmp) y haga clic en **OK**. Al seleccionar **Introduzca múltiples valores**, puede agregar varias extensiones de archivos delimitadas por líneas, comas o punto y coma (por ejemplo, seleccione **Punto y coma** del menú desplegable como separador y escriba `edb;eml;tmp`).
Puede usar el símbolo especial ? (signo de interrogación). El signo de interrogación representa cualquier símbolo (por ejemplo, `?db`).

Para mostrar la extensión (tipo de archivo) de todos los archivos en un sistema operativo Windows, desmarque la casilla **Ocultar extensiones de todos tipos de archivos conocidos** en **Panel de control** > **Opciones de carpeta** > **Ver**.

Exclusiones de procesos

La función Exclusión de procesos permite excluir los procesos de las aplicaciones únicamente del análisis en tiempo real de antimalware. Debido al rol crítico de los servidores dedicados (servidor de aplicación, servidor de almacenamiento, etc.) las copias de respaldo periódicas son obligatorias para garantizar la recuperación oportuna de un incidente de cualquier tipo.

Para mejorar la velocidad de las copias de respaldo, la integridad del proceso y la disponibilidad del servicio, durante las copias de respaldo se utilizan algunas técnicas que son conocidas por entrar en conflicto con la protección del malware a nivel del archivo. Pueden ocurrir problemas similares cuando se intentan realizar migraciones en vivo en máquinas virtuales.

La única manera efectiva de evitar ambas situaciones es desactivar el software Anti-Malware. Al excluir los procesos específicos (por ejemplo, aquellos de la solución de copias de respaldo) todas las operaciones de archivos atribuidas a dichos procesos excluidos se ignorarán y se considerarán seguras, minimizando de esta manera la interferencia con los procesos de copia de respaldo. Le recomendamos que tenga precaución cuando cree exclusiones; una herramienta de copia de respaldo que haya sido excluida podrá acceder a los archivos infectados sin activar una alerta, motivo por el cual los permisos extendidos solamente se permiten en el módulo de protección en tiempo real.

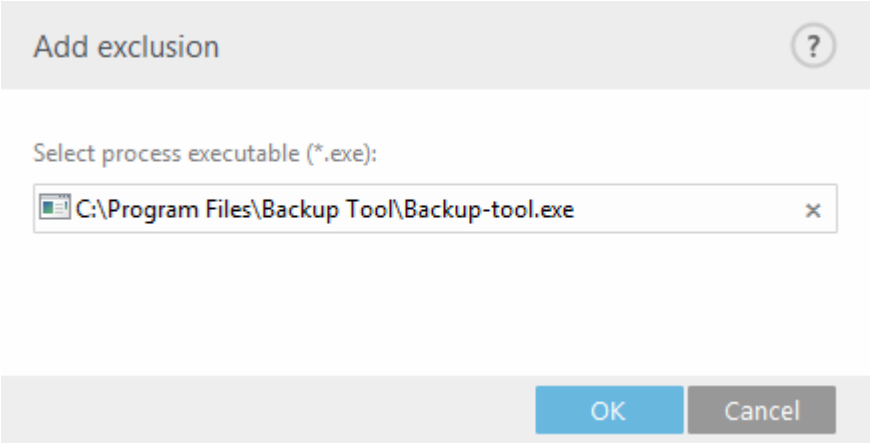
Las Exclusiones de procesos ayudan a minimizar el riesgo de conflictos potenciales y a mejorar el rendimiento de aplicaciones excluidas, lo que a su vez tiene un efecto positivo sobre el rendimiento general y la estabilidad del sistema operativo. La exclusión de un proceso/aplicación es una exclusión de su archivo ejecutable (*.exe*).

Puede agregar archivos ejecutables a la lista de procesos excluidos mediante la **Configuración avanzada (F5)** > **Computer** > **Protección del sistema de archivos en tiempo real** > **Básica** > **Exclusiones de procesos** o use la lista de procesos en ejecución del menú principal en **Herramientas** > **Procesos en ejecución**.

El objetivo de esta función es excluir las herramientas de copia de seguridad. Excluir el proceso de la herramienta de copia de seguridad del análisis no solamente garantiza la estabilidad del sistema, sino que tampoco afecta al rendimiento de la copia de seguridad, ya que ésta no se ralentiza mientras se está ejecutando.

Haga clic en **Editar** para abrir la ventana de administración de **Exclusiones de procesos**, en la que puede **Agregar** exclusiones y busque el archivo ejecutable (por ejemplo, Backup-tool.exe), que se excluirá de la exploración.
Apenas se agrega el archivo *.exe* a las exclusiones, la actividad de este proceso no es monitoreada por ESET Mail Security y no se realiza ninguna exploración sobre ninguna operación de archivo realizada por el proceso.

Si no utiliza la función de exploración al seleccionar el ejecutable del proceso, deberá introducir manualmente una ruta completa al ejecutable. De lo contrario, la exclusión no funcionará correctamente y HIPS puede informar de errores.



También puede **Editar** los procesos existentes o **Eliminarlos** de las exclusiones.

La protección de acceso a la web no toma en cuenta esta exclusión, entonces, si excluye el archivo ejecutable de su navegador web, los archivos descargados aún se explorarán. De esta manera, las infiltraciones podrán detectarse de todos modos. Esta situación representa solamente un ejemplo, y no recomendamos crear exclusiones para los navegadores web.

Protección basada en la nube

ESET LiveGrid® es un sistema avanzado de alerta temprana compuesto por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes en base a la reputación y mejora el rendimiento de las exploraciones por medio de las listas blancas. La información de la amenaza nueva se transmite en tiempo real a la nube, lo que le permite al Laboratorio de búsqueda de malware de ESET proporcionar una respuesta oportuna y una protección consistente en todo momento. Los usuarios pueden verificar la reputación de los procesos en ejecución y de los archivos directamente desde la interfaz del programa o desde el menú contextual, con información adicional disponible desde ESET LiveGrid®.

Al instalar ESET Mail Security, seleccione una de las siguientes opciones:

- Puede decidir no habilitar ESET LiveGrid®. Su software no perderá ninguna funcionalidad pero, en algunos casos, ESET Mail Security su respuesta a las amenazas nuevas puede ser más lenta que una actualización de la base de datos del motor de detección.

- Puede configurar ESET LiveGrid® para enviar información anónima sobre las amenazas nuevas y el contexto donde se detectó dicho código. Es posible enviar este archivo a ESET para su análisis detallado. El estudio de estos códigos ayudará a ESET a actualizar su capacidad de detección de amenazas.

ESET LiveGrid® recopilará información sobre el equipo en relación con las nuevas amenazas detectadas. Dicha

información puede incluir una muestra o copia del archivo donde apareció la amenaza, la ruta a ese archivo, el nombre del archivo, la fecha y la hora, el proceso mediante el cual apareció la amenaza y la información sobre el sistema operativo del equipo.

En forma predeterminada, ESET Mail Security está configurado para enviar archivos sospechosos al laboratorio de virus de ESET para su análisis detallado. Los archivos con ciertas extensiones, como .docx o .xlsx, siempre se excluyen. También puede agregar otras extensiones si usted o su organización prefieren no enviar ciertos archivos específicos.

Habilitar el sistema de reputación ESET LiveGrid® (recomendado)

El sistema de reputación ESET LiveGrid® mejora la eficacia de las soluciones antimalware de ESET al comparar los archivos analizados con una base de datos de elementos de listas blancas y negras en la nube.

Habilitar el sistema de retroalimentación ESET LiveGrid®

Se enviarán datos al ESET Research Lab para su análisis posterior.

Enviar informes de error y datos de diagnóstico

Enviar datos tales como informes de errores, módulos o volcados de memorias.

Enviar estadísticas anónimas

Permite que ESET recolecte información anónima sobre amenazas recientemente detectadas, como el nombre de la amenaza, fecha y hora de detección, método de detección y metadatos asociados, archivos explorados (hash, nombre de archivo, origen del archivo, telemetría), URL bloqueadas o sospechosas, versión y configuración del producto, incluida la información sobre su sistema.

Correo electrónico de contacto (opcional)

Puede incluir su correo electrónico junto con los archivos sospechosos, así podrá usarse para contactarlo en caso de que se requiera información adicional para el análisis. Recuerde que no recibirá ninguna respuesta de ESET a menos que se necesite información adicional.

Envío de muestras

Envío automático de muestras infectadas
Enviará todas las muestras infectadas a ESET para su análisis y para mejorar la detección futura.
- Todas las muestras infectadas
- Todas las muestras, excepto los documentos
- No enviar

Envío automático de muestras sospechosas
Las muestras sospechosas que se asemejan a amenazas, y/o muestras con características o comportamientos inusuales se envían a ESET para su análisis.
- **Ejecutables** - Incluye archivos ejecutables: .exe, .dll, .sys
- **Archivos** - Incluye tipos de archivo del agente: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Scripts** - Incluye tipos de archivo de script: .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Otros** - Incluye tipos de archivo:.jar, .reg, .msi, .swf, .lnk
- **Posibles correos electrónicos spam**: mejora la detección global del spam.
- **Documentos** – Incluye documentos de Microsoft Office o PDFs con contenido activo

Exclusiones
Hacer clic en la opción Editar junto a Exclusiones en ESET LiveGrid® le permite configurar la manera en que las amenazas se envían a los laboratorios de virus de ESET para su análisis.
Tamaño máximo de muestras (MB)
Define el tamaño máximo de las muestras a explorar.

ESET LiveGuard Advanced

Para habilitar el servicio ESET LiveGuard Advanced en una máquina del cliente utilizando ESET PROTECT Web Console. En ESET PROTECT Web Console, cree una política nueva o edite una existente y asígnela a las máquinas donde quiere usar ESET LiveGuard Advanced.

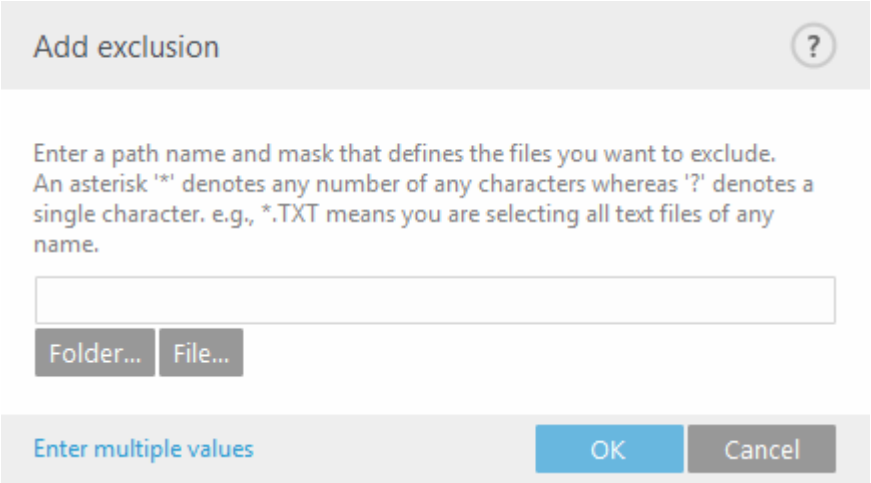
Filtro de exclusión

El filtro de exclusión permite excluir ciertos archivos o carpetas del envío. Por ejemplo, quizá resulte útil excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo.

Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, ni siquiera si contienen código sospechoso.

Los tipos de archivos más comunes se excluyen en forma predeterminada (*.doc*, etc.). Si lo desea, puede agregar archivos a la lista de archivos excluidos.

Si usted ya usó ESET LiveGrid® y lo deshabilitó, es posible que queden paquetes de datos para enviar. Aun después de su desactivación, dichos paquetes se enviarán a ESET. Una vez que se envíe toda la información actual, no se crearán más paquetes.



Si encuentra un archivo sospechoso, puede enviarlo a nuestro laboratorio de amenazas para su análisis. Si se trata de una aplicación maliciosa, se agregará su detección en la siguiente actualización del módulo de detección.

Exploración de malware

Esta sección ofrece opciones para seleccionar los parámetros de exploración.

> Este selector de perfiles de exploración se aplica a la **Exploración a petición** y la Exploración de Hyper-V.

Perfil seleccionado

Un conjunto especial de parámetros utilizados por la exploración a petición. Puede utilizar uno de los perfiles de exploración definidos previamente o crear uno nuevo. Los perfiles de exploración utilizan diferentes parámetros de motores de ThreatSense.

Lista de perfiles

Para crear uno nuevo, haga clic en **Editar**. Ingrese su nombre para el perfil y luego haga clic en **Agregar**. El nuevo perfil se mostrará en el menú desplegable **Perfil seleccionado** que lista los perfiles de exploración existentes.

Objetos para explorar

Para explorar un objeto específico, haga clic en **Editar** y elija una opción del menú desplegable o seleccione los objetos específicos desde la estructura (de árbol) de la carpeta.

ThreatSense parámetros

Modifica los parámetros de exploración para exploración del equipo a petición.

Protección de acuerdo a las necesidades y con aprendizaje automático

El motor de detección y el componente de aprendizaje automático llevan a cabo los informes.

Administrador de perfiles

El menú desplegable Perfil de exploración le permite seleccionar los perfiles predefinidos que se explorarán.

- Exploración inteligente
- Exploración del menú contextual
- Exploración exhaustiva
- Mi perfil (aplicable a exploración de Hyper-V, perfiles de actualización)

Para obtener ayuda sobre cómo crear un perfil de exploración acorde a sus necesidades, consulte la sección Configuración de los parámetros del motor ThreatSense, donde obtendrá la descripción de cada parámetro de la configuración de la exploración.

El administrador de perfiles se utiliza en tres lugares dentro de ESET Mail Security.

Exploración del equipo a petición

Es posible guardar los parámetros preferidos de exploración para usarlos en el futuro. Se recomienda crear un perfil distinto (con varios objetos para explorar, métodos de exploración y otros parámetros) para cada exploración usada regularmente.

Actualización

El editor de perfiles permite a los usuarios crear nuevos perfiles de actualización. Solamente es necesario crear perfiles de actualización personalizados si su equipo usa varios medios para conectarse a los servidores de actualización.

Exploración Hyper-V

Crear un perfil nuevo, seleccione **Editar** junto a **Lista de perfiles**. El nuevo perfil se mostrará en el menú desplegable **Perfil seleccionado** que lista los perfiles de exploración existentes.

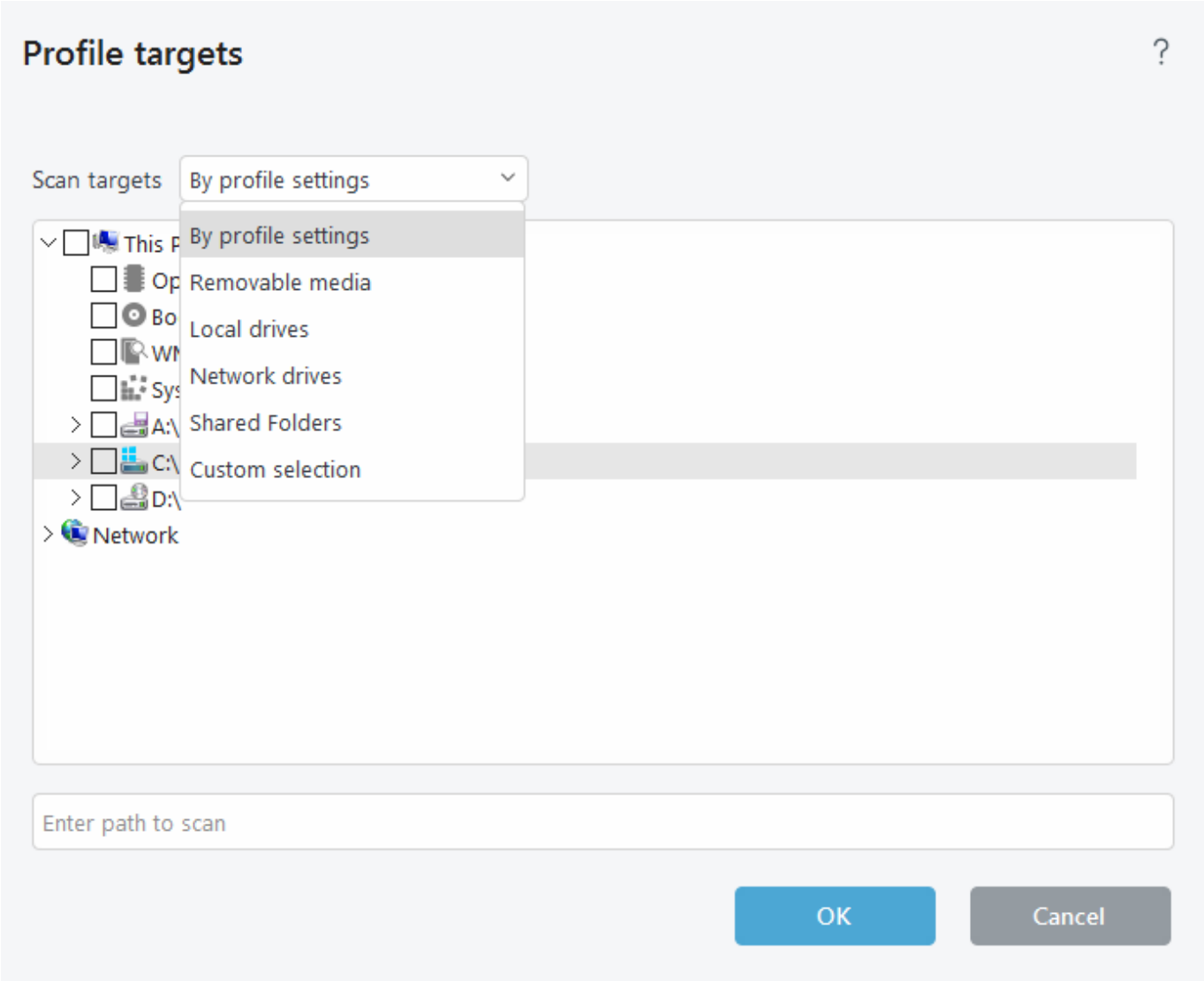
Objetos de perfil

Puede especificar qué se explorará para detectar infiltraciones. Elija objetos (memoria, sectores de arranque y UEFI, unidades, archivos y carpetas o red) de la estructura de árbol que enumera todos los destinos disponibles en su sistema. Haga clic en el ícono del engranaje en la esquina superior izquierda para obtener acceso a los menús desplegables **Destinos de exploración** y **Perfil de exploración**.

Este selector de perfiles de exploración se aplica a la Exploración a petición y la Exploración de Hyper-V.

Memoria operativa	Explora todos los procesos y los datos que utiliza actualmente la memoria operativa.
Sectores de inicio/UEFI	Explora los sectores de inicio y la UEFI en busca de la presencia de malware. Puede obtener más información sobre el Explorador UEFI en el glosario.
Base de datos WMI	Explora toda la base de datos del Instrumental de administración de Windows (WMI), todos los espacios de nombres, todas las clases de instancias y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
Registro del sistema	Explora todo el registro del sistema, todas las claves y las subclaves. Busca referencias a archivos infectados o malware incrustado como datos. Durante la limpieza de las detecciones, la referencia permanece en el registro para asegurarse de que no se pierde ningún dato importante.

Para ir rápidamente a un objeto de exploración o agregar una carpeta o archivo(s) de destino, ingrese el directorio de destino en el campo en blanco situado debajo de la lista de carpetas.



El menú desplegable **Objetos para explorar** le permite seleccionar los objetos predefinidos que se explorarán.

Por configuración de perfil	Selecciona los objetos especificados en el perfil de exploración seleccionado.
Medios extraíbles	Selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.
Unidades locales	Selecciona todas las unidades del disco rígido.
Unidades de red	Selecciona todas las unidades de red asignadas.
Carpetas compartidas	Selecciona todas las carpetas compartidas en el servidor local.
Selección personalizada	Borra todas las selecciones. Una vez borradas, puede hacer su elección personalizada.

Para navegar rápidamente a un objetivo de exploración (archivo o carpeta) con el fin de incluirlo para la exploración, escriba su ruta en el campo de texto debajo de la estructura de árbol. La entrada de la ruta distingue entre mayúsculas y minúsculas.

El menú desplegable **Perfil de exploración** le permite seleccionar los perfiles predefinidos que se explorarán:

- Exploración inteligente
- Exploración del menú contextual

- Exploración exhaustiva
- Exploración del equipo

Estos perfiles de exploración usan diferentes parámetros del motor ThreatSense.

Explorar sin desinfectar

Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione **Explorar sin desinfectar**. Esto es útil cuando solo desea obtener un resumen de si hay elementos infectados y ver los detalles acerca de estas infecciones, si las hay. Puede elegir de entre tres niveles de desinfección al hacer clic en **Configuración** > **ParámetrosThreatSense** > **Desinfección**. La información sobre la exploración se guarda en un registro de exploración.

Ignorar exclusiones

Cuando selecciona Ignorar exclusiones, le permite realizar una exploración mientras ignora exclusiones que de otro modo se aplicarían.

Objetos para explorar

Si solo desea escanear un destino específico, puede utilizar la **Exploración personalizada** y seleccionar una opción en el menú desplegable de **Objetos para explorar** o seleccionar objetivos específicos de la estructura de carpetas (árbol).

El selector de perfil de objetivos para exploración es aplicable a:

- Escaneo a petición
- Exploración Hyper-V

Para ir rápidamente hasta un objeto para explorar o para agregar un objeto o carpeta para explorar, ingréselo en el campo vacío debajo de la lista de carpetas. Esta acción solo será posible si no se seleccionó ningún objeto para explorar en la estructura con forma de árbol y el menú **Objetos para explorar** está configurado en **Sin selección**.

Memoria operativa	Explora todos los procesos y los datos que utiliza actualmente la memoria operativa.
Sectores de inicio/UEFI	Explora los sectores de inicio y la UEFI en busca de la presencia de malware. Puede obtener más información sobre el Explorador UEFI en el glosario.
Base de datos WMI	Explora toda la base de datos del Instrumental de administración de Windows (WMI), todos los espacios de nombres, todas las clases de instancias y todas las propiedades. Busca referencias a archivos infectados o malware incrustados como datos.
Registro del sistema	Explora todo el registro del sistema, todas las claves y las subclaves. Busca referencias a archivos infectados o malware incrustado como datos. Durante la limpieza de las detecciones, la referencia permanece en el registro para asegurarse de que no se pierde ningún dato importante.

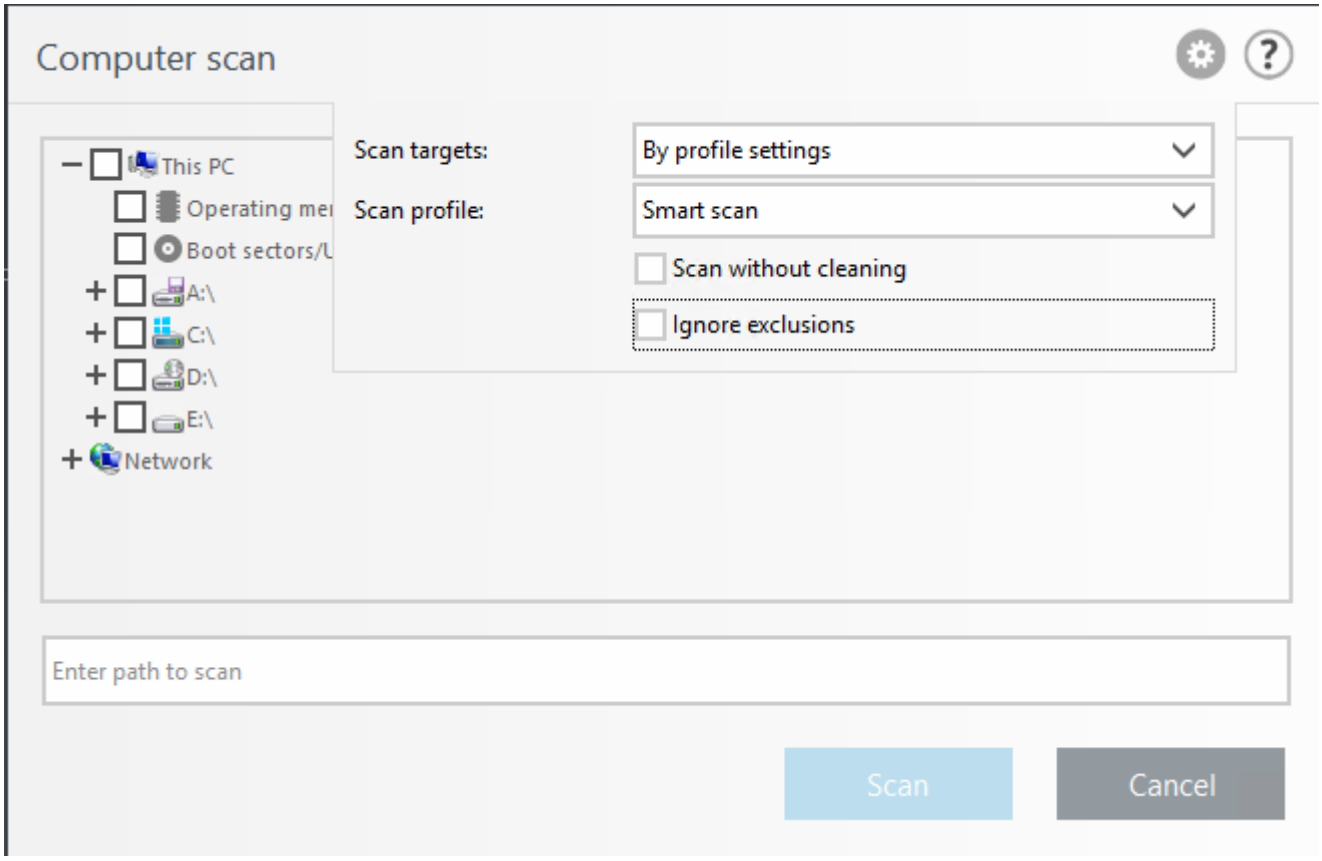
El menú desplegable **Objetos para explorar** le permite seleccionar los objetos predefinidos que se explorarán.

Por configuración de perfil	Selecciona los objetos especificados en el perfil de exploración seleccionado.
Medios extraíbles	Selecciona disquetes, dispositivos de almacenamiento USB, CD, DVD.

Por configuración de perfil	Selecciona los objetos especificados en el perfil de exploración seleccionado.
Unidades locales	Selecciona todas las unidades del disco rígido.
Unidades de red	Selecciona todas las unidades de red asignadas.
Carpetas compartidas	Selecciona todas las carpetas compartidas en el servidor local.
Selección personalizada	Borra todas las selecciones. Una vez borradas, puede hacer su elección personalizada.

En el menú desplegable Perfil de exploración, puede elegir un perfil que podrá usar con los objetos para explorar seleccionados. El perfil predeterminado es Análisis inteligente. El perfil predeterminado es **Análisis inteligente**. Hay otros dos perfiles de exploración predefinidos denominados: Análisis profundo y **Análisis del menú contextual**. Estos perfiles de exploración usan diferentes parámetros del motor ThreatSense.

La ventana **Exploración personalizada**:



Explorar sin desinfectar – Si solo le interesa explorar el sistema sin realizar acciones adicionales de desinfección, seleccione Explorar sin desinfectar. Esto es útil cuando solo desea obtener un resumen de si hay elementos infectados y ver los detalles acerca de estas infecciones, si las hay. Puede elegir de entre tres niveles de desinfección al hacer clic en Configuración > ParámetrosThreatSense > Desinfección. La información sobre la exploración se guarda en un registro de exploración.

Ignorar exclusiones – Le permite realizar una exploración mientras ignora exclusiones que de otro modo se aplicarían.

Acción después de la exploración: elija la acción que desea realizar una vez finalizada la exploración en el menú desplegable.

La exploración no se puede interrumpir: para denegarles a los usuarios sin privilegios la capacidad de detener las medidas que se tomaron luego de la exploración.

El usuario puede pausar la exploración durante (min): permite que el usuario limitado pause la exploración del equipo durante el límite de tiempo especificado.

Interrumpir la exploración automáticamente después de (min): para cancelar la exploración si tarda más que el límite de tiempo especificado.

Analizar como administrador – Permite ejecutar la exploración desde una cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene los privilegios necesarios para acceder a los archivos apropiados que se van a explorar. Tenga en cuenta que este botón no está disponible si el usuario actual no puede realizar operaciones UAC como administrador.

Exploración en estado inactivo

Cuando el equipo está en estado de inactividad, se lleva a cabo una exploración silenciosa del equipo en todas las unidades locales. **La detección en estado inactivo** se ejecutará cuando su equipo se encuentre en los siguientes estados:

- Pantalla apagada o protector de pantalla
- Bloqueo de equipo
- Cierre de sesión de usuario

Ejecutar aunque el equipo esté funcionando con la batería

De forma predeterminada, el escáner del estado de inactividad no funcionará cuando la computadora (portátil) funcione a batería.

Habilitar registro

Para registrar el resultado de la exploración del equipo en la sección Archivos de registro (desde la ventana principal del programa haga clic en Archivos de registro y seleccione el tipo de registro de Exploración del equipo en el menú desplegable).

ThreatSense parámetros

Para modificar los parámetros de exploración para el explorador en estado inactivo.

Exploración en el inicio

En forma predeterminada, la exploración automática de archivos se realizará durante el inicio del sistema (ingreso del usuario) y después de la correcta actualización del módulo. Esta exploración es controlada por la Configuración y las tareas programadas.

Las opciones de exploración en el inicio son parte de las tareas programadas de **Verificación de archivos de inicio del sistema**.

Para modificar las Configuraciones de exploración en el inicio, navegue a **Herramientas** > **Tareas programadas**, seleccione una de las tareas llamada **Exploración automática de archivos durante el inicio del sistema** (inicio de sesión del usuario o actualización de módulo) y haga clic en **Editar**. En el último paso haga clic en el asistente,

donde podrá modificar las opciones detalladas de la Exploración automática de archivos durante el inicio del sistema.

Verificación de archivos de inicio automática

Al crear una tarea programada de verificación de archivos de inicio del sistema, tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Objetos para explorar** especifica la profundidad de la exploración para la ejecución de archivos al inicio del sistema. Los archivos se organizan en orden ascendente de acuerdo con el siguiente criterio:

- Todos los archivos registrados (la mayoría de archivos explorados)
- Archivos poco usados
- Archivos usados habitualmente
- Archivos de uso más frecuente
- Solo los archivos más frecuentemente usados (los archivos menos explorados)

También se incluyen dos grupos específicos de Objetos para explorar:

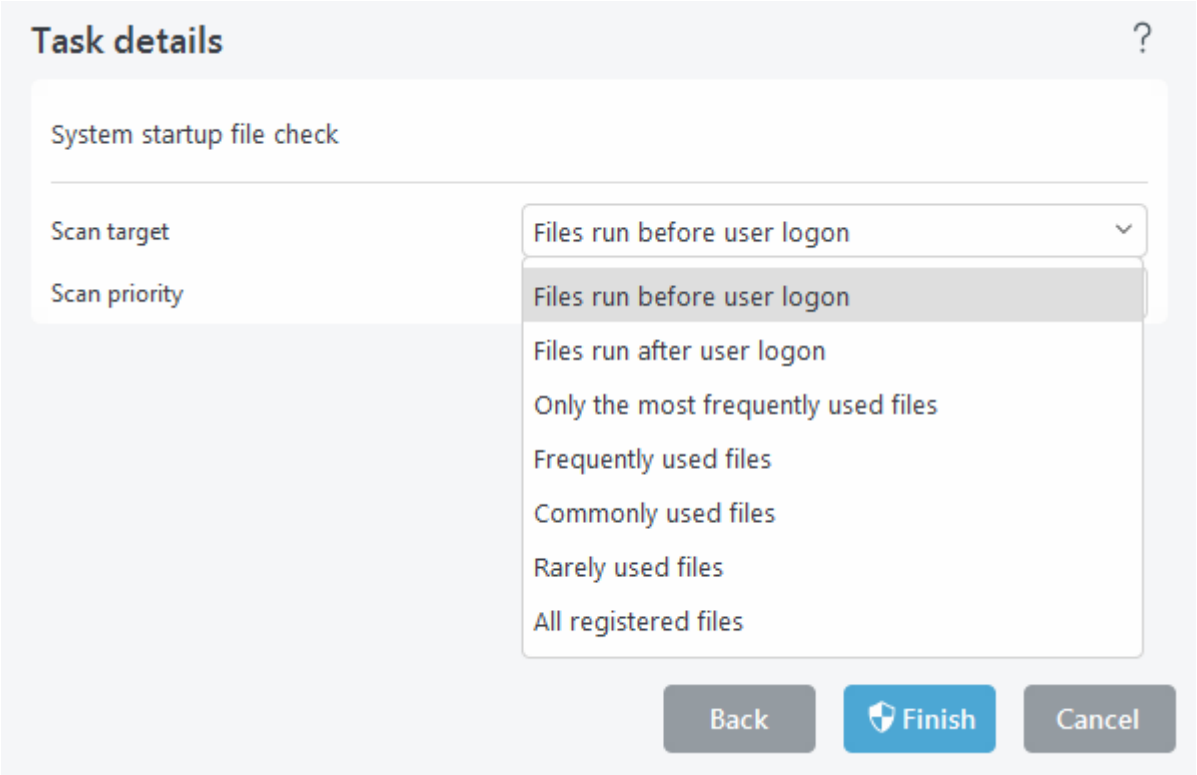
Archivos ejecutados antes del inicio de sesión del usuario

Contiene archivos de las ubicaciones a las que puede accederse sin que el usuario se registre (incluye casi todas las ubicaciones de inicio tales como servicios, objetos del ayudante de exploración, winlogon notify, entradas de las tareas programadas de Windows, dll conocidos, etc.).

Archivos ejecutados después del inicio de sesión del usuario

Contiene archivos de las ubicaciones a las que puede accederse solo después de que un usuario se registre (incluye archivos que solo se ejecutan para un usuario específico, por lo general archivos en *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de archivos a escanear son fijas para cada grupo antes mencionado.



Prioridad de exploración:

El nivel de prioridad usado para determinar cuándo se iniciará una exploración:

- **Normal**: en una carga promedio del sistema,
- **Inferior**: en una carga baja del sistema,
- **Más baja**: cuando la carga del sistema es lo más baja posible,
- **Cuando está inactivo**: la tarea se realizará solo cuando el sistema esté inactivo.

Medios extraíbles

ESET Mail Security proporciona la exploración automática de los medios extraíbles (CD/DVD/USB). Este módulo le permite explorar los medios insertados. Resulta útil si el administrador del equipo desea prevenir que los usuarios usen los medios extraíbles con contenido no solicitado.

Cuando se inserten los medios extraíbles, se mostrará el siguiente cuadro de diálogo:

- **Explorar ahora** – desencadenará la exploración de los medios extraíbles.
- **No explorar**: no se explorarán los medios extraíbles.
- **Configuración**: abre la Configuración avanzada.
- **Usar siempre la opción seleccionada**: cuando se seleccione, se llevará a cabo la misma acción cuando se inserte un medio extraíble en el futuro.

Además, ESET Mail Security presenta la función Control de dispositivos, que le permite definir las reglas para el uso de dispositivos externos en un equipo determinado.

Para acceder a la configuración de la exploración de medios extraíbles, abra **Configuración avanzada** (**F5**) **Notificaciónes** > **Alertas interactivas** > **Editar**. Si **Preguntar al usuario** no está seleccionado, elija la acción que se realizará cuando se inserte un medio extraíble en el equipo:

- **No explorar** – no se realizará ninguna acción y se cerrará la ventana Se detectó **un nuevo dispositivo**.
- **Exploración automática del dispositivo** – se llevará a cabo una exploración del equipo a petición en los dispositivos de medios extraíbles insertados.
- **Exploración forzada del dispositivo**: se realizará una exploración del equipo del medio extraíble insertado y no se podrá cancelar.
- **Mostrar opciones de exploración**: abre la sección de configuración de **Alertas interactivas**.

Protección de documentos

La función para la protección de documentos explora los documentos de Microsoft Office antes de que se abran, así como los archivos descargados automáticamente por Internet Explorer, por ej., los elementos ActiveX de Microsoft. La protección de documentos proporciona un nivel de protección adicional a la protección del sistema de archivos en tiempo real. Puede deshabilitarse para mejorar el rendimiento en los sistemas que no están expuestos a un alto volumen de documentos de Microsoft Office.

Integrar al sistema

Esta opción mejora la protección de documentos de Microsoft Office (no es necesaria en circunstancias normales).

ThreatSense parámetros

Modifica los parámetros para la protección de documentos.

> i Esta función se activa por medio de las aplicaciones que usan Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y posterior, o Microsoft Internet Explorer 5.0 y posterior).

Exploración Hyper-V

La versión actual de la exploración Hyper-V admite la exploración del sistema virtual en línea o fuera de línea en Hyper-V. A continuación, se muestran los tipos de exploración compatibles de acuerdo con el sistema alojado de Windows Hyper-V y el estado del sistema virtual:

Sistemas virtuales con función Hyper-V	VM en línea	VM fuera de línea
Windows Server 2022 Hyper-V	Sólo lectura	Solo lectura/desinfección
Windows Server 2019 Hyper-V	Sólo lectura	Solo lectura/desinfección
Windows Server 2016 Hyper-V	Sólo lectura	Solo lectura/desinfección
Windows Server 2012 R2 Hyper-V	Sólo lectura	Solo lectura/desinfección
Windows Server 2012 Hyper-V	Sólo lectura	Solo lectura/desinfección

Requisitos de hardware

El servidor no debería tener problemas de rendimiento al ejecutar las máquinas virtuales. La actividad de

exploración usa principalmente recursos de la CPU. Para explorar máquinas virtuales en línea, se necesita de espacio libre en el disco. El espacio del disco debe ser como mínimo el doble del espacio utilizado por los puntos de comprobación o instantáneas y los discos virtuales.

Limitaciones específicas

- La exploración en almacenamiento RAID, volúmenes distribuidos y Discos Dinámicos no es compatible debido a la naturaleza de los Discos Dinámicos. Por lo tanto, recomendamos que evite usar el tipo de Disco Dinámico en sus VM.
- La exploración siempre se realiza en la VM actual y no afecta instantáneas ni puntos de verificación.
- Actualmente, no se admite ejecutar Hyper-V en un host en un clúster con ESET Mail Security.

> Mientras que ESET Security es compatible con la exploración de MBR de disco virtual, el único método compatible es la exploración de solo lectura para estos objetivos. Esta configuración puede cambiarse en **Configuración avanzada** (**F5**) > **Computer** > **Exploración de Hyper-V** > parámetros de ThreatSense > **Sectores de inicio**.

La máquina virtual que se va a explorar está "desconectada" (apagada)

ESET Mail Security usa el administrador de Hyper-V para detectar y conectarse a los discos virtuales. De este modo, ESET Mail Security tiene el mismo acceso al contenido de los discos virtuales al acceder a los datos y a los archivos de cualquier unidad genérica.

La máquina virtual que se va a explorar está "conectada" (se está ejecutando, está en pausa, guardada)

ESET Mail Security usa administrador de Hyper-V para detectar los discos virtuales. La conexión real a estos discos no es posible. Por lo tanto, ESET Mail Security crea un punto de control/una instantánea de la máquina virtual, y luego se conecta al punto de control/a la instantánea. Una vez finalizada la exploración, se elimina el punto de control/la instantánea. Esto significa que la exploración de solo lectura se puede llevar a cabo porque la actividad de la exploración no afecta la ejecución de las Máquinas virtuales.

Permite hasta un minuto para que ESET Mail Security cree una instantánea o punto de control durante la exploración. Esto resultaría de ayuda al ejecutar una exploración Hyper-V en un mayor número de máquinas virtuales.

Convención de nomenclatura

El módulo de exploración de Hyper-V usa la siguiente convención de nomenclatura:

```
VirtualMachineName\DiskX\VolumeY
```

Donde X es el número de disco mientras que Y es el número de volumen. Por ejemplo:

```
Computer\Disk0\Volume1
```

El sufijo de número se añade a partir del orden de detección, que es idéntico al orden que se ve en el Administrador de discos de la VM. Esta convención de nombres se usa en la menú desplegable de estructura de árbol de objetivos que se explorarán, en la barra de progreso y en los archivos de registro.

Ejecución de una exploración

- Bajo demanda: haga clic en **Exploración Hyper-V** para ver una lista de las máquinas virtuales y volúmenes

disponibles para explorar. Seleccione la(s) máquina(s) virtual(es), disco(s) o volumen(es) que desea explorar y haga clic en **Explorar**.

- Para crear una tarea programada.
- A través de ESET PROTECT como una tarea de cliente llamada Exploración del servidor.
- La exploración Hyper-V se puede administrar e iniciar mediante eShell.

Es posible ejecutar varias exploraciones de Hyper-V simultáneamente. Recibirá una notificación con un enlace a los archivos de registro cuando se complete la exploración.

Problemas posibles

- Al ejecutar la exploración de una máquina virtual en línea, debe crearse un punto de control o una instantánea de la máquina virtual específica. Durante la creación de un punto de control o una instantánea, algunas acciones genéricas de la máquina virtual pueden estar limitadas o deshabilitadas.
- Si se está explorando una máquina virtual sin conexión, no podrá encender la VM hasta que haya finalizado la exploración.
- El administrador de Hyper-V permite nombrar igual a dos máquinas virtuales diferentes, lo que representa un problema cuando se intenta identificarlas, al revisar los registros de exploración.

Para crear un perfil nuevo, seleccione **Editar** junto a **Lista de perfiles**, ingrese su propio **Nombre de perfil** y luego haga clic en **Agregar**. El nuevo perfil se mostrará en el menú desplegable **Perfil seleccionado** que lista los perfiles de exploración existentes.

El menú desplegable **Objetos para explorar** para **Hyper-V** le permite seleccionar los objetos predefinidos que se explorarán:

Por configuración de perfil	Selecciona los objetos especificados en el perfil de exploración seleccionado.
Todas las máquinas virtuales	Selecciona todas las máquinas virtuales.
Máquinas virtuales en línea	Selecciona todas las máquinas virtuales en línea.
Máquinas virtuales fuera de línea	Selecciona todas las máquinas virtuales fuera de línea.
No hay selección	Borra todas las selecciones.

Haga clic en el ícono ⚙ y modifique el intervalo para **Detener exploración si su duración es mayor a (minutos)** y cambie al tiempo que prefiera (entre 1 y 2880 minutos).

Haga clic en **Explorar** para ejecutar la exploración con los parámetros personalizados establecidos. Una vez que todas las exploraciones hayan terminado, revise **Archivos de registro** > Exploración Hyper-V.

Protección para Hyper-V y aprendizaje automatizado

El motor de detección y el componente de aprendizaje automático llevan a cabo los informes.

ThreatSense parámetros

Para modificar los parámetros de exploración para Exploración de Hyper-V.

HIPS

El Sistema de prevención de intrusiones basado en el host (HIPS) protege su sistema de malware y actividades no deseadas que intentan perjudicar el equipo. El sistema HIPS usa el análisis avanzado de conducta combinado con las capacidades de detección del filtrado de red para monitorear los procesos activos, los archivos y las claves de registro. El HIPS es independiente de la protección del sistema de archivos en tiempo real y no es un firewall; solo monitorea los procesos activos en el sistema operativo.

las modificaciones de la configuración del HIPS deben realizarse únicamente por un usuario experimentado. La configuración incorrecta de HIPS puede llevar a la inestabilidad del sistema.

Habilitar la autodefensa

ESET Mail Security cuenta con tecnología integrada de Autodefensa que evita que el software malicioso dañe o deshabilite la protección contra malware, por lo que puede estar seguro de que su sistema permanece protegido constantemente. Los cambios en la configuración Habilitar HIPS y Habilitar SD (Autodefensa) se aplican luego del reinicio del sistema operativo Windows. La deshabilitación del sistema HIPS completo también requiere reiniciar el equipo.

Habilitar el servicio protegido

Microsoft ha presentado un concepto de servicios protegidos con Microsoft Windows Server 2012 R2. Evita un servicio contra ataques de malware. El núcleo de ESET Mail Security se ejecuta como un servicio protegido de forma predeterminada. Esta característica está disponible en Microsoft Windows Server 2012 R2 y en los sistemas operativos de servidor más recientes.

Habilitar Advanced Memory Scanner

Trabaja en conjunto con el Bloqueador de exploits para fortalecer la protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado. La exploración de memoria avanzada está habilitada en forma predeterminada. Obtenga más información sobre este tipo de protección en el glosario.

Habilitar bloqueador de exploits

Está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de Microsoft Office. El bloqueador de exploits está habilitado en forma predeterminada. Obtenga más información sobre este tipo de protección en el glosario.

Habilite la protección Ransomware

Para utilizar esta funcionalidad, habilite HIPS y ESET Live Grid. Obtenga más información sobre el Ransomware en el glosario.

Modo de filtrado

Puede seleccionar uno de los siguientes modos de filtrado:

- **Modo automático**: las operaciones están habilitadas, excepto las que se encuentran bloqueadas por las reglas predefinidas que protegen su sistema. Todo está permitido excepto las acciones negadas por la regla.

- **Modo inteligente**: se notificará al usuario solo en caso de eventos muy sospechosos.

- **Modo interactivo**: el programa le solicitará al usuario que confirme las operaciones. Permitir / denegar acceso, Crear regla, Recordar temporalmente esta acción.

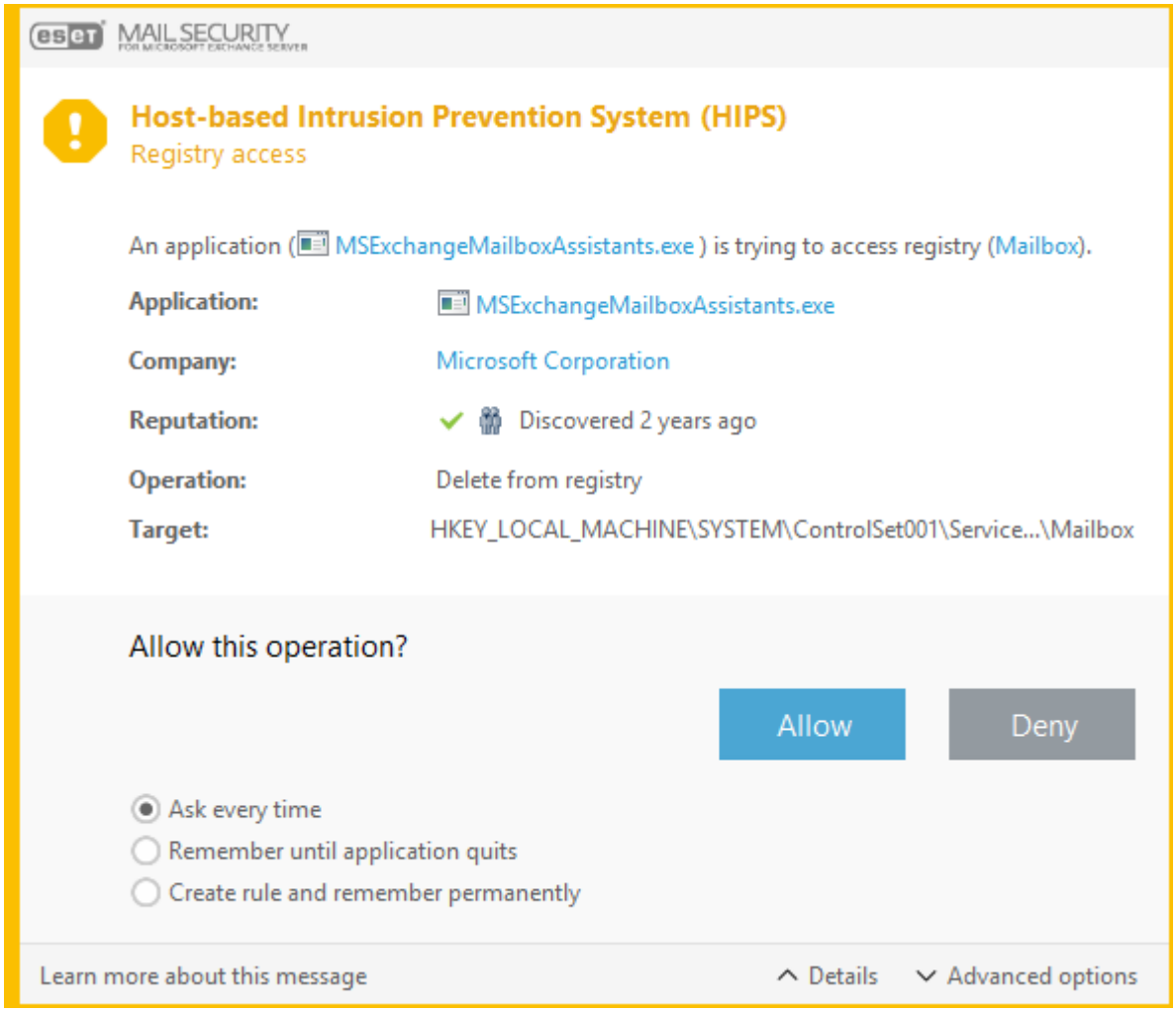
- **Modo basado en políticas**: las operaciones están bloqueadas. Únicamente acepta reglas predefinidas por el usuario.

- **Modo de aprendizaje**: las operaciones están habilitadas y se crea una regla luego de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Cuando selecciona el Modo de aprendizaje en el menú desplegable del modo de filtrado de HIPS, la configuración El modo de aprendizaje finalizará cuando estará disponible. Seleccione el tiempo durante el cual desea activar el modo de aprendizaje (el tiempo máximo es de 14 días). Cuando el tiempo especificado haya pasado, se le solicitará que edite las reglas creadas por HIPS mientras estuvo en el modo de aprendizaje. También puede elegir un modo de filtrado diferente, o posponer la decisión y continuar usando el modo de aprendizaje.

Reglas

Las reglas determinan qué aplicaciones tendrán acceso a qué archivos, partes del registro u otras aplicaciones. El sistema HIPS monitorea los sucesos dentro del sistema operativo y reacciona consecuentemente en función de reglas similares a las usadas por el firewall personal. Haga clic en Editar para abrir la ventana de administración de reglas de HIPS. Si la acción predeterminada para una regla está configurada para **Preguntar**, una ventana de diálogo aparecerá cada vez que se active la regla. Puede elegir **Bloquear** o **Permitir** la operación. Si no elige una acción en el tiempo dado, se seleccionará una nueva acción en función de las reglas.

La ventana de diálogo le permite crear una regla en función de cualquier acción nueva que el HIPS detecte para, posteriormente, definir las condiciones mediante las cuales se **permitirá** o se **bloqueará** dicha acción. Haga clic en **Detalles** para acceder a más información. Las reglas creadas de esta forma se consideran equivalentes a las creadas manualmente. En consecuencia, la regla creada desde una ventana de diálogo puede ser menos específica que la que activa la ventana de diálogo. Esto significa que, luego de crear dicha regla, la misma operación puede ejecutar la misma ventana.



Preguntar siempre

La ventana de diálogo se mostrará cada vez que se active la regla. Puede elegir **Bloquear** o **Permitir** la operación.

Recordar hasta salir de la aplicación

Al elegir una acción **Rechazar** o **Permitir**, se creará una regla HIPS temporal que se utilizará hasta que la aplicación en cuestión se cierre. Así mismo, si modifica el modo de filtrado, modifica las reglas o cuándo se actualiza el módulo HIPS, y si reinicia el sistema, se eliminarán las reglas temporales.

Crear regla y recordar permanentemente

Crear una nueva regla HIPS. Puede modificar esta regla más adelante en la sección de administración de reglas HIPS.

Configuraciones de reglas HIPS

Esta ventana le brinda una visión general de las reglas HIPS existentes.

Regla	Nombre de la regla definido por el usuario o elegido automáticamente.
Habilitado	Desactive este interruptor si desea conservar la regla en la lista pero no quiere usarla.
Acción	La regla especifica una acción, Permitir, Bloquear o Preguntar, que se deberá llevar a cabo bajo las condiciones adecuadas.

Regla	Nombre de la regla definido por el usuario o elegido automáticamente.
Fuentes	La regla solo se usará si una aplicación o un número de aplicaciones accionan el evento.
Destinos	La regla solo se usará si la operación se relaciona con un archivo, una aplicación o una entrada de registro específicos.
Gravedad de registro	Si activa esta opción, la información sobre esta regla se incluirá en el registro de HIPS.
Notificar	Si se acciona un evento, aparece una ventana pequeña en el área de notificación de Windows.

Cree una nueva regla, haga clic en **Agregar** nuevas reglas de HIPS o **Editar** las entradas seleccionadas.

Nombre de regla

Nombre de la regla definido por el usuario o elegido automáticamente.

Acción

La regla especifica una acción, **Permitir**, **Bloquear** o **Preguntar**, que se deberá llevar a cabo bajo las condiciones adecuadas.

Operaciones que afectan

Debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se usará para este tipo de operación y para el destino seleccionado. La regla consta de partes que describen las condiciones que desencadenan esta regla.

Aplicaciones de origen

La regla solo se usará cuando esta aplicación o estas aplicaciones accionen el suceso. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar carpetas o archivos, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

> i Algunas operaciones de reglas específicas predefinidas por el sistema HIPS no se pueden bloquear y están permitidas en forma predeterminada. Además, el sistema HIPS no monitorea todas las operaciones del sistema. HIPS monitorea las operaciones que se pueden considerar no seguras.

Descripciones de las operaciones más importantes:

Operaciones de archivos

Eliminar el archivo	La aplicación pide permiso para eliminar el archivo de destino.
Escribir en el archivo	La aplicación pide permiso para escribir en el archivo de destino.
Acceso directo al disco	La aplicación está intentando leer el disco o escribir en él de una forma que no es la estándar, lo que evade los procedimientos comunes de Windows. Esto puede provocar que se modifiquen los archivos sin haber aplicado las reglas correspondientes. Esta operación puede haberse generado por malware que intenta evadir la detección, un software de creación de copias de seguridad que intenta hacer una copia exacta del disco, o un administrador de particiones que intenta reorganizar los volúmenes de disco.
Instalar enlace global	Se refiere al llamado de la función SetWindowsHookEx de la biblioteca MSDN.
Cargar controlador	Instalación y carga de controladores en el sistema.

La regla solo se usará si la operación está relacionada con este destino. Seleccione **Archivos específicos** en el

menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Alternativamente, puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas las aplicaciones.

Operaciones de la aplicación

Depurar otra aplicación	Adjuntar un depurador al proceso. Cuando se depura una aplicación, es posible ver y modificar muchos detalles de su conducta, así como acceder a sus datos.
Interceptar eventos desde otra aplicación	La aplicación de origen está intentando capturar eventos dirigidos a una aplicación específica (por ejemplo, un registrador de pulsaciones de teclas que intenta capturar eventos del navegador).
Finalizar/suspender otra aplicación	Suspende, reanuda o termina un proceso (se puede acceder directamente desde el Explorador de procesos o desde la ventana de procesos).
Iniciar una nueva aplicación	Inicio de aplicaciones o procesos nuevos.
Modificar el estado de otra aplicación	La aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar un código en su nombre. Esta funcionalidad puede resultar útil para proteger una aplicación esencial mediante su configuración como aplicación de destino en una regla que bloquee el uso de dicha operación.

La regla solo se usará si la operación está relacionada con este destino. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Alternativamente, puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.

Operaciones de registros

Modificar las configuraciones de inicio	Cualquier cambio en la configuración que defina qué aplicaciones se ejecutarán durante el inicio de Windows. Pueden encontrarse, por ejemplo, al buscar la clave Ejecutar en el registro de Windows.
Eliminar del registro	Elimina una clave de registro o su valor.
Volver a nombrar la clave de registro	Vuelve a nombrar claves de registros.
Modificar el registro	Crea nuevos valores de claves de registro, modifica los valores existentes, cambia datos de lugar en el árbol de la base de datos o configura derechos de usuarios o de grupos para las claves de registro.

La regla solo se usará si la operación está relacionada con este destino. Seleccione **Entradas específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas. Alternativamente, puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

Puede usar caracteres globales con ciertas restricciones al ingresar un destino. En lugar de usar una clave específica, se puede usar el símbolo * (asterisco) en las rutas del registro. Por ejemplo, *HKEY_USERS*\software can mean HKEY_USER\.default\software* pero no *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** no es una ruta válida a una clave de registro. Una ruta a una clave de registro que contenga *** define “esta ruta o cualquier ruta de cualquier nivel que se encuentre después de ese símbolo”. Esta es la única manera de usar caracteres globales para archivos de destino. Primero se evaluará la parte específica de la ruta, y luego la ruta que sigue al carácter global (*).

Puede recibir una notificación si crea una regla demasiado general.

Configuración avanzada de HIPS

Las opciones que se muestran a continuación resultan útiles para la depuración y el análisis de la conducta de una aplicación:

Controladores siempre permitidos para cargar

Los controladores seleccionados siempre tienen permitido cargar independientemente del modo de filtrado configurado, a menos que se bloquee explícitamente por una regla de usuario. Los controladores que se muestran en esta lista siempre tendrán permitido cargar independientemente del modo de filtrado de HIPS, a menos que se bloquee explícitamente por una regla de usuario. Puede **Agregar** un nuevo controlador, **Editar** o **Eliminar** un controlador seleccionado de la lista.

> haga clic en **Restablecer** si no desea que se incluyan los controladores que ha agregado en forma manual. Esto puede ser útil si ha agregado varios controladores y no puede eliminarlos de la lista en forma manual.

Registrar todas las operaciones bloqueadas

Todas las operaciones bloqueadas se escribirán en el registro del sistema HIPS. Use esta función solo cuando solucione problemas o lo solicite el Soporte técnico de ESET, ya que podría generar un archivo de registro enorme y ralentizar el sistema.

Notificar cuando ocurran cambios en las aplicaciones de Inicio

Muestra una notificación del escritorio cada vez que se agrega o quita una aplicación del inicio del sistema.

Actualizar configuración

Esta sección especifica la información de origen de la actualización, como los servidores de actualización que se utilizan y los datos de autenticación de estos servidores.

> Para que las actualizaciones se descarguen correctamente, es esencial que complete correctamente todos los parámetros de actualización. Si usa un firewall, asegúrese de que el programa de ESET tenga permiso para comunicarse con Internet (por ejemplo, una comunicación HTTP).

Básico

Seleccionar el perfil de actualización predeterminado
Elija un perfil existente o cree uno nuevo para aplicarlo de forma predeterminada para las actualizaciones.
Cambio automático de perfil
Asigne un perfil de actualización en función de las redes conocidas en el firewall. El cambio automático de perfil permite cambiar el perfil de una red específica en función de la configuración de Tareas programadas. Consulte las páginas de ayuda para obtener más información
Configurar notificaciones de actualización
Haga clic en **Editar** para seleccionar qué notificaciones de la aplicación se muestran. Puede elegir si las notificaciones Se muestran en el escritorio o Se reenvían al correo electrónico.
Borrar caché de actualización
En caso de que experimente problemas con una actualización, haga clic en **Borrar** para borrar el caché de actualización temporal.

Actualizaciones del producto

Actualizaciones automáticas
Activado de forma predeterminada. Use el control deslizante para desactivar las actualizaciones automáticas si necesita impedir temporalmente que ESET Mail Security se actualice. Le recomendamos que mantenga activada esta configuración para asegurarse de que su ESET Mail Security tenga las actualizaciones de componentes del programa (PCU) más recientes y de que se aplican las microactualizaciones de componentes del programa (µPCU) cuando hay una nueva actualización disponible.

> Las actualizaciones se aplican luego del próximo reinicio del servidor.

Alertas del motor de detección obsoletas

Establecer la antigüedad máxima del motor de detección de forma automática / Antigüedad máxima del motor de detección (días)
Use el control deslizante para desactivar la antigüedad automática del motor de detección y defina manualmente el tiempo máximo (en días) luego del cual se informa que la antigüedad del motor de detección está desactualizada. El valor predeterminado es 7.

Módulo de reversión

Si sospecha que la nueva actualización del motor de detección o de los módulos de programas puede ser inestable o estar corrupta, puede regresar a la versión anterior y deshabilitar cualquier actualización para un período elegido. Como alternativa, puede habilitar las actualizaciones previamente deshabilitadas si las hubiera pospuesto indefinidamente. ESET Mail Security registra instantáneas del motor de detección y de los módulos de programa para usar con la característica de Reversión. Para crear instantáneas del motor de detección, deje habilitado **Crear instantáneas de los módulos**.
Número de instantáneas almacenadas localmente
Define la cantidad de instantáneas de módulos anteriores almacenadas.
Revertir a módulos anteriores
Haga clic en Revertir para revertir los módulos del programa a la versión anterior y desactivar temporalmente las actualizaciones.

Perfiles

Para crear un perfil de actualización personalizado, seleccione **Editar** junto a **Lista de perfiles**. Ingrese su propio **Nombre de perfil** y luego haga clic en **Agregar**. Seleccione el perfil para editar y modifique los parámetros para los tipos de actualización de los módulos o cree un **Mirror de actualización**.

Actualizaciones

Seleccione el tipo de actualización en el menú desplegable:
• **Actualización normal**: de manera predeterminada, el tipo Actualización se define en Normal para garantizar que los archivos de actualización se descarguen automáticamente del servidor de ESET con el menor tráfico de red.
• **Actualización previa al lanzamiento**: son actualizaciones que se evaluaron detalladamente y de manera interna y estarán disponibles al público en general en poco tiempo. Puede beneficiarse de la habilitación de las actualizaciones previas a la publicación al tener acceso a las soluciones y los métodos de detección más recientes. Sin embargo es posible que las actualizaciones previas a la publicación no sean lo suficientemente estableces en todo momento y NO DEBEN utilizarse en estaciones de trabajo y servidores de producción donde se necesita de estabilidad y disponibilidad máximas.
• **Actualización demorada**: permite hacer la actualización desde los servidores de actualización especial que proporcionan nuevas versiones de bases de datos de virus con un retraso de por lo menos X horas (es decir, bases de datos probadas en un entorno real y por lo tanto consideradas estables).

Habilitar la optimización de entrega de actualización

Cuando esta opción está activada, los archivos de actualización se descargan de CDN (red de entrega de contenido). Desactivar esta configuración puede provocar interrupciones y ralentizaciones de la descarga cuando los servidores de actualizaciones de ESET dedicados están sobrecargados. La desactivación es útil cuando un firewall solo tiene acceso a direcciones IP del servidor de actualización de ESET o si una conexión a los servicios de CDN no funciona.

Preguntar antes de descargar la actualización

Cuando haya una nueva actualización disponible, se le preguntará antes de descargarla.

Preguntar si un archivo de actualización es más grande que (kB)

Si el tamaño del archivo de actualización es mayor que el valor especificado en el campo, el programa mostrará una notificación.

Actualizaciones de módulo

Las actualizaciones del módulo están configuradas en **Seleccionar automáticamente** en forma predeterminada. El servidor de actualización es la ubicación donde se almacenan las actualizaciones. Si usa un servidor de ESET, recomendamos que deje seleccionada la opción predeterminada.

Cuando use un servidor HTTP local (también conocido como Mirror), el servidor de actualización debe definirse de la siguiente manera: http://computer_name_or_its_IP_address:2221
Cuando use un servidor HTTP local con SSL, el servidor de actualización debe definirse de la siguiente manera: https://computer_name_or_its_IP_address:2221
Cuando use una carpeta compartida local, el servidor de actualización debe definirse de la siguiente manera: \\computer_name_or_its_IP_address\shared_folder

Permite actualizaciones de firmas de detección con mayor frecuencia

El motor de detección se actualizará en intervalos más cortos. Al desactivar esta opción, se puede afectar de forma negativa el índice de detección.

Permitir actualizaciones de módulo desde medios extraíbles

Le permite actualizar desde medios extraíbles si contiene un mirror creado. Cuando se selecciona **Automático**, la actualización no se ejecutará en el fondo. Si desea mostrar diálogos de actualización, seleccione **Preguntar siempre**.

Actualizaciones del producto

Pausar las actualizaciones automáticas para perfiles de actualización específicos desactiva temporalmente las actualizaciones automáticas del producto, por ejemplo, cuando se conectan a Internet a través de otras redes o conexiones medidas. Mantenga activada esta configuración para tener acceso constante a las características más recientes y a la máxima protección posible.

En algunos casos, es posible que sea necesario reiniciar el servidor para que se realicen las actualizaciones.

Opciones de conexión

Servidor proxy

Para acceder a las opciones de configuración del servidor proxy para un perfil de actualización determinado. Haga clic en Modo Proxy y seleccione una de las siguientes tres opciones:

- **No usar servidor proxy**: al realizar actualizaciones, ESET Mail Security no usará ningún servidor proxy.
- **Usar la configuración global del servidor proxy**: se usará la configuración del servidor proxy especificada en Configuración avanzada (F5) > Herramientas > Servidor proxy.
- **Conexión a través de un servidor proxy**: use esta opción si:

Debe usar un servidor proxy para actualizar ESET Mail Security, diferente del servidor proxy especificado en la configuración global (Herramientas > Servidor proxy). En este caso, será necesario especificar la configuración aquí: Dirección del Servidor proxy, Puerto de comunicación (3128, en forma predeterminada), además del Nombre de usuario y la Contraseña para el servidor proxy, de ser necesario.

La configuración del servidor proxy no se estableció en forma global, pero ESET Mail Security se conectará a un servidor proxy para descargar las actualizaciones.

El equipo está conectado a Internet mediante un servidor proxy. Durante la instalación del programa, la configuración se copia de Internet Explorer, pero si posteriormente se cambia (por ejemplo, cambia el ISP), verifique desde esta ventana que la configuración del proxy HTTP sea la correcta. De lo contrario, el programa no podrá conectarse a los servidores de actualización.

Los datos de autenticación como el **Nombre de usuario** y la **Contraseña** sirven para acceder al servidor proxy. Complete estos campos solo si el nombre de usuario y la contraseña son necesarios. Recuerde que estos campos no corresponden a su nombre de Usuario y Contraseña para ESET Mail Security y solo deben suministrarse si tiene la certeza de que se requiere una contraseña para acceder a Internet a través de un servidor proxy.

Utilice una conexión directa si el proxy no está disponible

Si un producto está configurado para usar HTTP Proxy y no puede llegar al proxy, el producto evadirá el proxy y se comunicará directamente con los servidores ESET.

Compartir de Windows

Cuando se lleva a cabo una actualización desde un servidor local que ejecuta Windows, se requiere autenticar cada conexión de red en forma predeterminada.

Conectarse a la LAN como

Para configurar su cuenta, seleccione una de las siguientes opciones:

- **Cuenta del sistema (predeterminado)**: usa la cuenta del sistema para la autenticación. Por lo general, no se lleva a cabo ningún proceso de autenticación si no se proporcionan los datos de autenticación en la sección principal correspondiente a la configuración de la actualización.
- **Usuario actual**: seleccione esta opción para asegurarse de que el programa realice la autenticación con la cuenta de un usuario que haya iniciado sesión. La desventaja de esta solución es que el programa no podrá conectarse al servidor de actualización cuando no haya ningún usuario registrado.
- **Usuario especificado**: seleccione esta opción para usar una cuenta de usuario específica para la autenticación. Use este método cuando falle la conexión predeterminada de la cuenta del sistema. Recuerde que la cuenta de usuario especificada debe tener acceso al directorio de archivos de actualización en el servidor local. Si el usuario no tiene acceso, el programa no podrá establecer una conexión o descargar las actualizaciones.

Cuando esté seleccionado el **Usuario actual** o el **Usuario especificado**, puede aparecer un error al cambiar la identidad del programa según el usuario deseado. Es recomendable ingresar los datos de autenticación de la LAN en la sección principal correspondiente a la configuración de la actualización. En esta sección de configuración de la actualización, los datos de autenticación deben ingresarse de la siguiente forma: domain_name\user (si es un grupo de trabajo, ingrese workgroup_name\name) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no se necesita realizar ninguna autenticación.

Desconectar del servidor tras la actualización

Seleccione esta opción para forzar una desconexión si la conexión al servidor permanece activa aunque las actualizaciones se hayan terminado de descargar.

Actualizar reflejo

Las opciones de configuración del servidor Mirror local se encuentran en **Configuración avanzada** (F5) en la pestaña **Actualización** > **Perfiles** > Mirror de actualización.

Revertir actualización

Si sospecha que una nueva actualización del motor de detección o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y deshabilitar las actualizaciones de manera temporal. También puede activar actualizaciones desactivadas anteriormente si las había pospuesto indefinidamente.

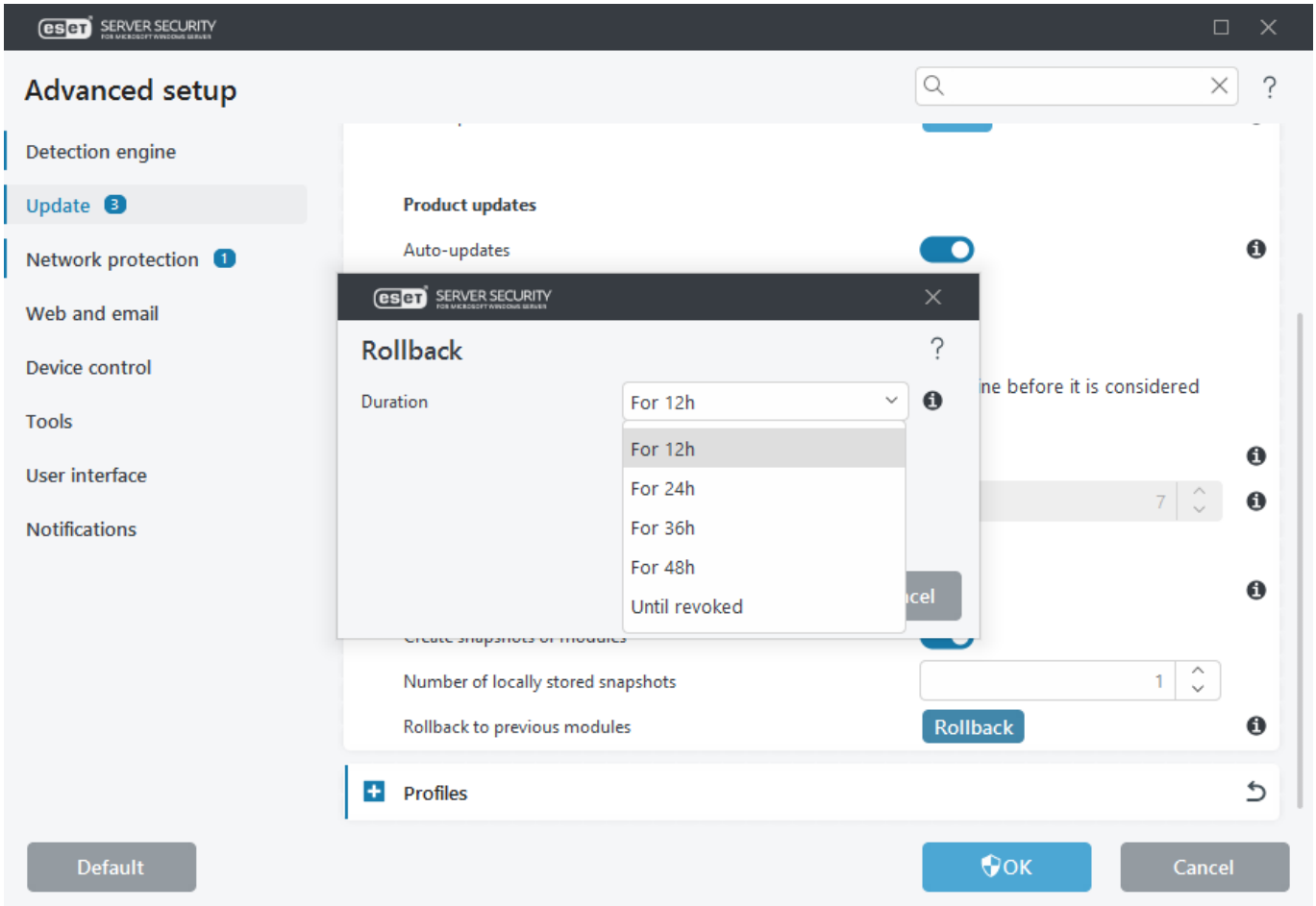
ESET Mail Security registra instantáneas del motor de detección y de los módulos del programa para usarlos con la característica de reversión. Para crear instantáneas de la base de datos de virus, mantenga habilitada la opción **Crear instantáneas de los módulos**.

Cuando se habilita **Crear instantáneas de los módulos**, se crea la primera instantánea durante la primera actualización. La siguiente se crea después de 48 horas.

El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas almacenadas del motor de detección.

> Cuando se alcanza el número máximo de instantáneas (por ejemplo, tres), se sustituye la instantánea más antigua por una nueva cada 48 horas. ESET Mail Security revierte las versiones de actualización del motor de detección y de los módulos del programa a la instantánea más antigua.

Si hace clic en **Revertir**, debe seleccionar un intervalo de tiempo del menú desplegable que represente el período en que las actualizaciones de la base de datos del motor de detección y del módulo del programa se pondrán en pausa.



Seleccione **Hasta que se revoque** para posponer las actualizaciones regulares de manera indefinida hasta

restaurar manualmente la funcionalidad de actualización. Dado que representa un potencial riesgo de seguridad, le recomendamos no seleccionar esta opción.

Si se realiza una reversión, el botón **Revertir** cambia a **Permitir actualizaciones**. Las actualizaciones no están permitidas para el intervalo de tiempo seleccionado en el menú desplegable **Suspender actualizaciones**.

La versión de la base de datos del motor de detección regresa a la versión más antigua disponible y se guarda como una instantánea en el sistema local de archivos del equipo.

Tarea programada - actualización

Si desea actualizar el programa desde dos servidores de actualización, será necesario crear dos perfiles de actualización diferentes. Si el primero no logra descargar los archivos de actualización, el programa cambia automáticamente al perfil alternativo. Esto es conveniente, por ejemplo, para equipos portátiles, que suelen actualizarse desde un servidor de actualización de la red de área local, pero cuyos dueños normalmente se conectan a Internet por medio de otras redes. Por lo tanto, si falla el primer perfil, el segundo descargará automáticamente los archivos de actualización desde los servidores de actualización de ESET.

Los siguientes pasos le guiarán durante una tarea de edición de **Actualización automática de rutina** existente.
1. En la pantalla principal de **Tareas programadas**, seleccione la tarea **Actualización** con el nombre **Actualización automática de rutina** y haga clic en **Editar**, se abrirá el asistente de configuración.
2. Configure la tarea de tareas programadas para que se ejecute, seleccione una de las siguientes opciones de programación para definir cuándo desea que se ejecute la tarea programada.
3. Si quiere evitar que la tarea se ejecute cuando el sistema funciona a batería (por ejemplo, UPS), haga clic en el interruptor junto a **Omitir tarea al ejecutar con alimentación de la batería**.
4. Seleccione perfil de actualización para usarlo en la actualización. Seleccione una acción para realizar en caso de que la ejecución de la tarea no se lleve a cabo por algún motivo.
5. Haga clic en **Finalizar** para aplicar la tarea.

Actualizar reflejo

ESET Mail Security le permite crear copias de archivos de actualización que se pueden usar para actualizar otras estaciones de trabajo en la red. El uso de un “servidor reflejado”: es conveniente tener una copia de los archivos de actualización en el entorno de la LAN debido a que las estaciones de trabajo no necesitan descargar los archivos de actualización desde el servidor de actualización del proveedor reiteradamente. Las actualizaciones se descargan al servidor reflejado local y, desde allí, se distribuyen a todas las estaciones de trabajo para evitar el riesgo de generar una sobrecarga en el tráfico de red.

La actualización de las estaciones de trabajo del cliente desde un Mirror optimiza el equilibrio de carga de la red y ahorra el ancho de banda de la conexión a Internet.

Para minimizar el tráfico de Internet en las redes donde ESET PROTECT se usa para administrar muchos clientes, recomendamos usar ESET Bridge en lugar de configurar un cliente como mirror. ESET Bridge se puede instalar con ESET PROTECT usando el instalador todo en uno o como un componente independiente. Para obtener más información y diferencias entre ESET Bridge, Apache HTTP Proxy, Mirror Tool y conectividad directa, consulte la página de ayuda en línea de ESET PROTECT.

Actualizar reflejo

Crear replicación de actualización
Activa las opciones de configuración del mirror.

Acceder a los archivos de actualización

Habilitar servidor HTTP
Si esta opción se encuentra habilitada, se puede acceder a los archivos de actualización a través de HTTP, sin necesidad de ingresar credenciales.
Carpeta de almacenamiento
Haga clic en **Editar** para buscar una carpeta en el equipo local o en la carpeta de la red compartida. Si la carpeta especificada requiere una autorización, deberá ingresar los datos de autenticación en los campos Nombre de usuario y Contraseña.
Haga clic en **Borrar**si desea cambiar una carpeta predeterminada definida para almacenar archivos duplicados *C:\ProgramData\ESET\ESET Security\mirror*.

Servidor HTTP

Puerto de servidor
El puerto predeterminado es 2221. Cambie este valor en caso de utilizar otro puerto.
Autenticación
Define el método de autenticación usado para acceder a los archivos de actualización. Se encuentran disponibles las siguientes opciones: **Ninguna**, **Básica** y **NTLM**.
- Seleccione **Básica** para usar la codificación de Base64 con la autenticación básica del nombre de usuario y la contraseña.
- La opción **NTLM** proporciona una codificación obtenida mediante un método seguro. Para la autenticación, se usa el usuario creado en la estación de trabajo que comparte los archivos de actualización.
- La configuración predeterminada es **Ninguna**, que otorga acceso a los archivos de actualización sin necesidad de autenticar.

> Si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta del Mirror debe estar ubicada en el mismo equipo que la instancia de ESET Mail Security que la crea.

SSL para el servidor HTTP
Añada su **Archivo de cadena de certificados**, o genere un certificado de firma automática si desea ejecutar el servidor HTTP con el soporte de HTTPS (SSL). Se encuentran disponibles los siguientes tipos de certificado: PEM, PFX y ASN. Para obtener una seguridad adicional, puede usar el protocolo HTTPS para descargar los archivos de actualización. Es casi imposible realizar un seguimiento de las transferencias de datos y credenciales de registro con este protocolo.
El **Tipo de clave privada** está configurada en **Integrada** de forma predeterminada (y por lo tanto, la opción Archivo de clave privada está deshabilitada de forma predeterminada). Esto significa que la clave privada es parte del archivo de cadena de certificados seleccionado.

Opciones de conexión

Compartir de Windows
Cuando se lleva a cabo una actualización desde un servidor local que ejecuta Windows, se requiere autenticar cada conexión de red en forma predeterminada.
Conectarse a la LAN como
Para configurar su cuenta, seleccione una de las siguientes opciones:
• **Cuenta del sistema** (predeterminado): se usa la cuenta del sistema para autenticación. Normalmente, no se lleva a cabo ningún proceso de autenticación si no se proporcionan los datos de autenticación en la sección principal correspondiente a la configuración de la actualización.
• **Usuario actual**: seleccione esta opción para asegurarse de que el programa realice la autenticación con la cuenta de un usuario que haya iniciado sesión. La desventaja de esta solución es que el programa no puede conectarse al servidor de actualización si ningún usuario ha iniciado sesión.
• **Usuario especificado**: seleccione esta opción para usar una cuenta de usuario específica para la autenticación. Use este método cuando falle la conexión predeterminada de la cuenta del sistema. Recuerde que la cuenta de usuario especificada debe tener acceso al directorio de archivos de actualización en el servidor local. Si el usuario no tiene acceso, el programa no puede establecer una conexión y descargar las actualizaciones.

Cuando esté seleccionado el **Usuario actual** o el **Usuario especificado**, puede aparecer un error al cambiar la identidad del programa según el usuario deseado. Es recomendable ingresar los datos de autenticación de la LAN en la sección principal correspondiente a la configuración de la actualización. En esta sección de configuración de la actualización, los datos de autenticación deben ingresarse de la siguiente forma: *domain_name\user* (si es un grupo de trabajo, ingrese *workgroup_name\name*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no se necesita realizar ninguna autenticación.

Desconectar del servidor tras la actualización
Seleccione esta opción para forzar una desconexión si la conexión al servidor permanece activa aunque las actualizaciones se hayan terminado de descargar.

Protección de la red

Administre la protección de red, haga clic en **Editar** para agregar una nueva o modificar la existente:

- Redes conocidas
- Zonas

Redes conocidas

Cuando use un equipo que se conecta con frecuencia a redes públicas o redes fuera de su red de trabajo normal, le recomendamos comprobar la credibilidad de la red de las nuevas redes a las que se esté conectando. Una vez definidas las redes, ESET Mail Security puede reconocer redes confiables (domésticas/de oficina) usando diversos parámetros de red configurados en Identificación de red.

Con frecuencia, los equipos ingresan redes con direcciones IP similares a las de la red confiable. En estos casos, ESET Mail Security puede considerar que una red desconocida es confiable (doméstica/oficina). Le recomendamos usar la Autenticación de red para evitar este tipo de situación.

Cuando un adaptador de red se conecte a una red o se vuelva a configurar su configuración de red, ESET Mail Security buscará en la lista de redes conocidas un registro que coincida con la nueva red. Si la identificación de red y la autenticación de red (opcional) coinciden, la red se marcará conectada en esta interfaz.

Si no se encuentra ninguna red conocida, la configuración de identificación de red creará una nueva conexión de red para identificar la red la próxima vez que se conecte a ella. De forma predeterminada, la nueva conexión de red usa el tipo de protección de red pública.

El cuadro de diálogo Nueva conexión de red detectada le pedirá que elija entre red pública, red doméstica o red de oficina, o usar el tipo de protección de configuración de Windows. Si un adaptador de red está conectado a una red conocida y esa red se marca como Red doméstica o red de oficina, las subredes locales del adaptador se agregarán a la zona de confianza.

Tipo de protección de nuevas redes

Seleccione cuál de las siguientes opciones: **Usar configuración de Windows**, **Preguntar al usuario** o **Marcar como pública** se usa de forma predeterminada para las redes nuevas. Cuando seleccione **Usar ajuste de Windows**, no aparecerá un cuadro de diálogo y la red a la que está conectado se marcará automáticamente según su configuración de Windows. Esto permitirá el acceso a determinadas características (por ejemplo, el uso compartido de archivos y el escritorio remoto) desde las redes nuevas.

Las redes conocidas pueden configurarse manualmente en la ventana Editor de redes conocidas.

Agregar red

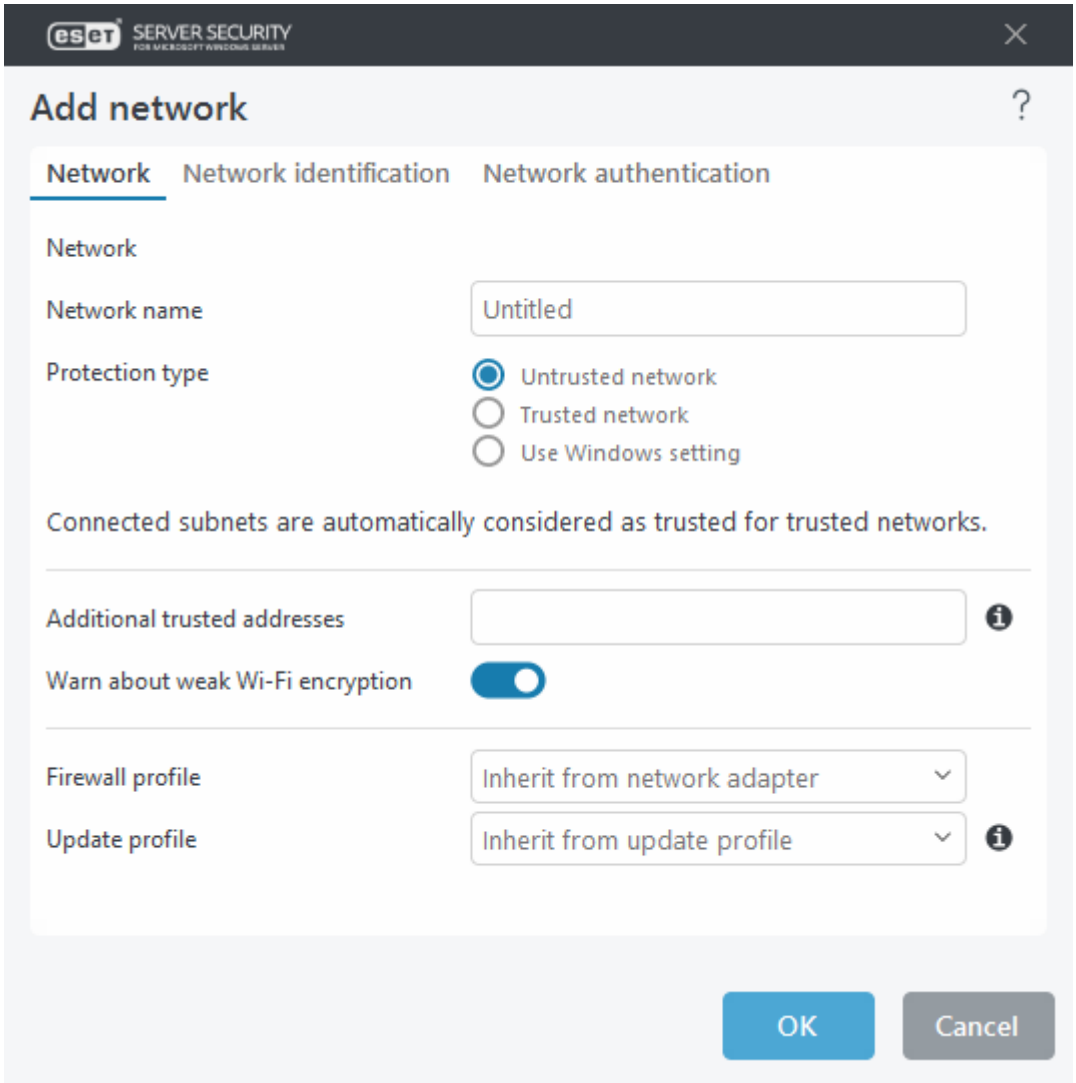
Los ajustes de configuración de red están organizados en las siguientes pestañas:

Red

Puede definir el **Nombre de la red** y seleccionar el **Tipo de protección** para la red. Muestra si la red está configurada como **Red confiable**, **Red no confiable** o **Usar configuración de Windows**.

Además, las direcciones agregadas en **Direcciones de confianza adicionales** se añaden siempre a la zona de confianza de los adaptadores conectados a esta red (sea cual sea el tipo de protección de la red).

- **Advertencia sobre cifrado de WiFi débil**: ESET Mail Security le informará cuando se conecte a una red inalámbrica no protegida o a una red con un nivel de protección débil.
- El **perfil de firewall** se heredará del adaptador de red.
- **Perfil de actualización**: seleccione el perfil de actualización que se usará al conectarse a esta red.



Identificación de la red

Se realiza de acuerdo con los parámetros del adaptador de red local. Todos los parámetros seleccionados se comparan con los parámetros reales de las conexiones de red activas. Se permiten direcciones IPv4 e IPv6.

Autenticación de red

Busca un servidor específico en la red y usa el cifrado asimétrico (RSA) para autenticar ese servidor. El nombre de la red que se está autenticando debe coincidir con el nombre de la zona definido en la configuración del servidor de autenticación. El nombre distingue entre mayúsculas y minúsculas. Especifique un nombre del servidor, un puerto de escucha del servidor y una clave pública correspondiente a la clave privada del servidor. El nombre del servidor puede ingresarse en forma de dirección IP, DNS o nombre de NetBios y puede seguirse por una ruta que especifique la ubicación de la clave en el servidor (por ejemplo, *server_name_/directory1/directory2/authentication*). Puede especificar servidores alternativos que desea utilizar anexándolos a la ruta, separados por punto y coma.

La clave pública se puede importar con cualquiera de los siguientes tipos de archivo:

- Clave pública cifrada PEM (.pem): esta clave puede generarse con el servidor de autenticación de ESET.
- Clave pública cifrada
- Archivo de certificado de clave pública (.crt)

Haga clic en **Probar** para probar su configuración. Si la autenticación es correcta, se mostrará que la autenticación del servidor se ha realizado correctamente. Si la autenticación no está configurada de forma correcta, se mostrarán los siguientes mensajes de error:

Falló la autenticación del servidor. Firma no válida o que no coincide.	La firma del servidor no coincide con la clave pública ingresada.
Falló la autenticación del servidor. El nombre de la red no coincide.	Desactive este interruptor si desea conservar la regla en la lista pero no quiere usarla.
Falló la autenticación del servidor. No válido o sin respuesta desde el servidor.	No se recibe ninguna respuesta si el servidor no se está ejecutando o no está accesible. Si otro servidor HTTP se está ejecutando en la dirección especificada, puede recibir una respuesta no válida.
Se ingresó una clave pública no válida.	Compruebe que el archivo de clave pública que ha ingresado no esté dañado.

Zonas

Una zona es una recopilación de direcciones de red que crean un grupo lógico de direcciones IP, útil cuando vuelve a usar el mismo conjunto de direcciones en varias reglas. A cada dirección de un grupo se le asignan reglas similares definidas de forma centralizada para todo el grupo. Un ejemplo de este tipo de grupo es una **zona de confianza**. Una zona de confianza representa un grupo de direcciones de red que no bloquea el firewall de ninguna forma.

Para agregar una zona de confianza:

1. Abra **Configuración avanzada** (**(F5)**) > **Protección de red** > **Básica** > **Zonas**.

2. Haga clic en **Editar** junto a las **Zonas**.

3. Haga clic en **Agregar**, escriba el **Nombre** y la **Descripción** de la nueva zona y agregue una dirección IP remota al campo **Dirección del equipo remoto (IPv4/IPv6, intervalo, máscara)**.

4. Haga clic en **OK**.

Columnas

- **Nombre**: nombre de un grupo de equipos remotos.

- **Direcciones IP**: direcciones IP remotas que pertenecen a una zona.

Elementos de control

Cuando agrega o edita una zona, están disponibles los siguientes campos:

- **Nombre**: nombre de un grupo de equipos remotos.

- **Descripción**: una descripción general del grupo.

- **Dirección del equipo remoto (IPv4, IPv6, intervalo, máscara)**: una dirección remota, un rango de direcciones o una subred.

- **Eliminar**: quita una zona de la lista.

> i No se pueden quitar zonas predefinidas.

Protección contra ataques en la red

Habilitar Protección contra ataques en la red (IDS)

Le permite configurar el acceso a ciertos servicios ejecutados en su equipo desde la Zona de confianza así como habilitar o deshabilitar la detección de varios tipos de ataques y vulnerabilidades que podrían emplearse para dañar su equipo.

Habilitar protección contra botnets

Detecta y bloquea la comunicación con servidores de control y comando maliciosos en función de los patrones típicos cuando el equipo está infectado y un bot intenta comunicarse

Excepciones de IDS

Puede pensar las excepciones del Sistema de Detección de Intrusiones (IDS) como reglas de protección de red. Haga clic en editar para definir las excepciones de IDS.

> i Si su entorno ejecuta una red de alta velocidad (10 GbE y posteriores), lea el artículo de la base de conocimiento para obtener información sobre elrendimiento de la velocidad de la red y ESET Mail Security.

Protección contra ataques por fuerza bruta

ESET Mail Security inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

Opciones avanzadas

Configure las opciones avanzadas de filtrado para detectar los distintos tipos de ataques y las vulnerabilidades que pueden ejecutarse contra su equipo.

Detección de intrusiones:

Protocolo SMB: detecta y bloquea varios problemas de seguridad en el protocolo SMB
Protocolo RPC: detecta y bloquea varios CVE en el sistema de llamada a procedimientos remotos desarrollado para el Distributed Computing Environment (DCE).
Protocolo RDP: detecta y bloquea varios CVE en el protocolo RDP (consulte arriba).
Bloquear la dirección no segura una vez detectado el ataque: las direcciones IP que han sido detectadas como fuentes de ataques y son agregadas a la lista negra para prevenir la conexión durante cierto período de tiempo.
Mostrar una notificación al detectar un ataque: activa el área de notificación de Windows en la esquina inferior derecha de la pantalla.
Mostrar notificaciones también para ataques entrantes contra vulnerabilidades de seguridad: le alerta si se detectan ataques hacia los vulnerabilidades de seguridad o si una amenaza intenta entrar en el sistema de esta manera.

Inspección del paquete:

Permitir una conexión entrante para intercambio de admin en el protocolo de SMB – Los recursos compartidos de administración (recursos compartidos de admin) son los recursos compartidos de red predeterminados que comparten particiones de disco duro (C$, D$, ...) en el sistema junto con la carpeta del sistema (ADMIN$). La desactivación de la conexión a los recursos compartidos de admin debería disminuir muchos riesgos de seguridad. Por ejemplo, el gusano Conficker realiza ataques de diccionario para conectarse a los recursos compartidos de admin.
Denegar dialectos SMB anteriores (no compatibles) – Rechaza sesiones SMB que utilicen un dialecto SMB antiguo no compatible con IDS. Los sistemas operativos modernos de Windows son compatibles con dialectos SMB antiguos por ser compatibles con sistemas operativos antiguos como Windows 95. El atacante puede usar un dialecto antiguo en una sesión SMB para sortear la inspección de tráfico. Deniegue los dialectos SMB antiguos si el equipo no necesita compartir archivos (o usar la comunicación SMB en general) con un equipo con una versión antigua de Windows.
Denegar sesiones SMB sin extensiones de seguridad – En las negociaciones de sesión de SMB es posible utilizar una seguridad ampliada para disponer de un mecanismo de autenticación más seguro que la autenticación Challenge/Response (LM) de LAN Manager. El esquema LM se considera débil y se desaconseja utilizarlo.
Permitir la comunicación con el servicio Security Account Manager: para obtener más información sobre este servicio, consulte [MS-SAMR].
Permitir la comunicación con el servicio Local Security Authority: para obtener más información sobre este servicio, consulte [MS-LSAD] y [MS-LSAT].
Permitir la comunicación con el servicio Remote Registry: para obtener más información sobre este servicio, consulte [MS-RRP].
Permitir la comunicación con el servicio Administrador de control de servicios: para obtener más información sobre este servicio, consulte [MS-SCMR].
Permitir la comunicación con el servicio Server: para obtener más información sobre este servicio, consulte [MS-SRVS].
Permitir la comunicación con los otros servicios: otros servicios de MSRPC.

Excepciones de IDS

Las excepciones del Sistema de Detección de Intrusiones (IDS) son, básicamente, reglas de protección de la red. Las excepciones se evalúan de manera descendente. El editor de excepciones de IDS le permite personalizar el comportamiento de protección del equipo en función de las distintas excepciones de IDS. Se aplica la primera excepción coincidente para cada tipo de acción (Bloquear, Notificar, Registrar), por separado. **Arriba**/**Superior**/**Abajo**/**Inferior** le permite ajustar el nivel de prioridad de las excepciones. Para crear una nueva excepción de IDS, haga clic en **Agregar**. Haga clic en **Editar** para modificar una excepción de IDS existente o en **Eliminar** para eliminarla.

Elija el tipo de **Alerta** de la lista desplegable. Especifique el **Nombre de amenaza** y la **Dirección**. Busque una **Aplicación** para la que desee crear la excepción. Especifique una lista de direcciones IP (IPv4 o IPv6) o subredes. Para ingresos múltiples, utilice una coma como delimitador.

Configure la **Acción** para la excepción de IDS al seleccionar una de las opciones del menú desplegable (**Predeterminado**, **Sí**, **No**). Haga esto para cada tipo de acción (**Bloquear**, **Notificar**, **Registrar**).

> ✔ Si quiere que se muestre una notificación en el caso de una alerta de excepción de IDS, así como el horario del evento registrado, deje el tipo de acción **Bloquear** como **Predeterminado** y para los otros dos tipos de acción (**Notificar** y **Registrar**), elija **Sí** del menú desplegable.

Sospecha de amenaza bloqueada

Esta situación puede ocurrir cuando una de las aplicaciones de su equipo está intentando transmitir tráfico malicioso a otro equipo de la red y se aprovecha de una vulnerabilidad de seguridad, o si alguien intenta explorar puertos de su red.

- Amenaza – Nombre de la amenaza.
- Origen: dirección de la red de origen.
- Destino: dirección de la red de destino.
- Detener bloqueo: crea una regla de IDS para la sospecha de amenazas con una configuración que permite la comunicación.
- Mantener bloqueo: bloquea la amenaza detectada. Si desea crear una regla de IDS con una configuración para bloquear la comunicación de esta amenaza, seleccione No volver a notificarme.

> La información que se muestra en esta ventana de notificación puede variar en función del tipo de amenaza detectada. Para obtener más información sobre amenazas y otros términos relacionados, consulte Tipos de ataques remotos o Tipos de detecciones.

Lista negra temporal de direcciones IP

Ver una lista de direcciones IP detectadas como la fuente de ataques y agregadas a la lista negra para bloquear las conexiones durante cierto período de tiempo (hasta una hora). Muestra las **direcciones IP** que han sido bloqueadas.

Motivo de bloqueo

Muestra el tipo de ataque que se ha evitado desde la dirección (por ejemplo, ataque de exploración de puerto TCP).

Tiempo de espera

Muestra la hora y la fecha en que la dirección desaparecerá de la lista negra.

Eliminar / Eliminar todo

Elimina la dirección IP seleccionada de la lista negra temporal antes de que caduque o elimina de forma inmediata todas las direcciones de la lista negra.

Agregar excepción

Agrega una excepción de firewall al filtrado IDS para la dirección IP seleccionada.

Protección contra ataques por fuerza bruta

La protección contra ataques por fuerza bruta bloquea los intentos de ataques para adivinar contraseñas de los servicios RDP y SMB. Un ataque por fuerza bruta es un método para descubrir una contraseña específica intentando de manera sistemática todas las combinaciones de letras, números y símbolos posibles.

- **Habilitar la protección contra ataques por fuerza bruta:** ESET Mail Security inspecciona el contenido del tráfico de red y bloquea los intentos de ataques para adivinar contraseñas.

- Reglas: crear, editar y ver reglas para las conexiones de red entrantes y salientes.

- Exclusiones – Lista de detecciones excluidas definidas por una dirección IP o una ruta de la aplicación. Puede crear y editar exclusiones en su ESET PROTECT Web Console.

Reglas de protección contra ataques por fuerza bruta

Las reglas de protección contra ataques por fuerza bruta le permiten crear, editar y ver reglas para las conexiones de red entrantes y salientes. Las reglas predefinidas no pueden quitarse ni editarse.

Cree una nueva regla, haga clic en **Agregar** nuevas reglas de protección contra ataques por fuerza bruta o **Editar** las entradas seleccionadas.

Esta ventana le brinda una visión general de las reglas de protección contra ataques por fuerza bruta existentes.

Nombre	Nombre de la regla definido por el usuario o elegido automáticamente.
Habilitado	Desactive este interruptor si desea conservar la regla en la lista pero no quiere usarla.
Acción	La regla especifica una acción, Permitir o Denegar, que se deberá llevar a cabo bajo las condiciones adecuadas.
Protocolo	El protocolo de comunicación que inspeccionará esta regla.
Perfil	Se pueden definir y aplicar reglas personalizadas para perfiles específicos.
Cantidad máxima de intentos	La cantidad máxima de intentos permitidos de repetición de ataques hasta que la dirección IP se bloquea y se agrega a la lista negra.
Periodo de retención de la lista negra (min.)	Define la hora de caducidad de la dirección de la lista negra. El periodo de tiempo predeterminado para contar el número de intentos es de 30 minutos.
IP de origen	Una lista de subredes/rangos/direcciones IP. Si incluye varias direcciones, deben estar separadas por una coma.
Zonas de origen	Le permite agregar una zona predefinida o creada con un rango de direcciones IP haciendo clic en Agregar.

Exclusiones de protección contra ataques por fuerza bruta

Las exclusiones de fuerza de bruta se pueden usar para eliminar la detección de fuerza bruta con criterios específicos. Estas exclusiones se crean a partir de ESET PROTECT en función de la detección por fuerza bruta. Las exclusiones se mostrarán si un administrador crea exclusiones de fuerza bruta en la consola web de ESET PROTECT. Las exclusiones solo pueden contener reglas de permiso y se evalúan antes de las reglas de IDS.

- **Detección** – Tipo de detección

- **Aplicación:** seleccione la ruta de archivos de una aplicación exceptuada haciendo clic en ... (por ejemplo, *C:\Program Files\Firefox\Firefox.exe*). No escriba el nombre de la aplicación.

- **IP remota:** una lista de subredes/rangos/direcciones IPv4 o IPv6 remotos. Las direcciones deben estar separadas por una coma.

Internet y correo electrónico

Puede configurar el filtrado de protocolos, la protección del cliente de correo electrónico, la protección de acceso a la web y el Anti-Phishing para proteger su servidor durante la comunicación por Internet.

Protección del cliente de correo electrónico

Controla toda la comunicación por correo electrónico, protege ante códigos maliciosos y permite elegir la acción para realizar cuando se detecta una infección.

Protección del acceso a la Web

Monitorea la comunicación entre los navegadores web y los servidores remotos, según las disposiciones normativas de HTTP y HTTPS. Esta característica también permite bloquear, permitir o excluir ciertas Direcciones URL.

Filtrado de protocolos

Ofrece una protección avanzada para los protocolos de aplicación y está provista por el motor de exploración ThreatSense. Este control funciona automáticamente, más allá de que se use un navegador web o un cliente de correo electrónico. También funciona para las comunicaciones encriptadas (SSL/TLS).

Protección antiphishing

Le permite bloquear páginas web conocidas por distribuir contenido phishing.

Filtrado de protocolos

El motor de exploración de ThreatSense, que integra múltiples técnicas avanzadas para la exploración de malware, proporciona la protección contra malware para los protocolos de aplicación. El filtrado de protocolos funciona en forma automática, independientemente del navegador de Internet o del cliente de correo electrónico usado. Si está habilitado el filtrado de protocolos, ESET Mail Security verificará las comunicaciones que utilizan protocolos SSL/TLS, vaya a **Internet y correo electrónico** > SSL/TLS.

Habilitar el filtrado del contenido de los protocolos de aplicación

En caso de desactivar el filtrado de protocolos, debe tener en cuenta que muchos componentes de ESET Mail Security (Protección de acceso a la web, Protección de protocolos de correo electrónico y Protección Anti-Phishing) dependen de éste y que no todas sus funciones estarán disponibles.

Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones específicas con reconocimiento de redes,

selecciónelas de la lista. La comunicación HTTP/POP3 de las aplicaciones seleccionadas no se verificará en busca de amenazas. Esta función le permite excluir aplicaciones específicas del filtrado de protocolos. Haga clic en **Editar** y **Agregar** para seleccionar un ejecutable de la lista de aplicaciones y excluirlo del filtrado de protocolos.

Es recomendable usar esta opción solo para aplicaciones que no funcionen correctamente cuando se verifica su comunicación.

Direcciones IP excluidas

Las direcciones IP en esta lista se excluirán del filtrado de protocolos. La comunicación HTTP/POP3/IMAP desde o hacia las aplicaciones seleccionadas no se verificará en busca de amenazas. La comunicación HTTP/POP3/IMAP desde/hacia las direcciones seleccionadas no se revisará en busca de amenazas.

Es recomendable que únicamente use esta opción para las direcciones confiables conocidas.

Haga clic en **Editar** y **Agregar** para especificar la dirección IP, el rango de direcciones o la subred a la que se aplicará la exclusión. Cuando selecciona **Ingresar múltiples valores**, puede agregar varias direcciones IP delimitadas por nuevas líneas, comas, o punto y coma. Cuando se habilita la selección múltiple, las direcciones se mostrarán en la lista de direcciones IP excluidas.

Las exclusiones son útiles cuando el filtrado de protocolos causa problemas de compatibilidad.

Clientes de Internet y correo electrónico

Dada la enorme cantidad de códigos maliciosos que circulan por Internet, la navegación segura es un aspecto crucial para la protección de los equipos. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código malicioso para introducirse en el sistema de incógnito; por este motivo, ESET Mail Security se centra en la seguridad de los navegadores web. Todas las aplicaciones que accedan a la red se pueden marcar como navegadores de internet. Las aplicaciones que ya usan los protocolos para la comunicación o las aplicaciones desde la ruta seleccionada se pueden agregar en la lista de clientes de Internet y correo electrónico.

SSL/TLS

ESET Mail Security tiene la capacidad de buscar amenazas en las comunicaciones que utilizan el protocolo Capa de sockets seguros (SSL) / Seguridad de la capa de transporte (TLS).

Puede usar varios modos de exploración para examinar las comunicaciones protegidas por SSL mediante certificados de confianza, certificados desconocidos o certificados excluidos de la verificación de las comunicaciones protegidas por SSL.

Habilitar el filtrado del protocolo de SSL/TLS

Si se deshabilita el filtrado de protocolos, el programa no explorará las comunicaciones con el protocolo SSL/TLS. El modo de filtrado del protocolo SSL/TLS está disponible en las siguientes opciones:

- **Modo automático**: seleccione esta opción para explorar todas las comunicaciones protegidas por SSL/TLS excepto las protegidas por certificados excluidos de la verificación. Si se establece una nueva comunicación que use un certificado firmado desconocido, no se notificará al usuario y se filtrará la comunicación en

forma automática. Al acceder a un servidor con un certificado no confiable que está marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.

- **Modo interactivo**: si ingresa un nuevo sitio protegido por SSL/TLS (con un certificado desconocido), se mostrará un cuadro de diálogo para la selección de la acción. Este modo le permite crear una lista de certificados SSL/TLS que se excluirán de la exploración.

- **Modo de política**: todas las conexiones de SSL/TLS se filtran, excepto las exclusiones configuradas.

Lista de aplicaciones SSL/TLS filtradas

Agregue una aplicación filtrada y establezca una de las acciones de exploración. Puede usar la lista de aplicaciones filtradas para personalizar la conducta de ESET Mail Security para aplicaciones específicas, y para recordar las acciones elegidas si selecciona el **modo Interactivo** en el **modo de filtrado de protocolos SSL/TLS**.

Lista de certificados conocidos

Le permite personalizar la conducta de ESET Mail Security para certificados SSL específicos. La lista se puede ver y administrar haciendo clic en Editar junto a **Lista de certificados conocidos**.

Excluir comunicación con dominios de confianza

Para excluir la comunicación mediante certificados de validación ampliada de la comprobación de protocolos (banca por Internet).

Bloquear las comunicaciones cifradas con el uso del protocolo obsoleto SSL v2

Las comunicaciones que usen esta versión anterior del protocolo SSL serán automáticamente bloqueadas.

Certificado raíz

Para que la comunicación SSL/TLS funcione correctamente en los navegadores o clientes de correo electrónico, es imprescindible agregar el certificado raíz para ESET a la lista de certificados raíz conocidos (desarrolladores). Agregar el certificado raíz a los navegadores conocidos deberá estar habilitada.

Seleccione esta opción para agregar automáticamente el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox). Para los navegadores que usan el almacén de certificaciones del sistema, el certificado se agrega en forma automática (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no compatibles, haga clic en **Ver el certificado** > **Detalles** > **Copiar en el archivo**... y luego impórtelo manualmente al navegador.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de certificado TRCA

En algunos casos, el certificado de un sitio web no se puede verificar mediante el almacén de **Entidades de certificación de raíz de confianza** (TRCA). Esto significa que alguien firma automáticamente el certificado (por ejemplo, el administrador de un servidor web o una pequeña empresa); por lo que considerar este certificado como confiable no siempre es un riesgo. La mayoría de los negocios (por ejemplo, los bancos) usan un certificado firmado por las TRCA.

Si se selecciona **Preguntar sobre la validez del certificado** (predeterminado), el programa le indicará al usuario que seleccione la acción a realizar cuando se establezca una comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a los sitios con certificados no verificados.

Si el certificado no es válido o está dañado

Esto significa que el certificado está vencido o no fue firmado correctamente. En este caso, es recomendable que deje **Bloquear las comunicaciones que usan el certificado** seleccionado.

Lista de certificados conocidos

Para personalizar el comportamiento de ESET Mail Security para certificados específicos de SSL / TLS, y para recordar las acciones elegidas si se selecciona el **Modo interactivo** en el modo de filtrado de protocolos SSL/TLS. Puede configurar el certificado seleccionado o **Agregar** un certificado desde una URL o archivo.

Una vez que esté en la ventana **Agregar certificado**, haga clic el botón **URL** o **Archivo** y especifique la URL del certificado o busque un archivo de certificado. Los siguientes campos se llenarán automáticamente utilizando los datos del certificado:

- **Nombre del certificado**: nombre del certificado.
- **Emisor del certificado**: nombre del creador del certificado.
- **Sujeto del certificado**: el campo del sujeto identifica la entidad asociada con la clave pública almacenada en el campo de la clave pública del sujeto.

Acción del acceso

- **Automático**: para dar acceso a certificados de confianza y preguntar sobre certificados no confiables.
- **Permitir o Bloquear**: para permitir o bloquear la comunicación asegurada por este certificado, independientemente de su confianza.
- **Preguntar**: para recibir un aviso cuando se encuentre un certificado específico.

Acción de exploración

- **Automático**: para explorar en modo automático y preguntar en modo interactivo.
- **Explorar o ignorar**: para explorar o ignorar la comunicación protegida por este certificado.
- **Preguntar**: recibir un aviso cuando se encuentre un certificado específico.

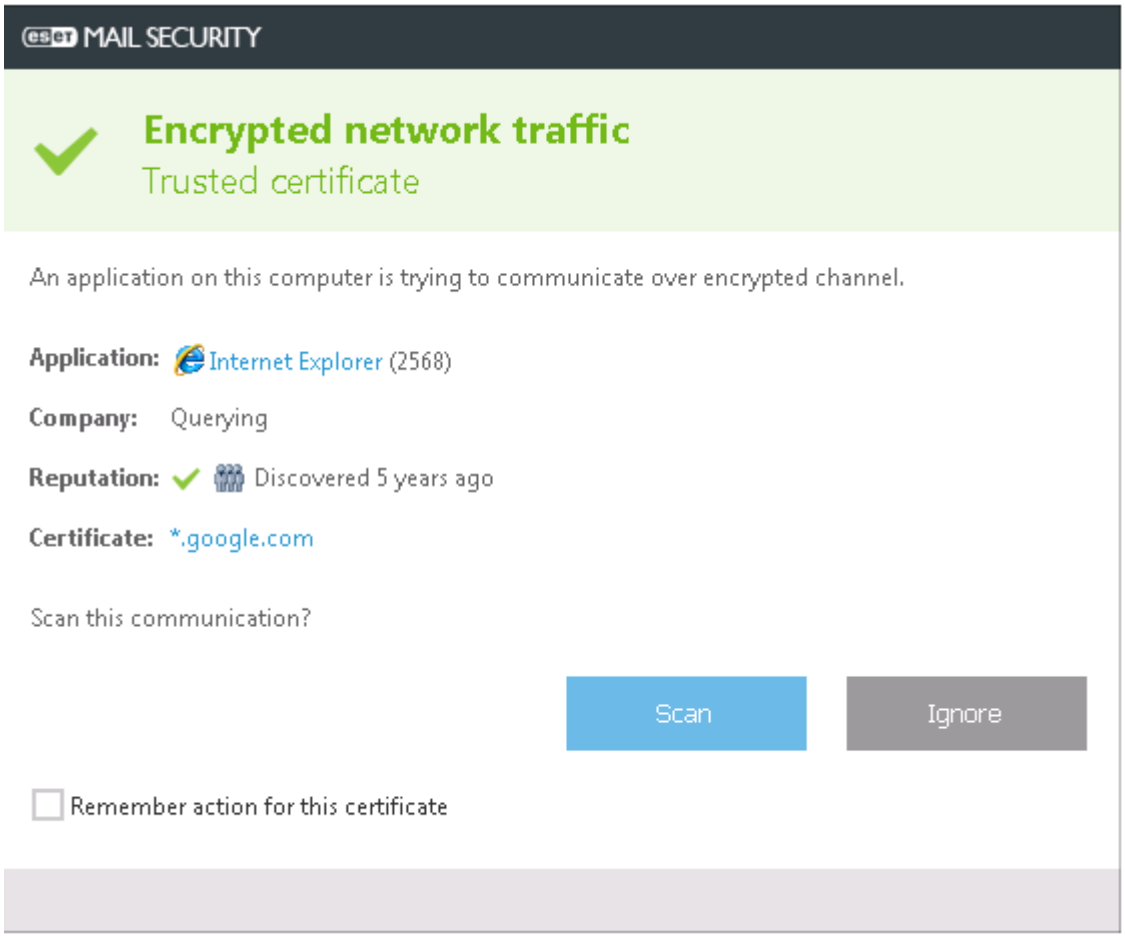
Comunicación cifrada SSL

Si su sistema está configurado para usar una exploración del protocolo SSL, se mostrará una ventana de diálogo para elegir una acción en dos situaciones distintas:

Primero, si un sitio web usa un certificado no válido o que no se puede verificar, y ESET Mail Security está

configurado para preguntarle al usuario en dichos casos (de forma predeterminada, sí para los certificados que no se pueden verificar; no para los que no son válidos), un cuadro de diálogo le preguntará si desea **Permitir** o **Bloquear** la conexión.

Segundo, si el **modo de filtrado de protocolos SSL** está configurado en **Modo interactivo**, un cuadro de diálogo para cada sitio web le preguntará si desea **Explorar** o **Ignorar** el tráfico. Algunas aplicaciones verifican que su tráfico SSL no esté modificado ni inspeccionado por nadie; en dichos casos, ESET Mail Security debe **Ignorar** dicho tráfico para que la aplicación siga funcionando.



En los dos casos, el usuario puede elegir recordar la acción seleccionada. Las acciones guardadas se almacenan en la Lista de certificados conocidos.

Protección del cliente de correo electrónico

La integración de ESET Mail Security con los clientes de correo electrónico incrementa el nivel de protección activa frente a códigos maliciosos en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, esta integración se puede habilitar en ESET Mail Security. Cuando se activa la integración, la barra de herramientas de ESET Mail Security se inserta directamente en el cliente de correo electrónico (la barra de herramientas para las versiones más recientes de Windows Live Mail no se inserta), lo que permite una protección de correo electrónico más eficaz.

Integración con el cliente de correo electrónico

Entre los clientes de correo electrónico actualmente compatibles, se incluyen Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La ventaja principal de este complemento es su independencia respecto al protocolo usado.

Cuando el cliente de correo electrónico recibe un mensaje cifrado, se descifra y se envía al módulo de exploración de virus. Incluso si la integración no está habilitada, la comunicación por correo electrónico permanece protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

Para obtener una lista completa de los clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimiento.

Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada

Si nota que el sistema funciona con mayor lentitud mientras trabaja con su cliente de correo electrónico (solo Microsoft Outlook). Esto puede ocurrir cuando se recupera un correo electrónico desde Kerio Outlook Connector Store, por ejemplo.

Habilitar protección de correo electrónico mediante complementos de clientes de correo

Le permite desactivar la protección del cliente de correo electrónico sin eliminar la integración en su cliente de correo electrónico. Puede deshabilitar todos los complementos a la vez, o selectivamente deshabilitar los siguientes:

- **Correo electrónico recibido**: activa o desactiva la verificación de los mensajes recibidos.
- **Correo electrónico enviado**: activa o desactiva la verificación de los mensajes enviados.
- **Correo electrónico leído**: activa o desactiva la verificación de los mensajes leídos.

Acción para realizar en los correos electrónicos infectados

- **Sin acción**: si se habilita esta opción, el programa identificará los archivos adjuntos infectados, pero dejará intactos los correos electrónicos, sin realizar acción alguna.
- **Eliminar correo electrónico**: el programa notificará al usuario sobre las infiltraciones y eliminará el mensaje.
- **Mover el correo electrónico a la carpeta de elementos eliminados**: los correos electrónicos infectados se enviarán automáticamente a la carpeta de elementos eliminados.
- **Mover el correo electrónico a la carpeta**: los correos electrónicos infectados se enviarán automáticamente a la carpeta especificada.
- **Carpeta**: especificar la carpeta personalizada donde desea mover los correos electrónicos infectados al detectarlos.

Repetir la exploración tras la actualización

Alterna la exploración reiterada luego de actualizar el motor de detección.

Aceptar los resultados de las exploraciones realizadas por otros módulos

Si se selecciona, el módulo de protección de correo electrónico aceptará los resultados de la exploración de otros módulos de protección (POP3, exploración de protocolos IMAP).

Protocolos de correo electrónico

Habilitar protección de correo electrónico mediante el filtrado de protocolos

Los protocolos IMAP y POP3 son los más utilizados para recibir comunicaciones de correo electrónico en una aplicación de cliente de correo electrónico. ESET Mail Security proporciona protección para estos protocolos independientemente del cliente de correo electrónico utilizado.

ESET Mail Security también admite la exploración de los protocolos IMAPS y POP3S, que usan un canal cifrado para transferir información entre el servidor y el cliente. ESET Mail Security verifica la comunicación mediante el SSL (protocolo de capa de conexión segura) y la TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en los puertos usados por los protocolos **IMAPS / POP3S**, independientemente de la versión del sistema operativo.

Configuración del módulo de exploración IMAPS / POP3S

Las comunicaciones cifradas no se explorarán cuando se usen las configuraciones predeterminadas. Para habilitar el escaneado de la comunicación cifrada, navegue hasta Comprobación del protocolo SSL/TLS.

El número de puerto identifica el tipo de puerto. Estos son los puertos de correo electrónico predeterminados para:

Nombre del puerto	Números de puerto	Descripción
POP3	110	Puerto POP3 no cifrado predeterminado.
IMAP	143	Puerto IMAP no cifrado predeterminado.
IMAP seguro (IMAP4-SSL)	585	Habilitar el filtrado del protocolo de SSL/TLS. Los números de puerto múltiples deben delimitarse con una coma.
IMAP4 a través de SSL (IMAPS)	993	Habilitar el filtrado del protocolo de SSL/TLS. Los números de puerto múltiples deben delimitarse con una coma.
POP3 seguro (SSL-POP)	995	Habilitar el filtrado del protocolo de SSL/TLS. Los números de puerto múltiples deben delimitarse con una coma.

Etiquetas de correo electrónico

La protección del correo electrónico proporciona el control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Mediante el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Mail Security proporciona el control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP).

Al examinar los mensajes entrantes, el programa usa todos los métodos avanzados de exploración incluidos en el motor de exploración ThreatSense. Esto significa que la detección de programas maliciosos se lleva a cabo incluso antes de verificar su coincidencia con la base de datos de detección de virus. La exploración de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico usado.

Luego de verificar el correo electrónico, se puede añadir al mensaje una notificación con el resultado de la exploración. Puede seleccionar **Añadir mensajes de etiqueta a los correos electrónicos recibidos y leídos** o **Añadir mensajes de etiqueta a los correos electrónicos enviados**.

Tenga en cuenta que, en ocasiones raras, los mensajes de etiqueta pueden ser omitidos en mensajes HTML

problemáticos o si los mensajes están adulterados por malware. Los mensajes de etiqueta se pueden añadir a los correos electrónicos recibidos y leídos, enviados o a ambas categorías.

Las opciones disponibles son:

- **Nunca**: no se agregará ningún mensaje de etiqueta en absoluto.
- **Cuando ocurre una detección**: únicamente se marcarán como verificados los mensajes que contengan software malicioso (predeterminado).
- **A todos los correos electrónicos explorados**: el programa añadirá mensajes a todos los correos electrónicos explorados.

Texto para agregar al asunto del correo electrónico detectado

Si desea modificar el formato del prefijo en el asunto de un correo electrónico infectado, edite esta plantilla. Esta función reemplazará el asunto del mensaje `Hello` al siguiente formato: `"[detección %DETECTIONNAME%] Hello`. La variable `%DETECTIONNAME%` representa la detección.

Barra de herramientas de Microsoft Outlook

El módulo de protección de Microsoft Outlook funciona como un complemento. Tras instalar ESET Mail Security, se agrega a Microsoft Outlook la siguiente barra de herramientas con las opciones de protección contra malware:

ESET Mail Security

Haga clic en el ícono para abrir la ventana principal del programa de ESET Mail Security.

Exploración reiterada de los mensajes

Permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte la sección Protección del cliente de correo electrónico.

Configuración del módulo de exploración

Muestra las opciones de configuración de la Protección del cliente de correo electrónico.

Barra de herramientas de Outlook Express y Windows Mail

El módulo de protección de Outlook Express y Windows Mail funciona como un complemento. Tras instalar ESET Mail Security, se agrega a Outlook Express o a Windows Mail la siguiente barra de herramientas con las opciones de protección contra malware:

ESET Mail Security

Haga clic en el ícono para abrir la ventana principal del programa de ESET Mail Security.

Exploración reiterada de los mensajes

Permite iniciar la verificación del correo electrónico en forma manual. Puede especificar los mensajes que se van a verificar así como activar la exploración repetida de los correos electrónicos recibidos. Para obtener más información, consulte la sección Protección del cliente de correo electrónico.

Configuración del módulo de exploración

Muestra las opciones de configuración de la Protección del cliente de correo electrónico.

Personalizar la apariencia

Se puede modificar el aspecto de la barra de herramientas según el cliente de correo electrónico. Anule la selección de la opción para personalizar el aspecto de manera independiente a los parámetros del programa de correo electrónico.

- **Mostrar el texto**: muestra las descripciones de los íconos.
- **Texto a la derecha**: las descripciones de las opciones se mueven del sector inferior al lado derecho de los íconos.
- **Íconos grandes**: muestra íconos grandes para las opciones del menú.

Cuadro de diálogo de confirmación

Esta notificación sirve para corroborar que el usuario realmente desee realizar la acción seleccionada, para eliminar posibles errores. El cuadro de diálogo también ofrece la opción de deshabilitar las confirmaciones.

Exploración reiterada de los mensajes

La barra de herramientas de ESET Mail Security, integrada en los clientes de correo electrónico, les permite a los usuarios especificar varias opciones de verificación del correo electrónico. La opción **Volver a explorar los mensajes** ofrece dos modos de exploración:

- **Todos los mensajes de la carpeta actual**: explora los mensajes en la carpeta actualmente abierta.
- **Solo los mensajes seleccionados**: explora únicamente los mensajes marcados por el usuario.
- **Volver a explorar los mensajes ya explorados**: le proporciona al usuario la opción de realizar otra exploración en los mensajes que ya se habían explorado antes.

Protección del acceso a la Web

La función de la protección del acceso a la Web es monitorear la comunicación entre los navegadores Web y los servidores remotos para protegerlo de amenazas en línea, según las disposiciones normativas de HTTP (protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se conocen por contenido malicioso se bloquea antes de que se descargue el contenido. Las demás páginas usar son exploradas por el motor de exploración ThreatSense cuando se cargan, y se bloquean si se detecta contenido malicioso. La protección de acceso a la Web ofrece dos niveles de protección: bloqueo según la lista negra y bloqueo según el contenido.

Básico

Se recomienda firmemente que deje la **Protección de acceso a la web** habilitada. Puede acceder a esta opción desde la ventana principal del programa de principal de ESET Mail Security cuando vaya a **Configuración** > **Internet y correo electrónico** > **Protección del acceso a la Web**.
Activar exploración avanzada de scripts del navegador
De forma predeterminada, el motor de detección verificará todos los programas de JavaScript ejecutados por navegadores de Internet.

Protocolos web

Le permite configurar la supervisión de estos protocolos estándar que son usados por la mayoría de los navegadores de Internet. En forma predeterminada, ESET Mail Security está configurado para supervisar el protocolo HTTP que se usa en la mayoría de los navegadores de Internet.
ESET Mail Security también admite la verificación del protocolo HTTPS. La comunicación de HTTPS usa un canal cifrado para transferir información entre el servidor y el cliente. ESET Mail Security verifica la comunicación mediante los protocolos SSL (protocolo de capa de socket seguro) y TLS (seguridad de la capa de transporte). El programa solo explorará el tráfico en los puertos definidos en **Puertos usados por los protocolos HTTPS**, independientemente de la versión del sistema operativo.
La comunicación cifrada no se explorará cuando se usen las configuraciones predeterminadas. Para habilitar la exploración de la comunicación cifrada, navegue a **Configuración avanzada** (**F5**) > **Internet y correo electrónico** > SSL/TLS.

ThreatSense parámetros

Configuración de ajustes como tipos de análisis (correos electrónicos, archivos, exclusiones, límites, etc.) y métodos de detección para la protección de acceso a la Web.

Administración de direcciones URL

La administración de direcciones URL le permite especificar direcciones HTTP que se bloquearán, autorizarán o excluirán de la comprobación. Los sitios web de la Lista de direcciones bloqueadas no estarán accesibles a no ser que también se incluyan en la Lista de direcciones permitidas. Los sitios web en la lista de direcciones excluidas de la verificación no se exploran en busca de códigos maliciosos cuando se accede a los mismos. El filtrado de protocolos SSL/TLS debe estar habilitado si desea filtrar las direcciones HTTPS además de las páginas Web HTTP. De lo contrario, solo se agregarán los dominios de los sitios HTTPS que haya visitado, y no se agregará la URL completa.

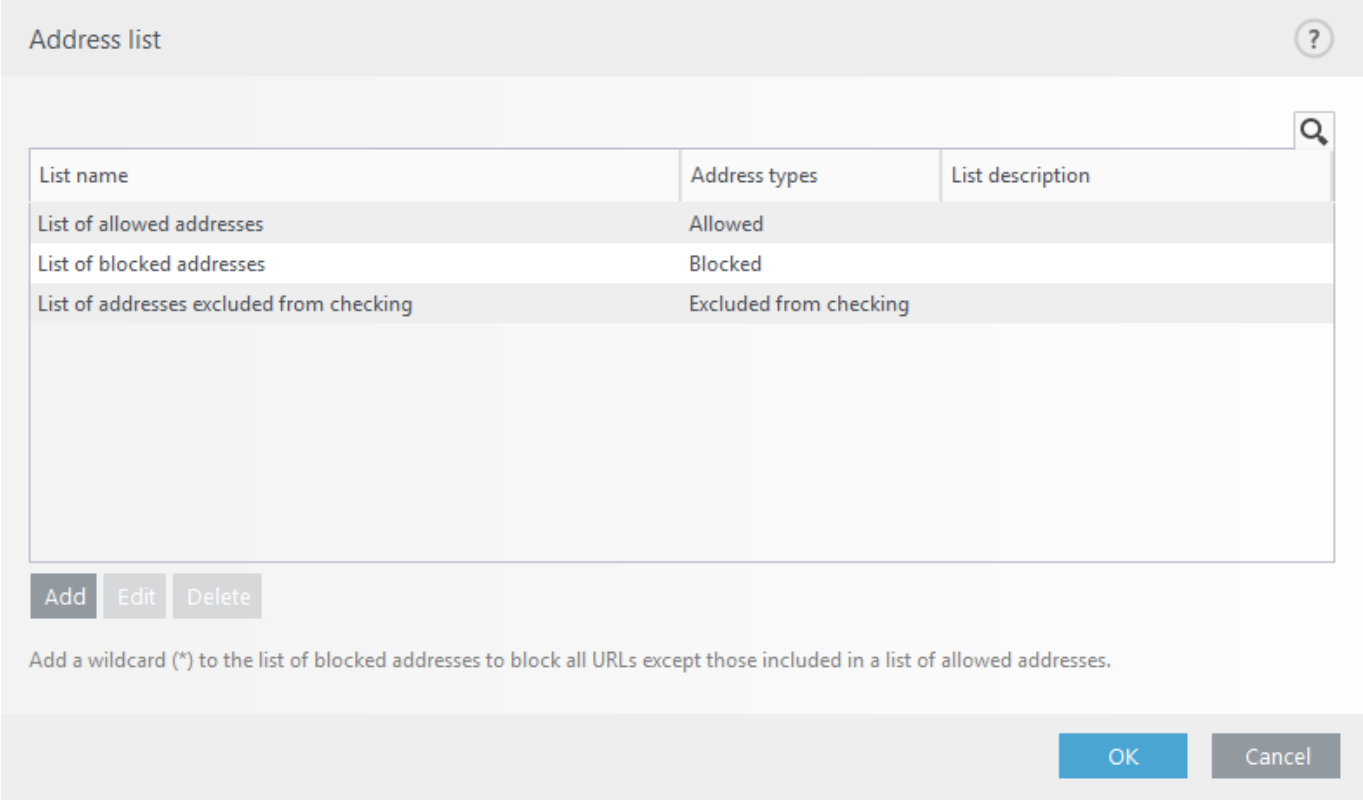
Una lista de direcciones bloqueadas puede contener direcciones de una lista negra pública externa, mientras que una segunda lista puede contener su propia lista negra, lo que facilitaría la actualización de la lista externa y mantendría intacta la suya.

Haga clic en **Editar** y **Agregar** para crear una nueva lista de direcciones además de las predefinidas. Esto puede ser útil si desea separar de manera lógica los diferentes grupos de direcciones. De forma predeterminada, las tres listas siguientes están disponibles:

- **Lista de direcciones excluidas de la verificación**: no se comprobará la existencia de códigos maliciosos en ninguna de las direcciones agregadas a esta lista.

- **Lista de direcciones permitidas**: si se habilita Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas, y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones que se encuentran en esta lista. Las direcciones de esta lista se permiten incluso si están incluidas en la lista de direcciones bloqueadas.

- **Lista de direcciones bloqueadas** : el usuario no tendrá acceso a las direcciones especificadas en esta lista, a menos que también aparezcan en la lista de direcciones permitidas.



Puede **Agregar** una nueva dirección URL a la lista. También puede ingresar múltiples valores con separador. Haga clic en **Editar** para modificar una dirección existente en la lista, o en **Eliminar** para eliminarla. La eliminación sólo es posible para las direcciones creadas con **Agregar**, no para las importadas.

En todas las listas, pueden usarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco representa cualquier número o carácter, mientras que el signo de interrogación representa cualquier carácter. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se usan correctamente en esta lista.

> Si desea bloquear todas las direcciones HTTP excepto las direcciones presentes en la Lista de direcciones permitidas activa, agregue un * a la Lista de direcciones bloqueadas activa.

Creación de una nueva lista

La lista incluirá las direcciones URL/máscaras de dominio que desee bloquear, permitir o excluir de la comprobación. Al crear una nueva lista, especifique lo siguiente:

- **Tipo de lista de direcciones**: elige el tipo (Excluida de la verificación, Bloqueado or Permitido) de la lista desplegable.

- **Nombre de la lista**: especifique el nombre de la lista. Este campo aparecerá en gris cuando se edite una de las tres listas predefinidas.

- **Descripción de la lista**: escriba una breve descripción de la lista (opcional). Aparecerá en gris cuando se edite una de las tres listas predefinidas.

- **Lista activa**: utilice el interruptor para desactivar la lista. Puede activarla más tarde cuando sea necesario.

- **Notificar al aplicar**: si desea que se le notifique cuando se utiliza una lista específica en la evaluación de un sitio HTTP que usted visitó. Se emitirá una notificación si un sitio web está bloqueado o permitido por estar incluido en una lista de direcciones bloqueadas o permitidas. Esta notificación incluirá el nombre de la lista que contiene el sitio web especificado.

- **Severidad de registro**: elija la severidad del registro (Ninguno, Diagnóstico, Información o Advertencia) de la lista desplegable. Los registros con el detalle Advertencia se pueden recopilar por ESET PROTECT.

ESET Mail Security les permite a los usuarios bloquear el acceso a determinados sitios Web para evitar que el navegador de Internet muestre su contenido. Además, permite especificar las direcciones que se van a excluir de la verificación. Si se desconoce el nombre completo del servidor remoto o si el usuario desea especificar un grupo completo de servidores remotos, se pueden usar las máscaras para identificar dicho grupo.

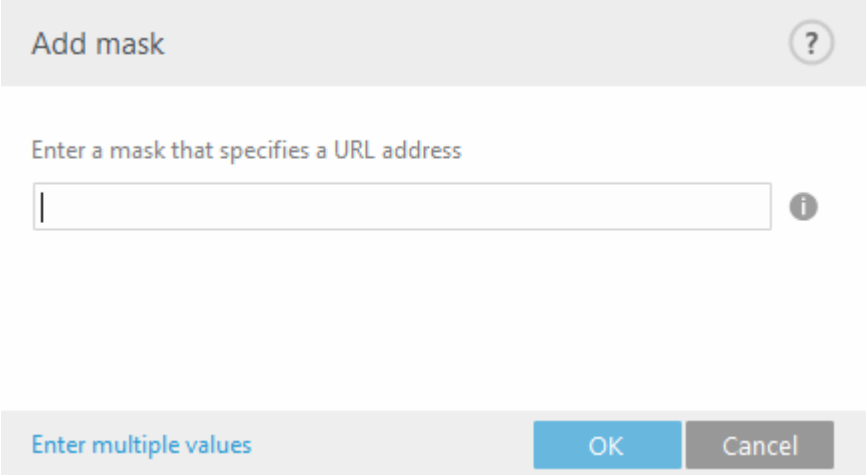
Las máscaras incluyen los símbolos ? y *:

- utilice ? para sustituir un símbolo

- utilice * para sustituir una cadena de texto

✔ **.c?m* se aplica a todas las direcciones cuya última parte comience por la letra c, termine por la letra m y contenga un símbolo desconocido entre las dos (*.com*, *.cam*, etc.).

Una primera secuencia *. se trata de modo especial si se utiliza al comienzo del nombre del dominio. Primero, el comodín * no puede representar un carácter de barra ("/") es este caso. Esto es para evitar evadir la máscara, por ejemplo la máscara *.domain.com no coincidirá con *https://anydomain.com/anypath#.domain.com* (dicho sufijo puede anexarse a cualquier URL sin afectar la descarga). Y segundo, el *. también coincide con una cadena vacía en este caso especial. Esto es para que sea posible que coincida todo el dominio incluidos los subdominios mediante una sola máscara. Por ejemplo la máscara *.domain.com también coincide con *https://domain.com*. Utilizar *domain.com sería incorrecto, ya que también coincidiría con https://anotherdomain.com..



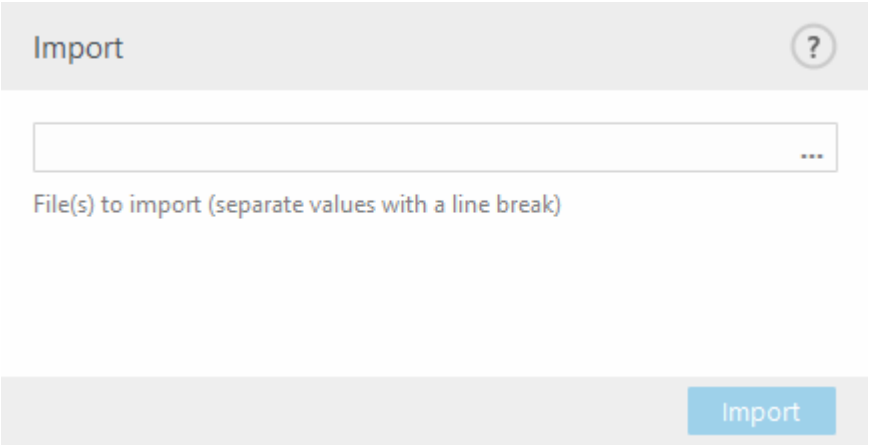
Ingresar valores múltiples

Puede agregar varias direcciones URL delimitadas por líneas, comas, o punto y coma. Cuando se habilita la selección múltiple, las direcciones se mostrarán en la lista.

Importar

Archivo de texto con direcciones URL para importar (valores separados por un salto de línea, por ejemplo `*.txt`

con la codificación UTF-8).

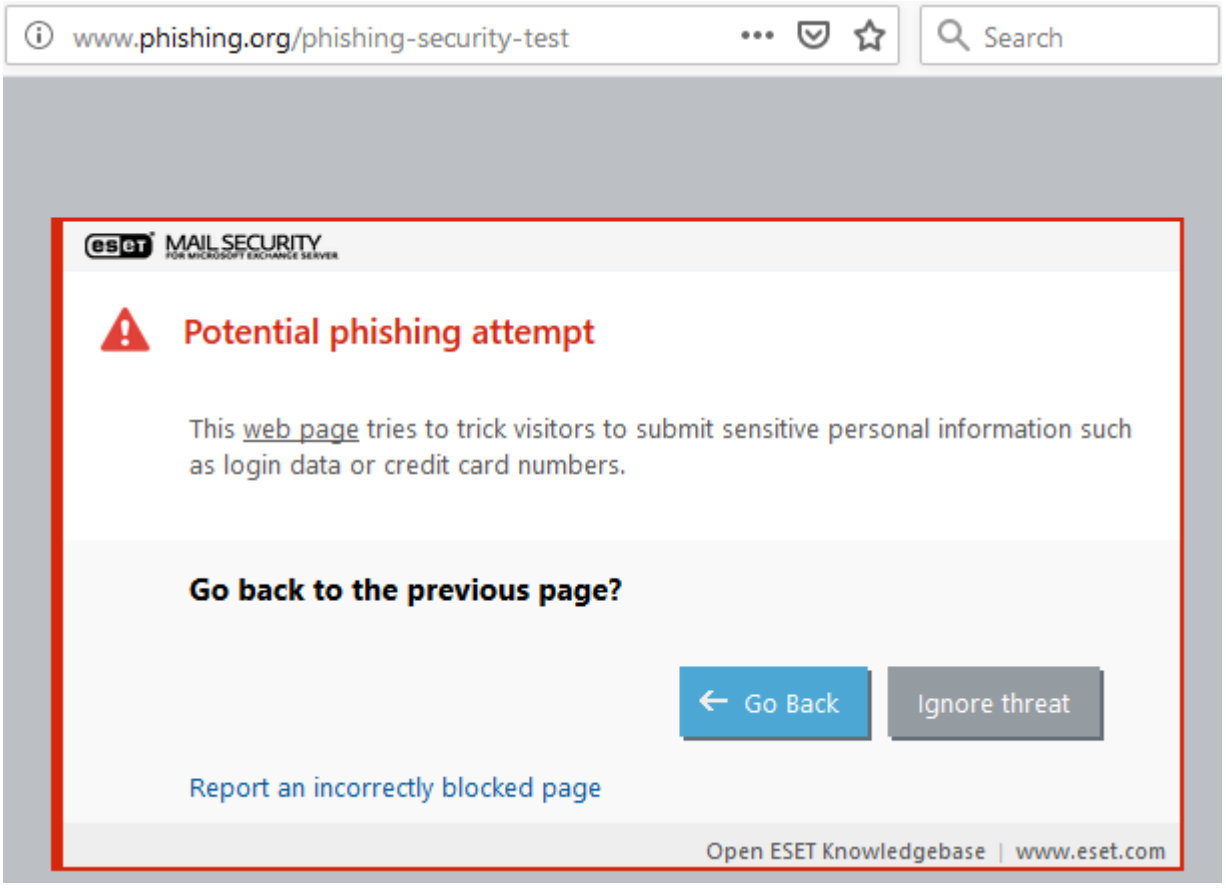


Protección web Anti-Phishing

El término phishing define una actividad criminal que usa la ingeniería social (manipula a los usuarios para obtener información confidencial). El phishing suele usarse para obtener el acceso a datos confidenciales, como números de cuentas bancarias, códigos de identificación personal y más.

ESET Mail Security incluye protección anti-phishing, que bloquea páginas web conocidas por distribuir este tipo de contenido. Le recomendamos firmemente que habilite Anti-Phishing en ESET Mail Security. Visite nuestro Artículo de la base de conocimiento para obtener más información acerca de la protección anti-phishing en ESET Mail Security.

Cuando acceda a un sitio web de phishing reconocido, se mostrará el siguiente diálogo en su navegador web. Si aún desea acceder al sitio web, haga clic en **Ignorar amenaza** (no recomendado).



> Los posibles sitios web de phishing de la lista blanca se vencerán, de forma predeterminada, luego de algunas horas. Para permitir un sitio web de manera permanente, use la herramienta Administración de direcciones URL.

Informar una página de phishing

En caso de que se encuentre con un sitio web sospechoso que parezca ser phishing u otro tipo de ataque malicioso, puede informar a ESET para su análisis. Antes de enviar un sitio web a ESET, asegúrese de que cumpla con uno o más de los siguientes criterios:

- el programa directamente no detecta el sitio web
- el programa detecta erróneamente el sitio usar como una amenaza. En este caso, puede Informar un sitio de phishing falso positivo.

Como alternativa, puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Recuerde usar un asunto descriptivo y proporcionar la mayor cantidad de información posible sobre el sitio web (por ejemplo, el sitio web que se lo recomendó, cómo se enteró de este sitio web, etc.).

Control de dispositivos

ESET Mail Security incluye el control del dispositivo automático (CD/DVD/USB/). Este módulo permite explorar, bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado. Resulta útil si el administrador del equipo desea prevenir el uso de dispositivos con contenido no deseado.

> Al habilitar el control de dispositivos utilizando el interruptor **Integrar al sistema**, se activará la función de control de dispositivos de ESET Mail Security. No obstante, es necesario reiniciar el sistema para que este cambio se aplique.

Se activará el Control del dispositivo, permitiéndole editar su configuración. Si se detecta un dispositivo bloqueado por una regla existente, se visualizará una ventana de notificación y no se otorgará el acceso al dispositivo.

Reglas

Una regla de control del dispositivo define la acción que se tomará cuando un dispositivo, que cumple con los criterios de las reglas, se conecte al equipo.

Grupos

Al hacer clic en Editar, podrá administrar grupos de dispositivos. Cree un nuevo Grupo de dispositivos o seleccione uno existente para agregar o quitar dispositivos de la lista.

> Puede ver las entradas de registro de control del dispositivo en Archivos de registro.

Reglas del dispositivo

Los dispositivos específicos pueden ser permitidos o bloqueados por el usuario, el grupo de usuarios, o cualquiera de los varios parámetros adicionales que se pueden especificar en la configuración de reglas. La lista de reglas

contiene varias descripciones de cada regla, tales como el nombre, el tipo de dispositivo externo, la acción que se realizará después de detectar un nuevo dispositivo y la gravedad de registro.

Puede **Agregar** una nueva regla o modificar la configuración de una existente. Ingrese una descripción de la regla en el campo **Nombre** para tener una mejor identificación. Haga clic en el interruptor junto a **Regla habilitada** para deshabilitar o habilitar esta regla; esto puede ser útil si no desea eliminar la regla permanentemente.

Aplicar durante

Puede restringir las reglas a través de Intervalos de tiempo. Primero cree el intervalo de tiempo, que aparecerá en el menú desplegable.

Tipo de dispositivo

Elija el tipo de dispositivo externo desde el menú desplegable (Almacenamiento en disco/Dispositivo portátil/Bluetooth/FireWire/...). Los tipos de dispositivos se heredan del sistema operativo y se pueden ver en el administrador de dispositivos del sistema siempre y cuando un dispositivo esté conectado al equipo. Los dispositivos de almacenamiento incluyen los discos externos o los lectores de tarjetas de memoria convencionales conectados por medio de USB o FireWire. Los lectores de tarjetas inteligentes incluyen todos los lectores de tarjetas inteligentes con un circuito integrado, tal como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras; estos dispositivos no proporcionan información sobre usuarios, únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

Acción

El acceso a los dispositivos que no son de almacenamiento se puede permitir o bloquear. Por el contrario, las reglas para los dispositivos de almacenamiento le permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/escritura** – se permitirá el acceso total al dispositivo.
- **Bloquear** – se bloqueará el acceso al dispositivo.
- **Solo lectura** – solo se permitirá el acceso de lectura al dispositivo.
- **Advertir** – siempre que se conecte un dispositivo, se le notificará al usuario si está permitido/bloqueado, y se generará una entrada de registro. Los dispositivos no se recuerdan, pero aún se mostrará una notificación en las conexiones posteriores del mismo dispositivo.

> i Observe que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivo. Si un dispositivo tiene espacio de almacenamiento, las cuatro acciones estarán disponibles. Para los dispositivos de no almacenamiento, solo existen dos (por ejemplo, la acción **Solo lectura** no está disponible para Bluetooth, entonces los dispositivos Bluetooth solo se pueden permitir o bloquear).

Tipo de criterios

Los parámetros adicionales que figuran a continuación se pueden usar para ajustar las reglas y personalizarlas para los dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID del proveedor.
- **Modelo** – el nombre determinado del dispositivo.

- **Número de serie**: los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.

> ℹ Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de todos los campos de texto distinguen entre mayúsculas y minúsculas, y admiten comodines (el signo de interrogación (?) representa un solo carácter, mientras que el asterisco (*) representa una cadena de cero o más caracteres).

Con el fin de descifrar los parámetros de un dispositivo, cree una regla para permitir ese el tipo de dispositivo, conecte el dispositivo a su equipo y luego revise los detalles del dispositivo en el Registro de control del dispositivo.

Elija la **Severidad de registro** de la lista desplegable:

- **Siempre** – registra todos los eventos.
- **Diagnóstico** – registra la información necesaria para ajustar el programa.
- **Información** – registra los mensajes de información, incluidos los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencia** – registra los errores críticos y mensajes de advertencia.
- **Ninguno** – no se realizará registro alguno.

Las reglas se pueden limitar a ciertos usuarios o grupos de usuarios al agregarlos a la Lista de usuarios. Haga clic en **Editar** para administrar la **lista de usuarios**.

- **Agregar** – abre el cuadro de diálogo Tipos de objeto: Usuarios o grupos, que le permite seleccionar los usuarios que desee.
- **Eliminar** – elimina al usuario seleccionado del filtro.

> ℹ todos los dispositivos se pueden filtrar por reglas del usuario, (por ejemplo: los dispositivos de imagen no proporcionan información sobre usuarios, únicamente sobre acciones invocadas).

Se encuentran disponibles las siguientes funciones:

Editar

Le permite modificar el nombre de una regla o parámetros seleccionados de los dispositivos contenidos allí (proveedor, modelo, número de serie).

Copiar

Crea una nueva regla basada en los parámetros de la regla seleccionada.

Eliminar

En caso de que desee eliminar la regla seleccionada. Como alternativa, puede utilizar la casilla de verificación situada junto a una regla determinada para desactivarla. Esto puede ser útil si no desea eliminar una regla en forma permanente para que pueda usarla en el futuro.

Llenar

Proporciona una visión general de todos los dispositivos actualmente conectados con la siguiente información: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible). Cuando seleccione un dispositivo (en la lista de Dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede ajustar todas las configuraciones).

Las reglas se incluyen en la lista por orden de prioridad, con las reglas de prioridad más alta en la parte superior. Puede seleccionar varias reglas y aplicar acciones, tal como eliminarlas o moverlas hacia arriba o abajo en la lista, al hacer clic en **Superior**/**Arriba**/**Abajo**/**Inferior** (botones de flechas).

Grupos de dispositivos

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo respectivo, y la parte izquierda de la ventana contiene una lista de los grupos existentes. Seleccione el grupo que contiene los dispositivos que desea mostrar en el panel derecho.

Puede crear distintos grupos de dispositivos para los que se aplicarán reglas diferentes. También puede crear un grupo único de dispositivos configurados como de **Lectura**/**Escritura** o **Solo lectura**. Esto garantiza que el Control de dispositivos bloqueará los dispositivos no reconocidos cuando se conectan a su equipo.

Tener un dispositivo externo conectado a su equipo puede presentar un riesgo de seguridad.

Se encuentran disponibles las siguientes funciones:

Agregar

Puede crear un nuevo grupo de dispositivos al ingresar su nombre, o un dispositivo a un grupo existente (de manera opcional, puede especificar detalles como el nombre del proveedor, modelo y número de serie), dependiendo de la parte de la ventana en la que ha hecho clic en el botón.

Editar

Le permite modificar el nombre de un grupo seleccionado o los parámetros de los dispositivos contenidos allí (proveedor, modelo, número de serie).

Eliminar

Elimina el grupo o dispositivo seleccionado, dependiendo del lugar de la ventana en el que hizo clic. Como alternativa, puede utilizar la casilla de verificación situada junto a una regla determinada para desactivarla. Esto puede ser útil si no desea eliminar una regla en forma permanente para que pueda usarla en el futuro.

Importar

Importa una lista de dispositivos desde un archivo. Cada dispositivo se inicia en la línea nueva.

El proveedor, **el modelo** y **el número de serie** deben estar presentes en cada dispositivo y separados con una coma.

Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Llenar

Proporciona una visión general de todos los dispositivos actualmente conectados con la siguiente información: el tipo de dispositivo, el proveedor del dispositivo, el modelo y el número de serie (si está disponible). Cuando seleccione un dispositivo (en la lista de Dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede ajustar todas las configuraciones).

Agregar dispositivo

Haga clic en Agregar en la ventana derecha para agregar un dispositivo a un grupo existente. Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas de diferentes dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas y admiten comodines (*, ?):

- **Proveedor** – filtre por nombre o ID del proveedor.
- **Modelo** – el nombre determinado del dispositivo.
- **Número de serie** – los dispositivos externos generalmente tienen sus propios números de serie. En caso de un CD/DVD, este es el número de serie que corresponde al medio determinado, no a la unidad de CD.
- **Descripción**: descripción del dispositivo para una mejor organización.

> Si no se definen estos parámetros, la regla ignorará estos campos mientras realiza la coincidencia. Los parámetros de filtrado de todos los campos de texto distinguen entre mayúsculas y minúsculas, y admiten comodines (el signo de interrogación (?) representa un solo carácter, mientras que el asterisco (*) representa una cadena de cero o más caracteres).

Tras crear un grupo de dispositivos, tendrá que agregar una nueva regla de control del dispositivo para el grupo de dispositivos creado y elegir la acción que desea realizar.

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** para salir de la ventana **Grupos de dispositivos** sin guardar los cambios.

> Observe que no todos los derechos (Acciones) están disponibles para todos los tipos de dispositivo. Si un dispositivo tiene espacio de almacenamiento, las cuatro acciones estarán disponibles. Para los dispositivos de no almacenamiento, solo existen dos (por ejemplo, la acción Solo lectura no está disponible para Bluetooth, entonces los dispositivos Bluetooth solo se pueden permitir o bloquear).

Configuración de herramientas

Puede personalizar la configuración avanzada para:

- Intervalos de tiempo
- Microsoft Windows® Update
- ESET CMD
- ESET RMM
- Licencia

- Proveedor WMI
- Destinos de las exploraciones de la consola de administración de ESET
- Archivos de registro
- Servidor proxy
- Modo presentación
- Diagnósticos
- Clúster

Intervalos de tiempo

Los intervalos de tiempo se utilizan dentro de las Reglas de control del dispositivo, que limitan las normas cuando son aplicados. Cree un intervalo de tiempo y selecciónelo al añadir reglas nuevas o modificar las existentes (parámetro **Aplicar durante**). Esto permite definir intervalos de tiempo utilizados comúnmente (horario de trabajo, fin de semana, etc.) y reutilizarlos de forma sencilla sin tener que volver a definirlos para cada regla. Un intervalo de tiempo debe poder aplicarse a cualquier tipo de regla pertinente que apoye el control basado en el tiempo.

Actualización de Microsoft Windows

Las actualizaciones de Windows proporcionan las reparaciones importantes para las vulnerabilidades potencialmente peligrosas y mejoran el nivel general de seguridad en su equipo. Por ese motivo, es imprescindible instalar las actualizaciones de Microsoft Windows en cuanto estén disponibles. ESET Mail Security lo mantendrá notificado sobre las actualizaciones faltantes según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá la descarga de ninguna actualización del sistema.
- **Actualizaciones opcionales**: las actualizaciones marcadas como de baja prioridad y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones recomendadas**: las actualizaciones marcadas como comunes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones importantes**: las actualizaciones marcadas como importantes y las de importancia mayor se ofrecerán para descargar.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de las actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará tras la verificación del estado con el servidor de actualización. Es posible que la información de actualización del sistema no esté disponible de inmediato después de guardar los cambios.

Explorador de la línea de comandos

Como alternativa a eShell, puede ejecutar el explorador a pedido ESET Mail Security desde la línea de comandos con `ecls.exe`, ubicado en la carpeta de instalación.

A continuación se muestra una lista de parámetros y conmutadores:

Opciones:

`/base-dir=FOLDER`	cargar módulos desde CARPETA
`/quar-dir=FOLDER`	FOLDER de cuarentena
`/exclude=MASK`	excluir de la exploración los archivos que coinciden con MASK
`/subdir`	explorar las subcarpetas (predeterminado)
`/no-subdir`	no explorar las subcarpetas
`/max-subdir-level=LEVEL`	subnivel máximo de carpetas dentro de las carpetas que se van a explorar
`/symlink`	seguir los vínculos simbólicos (predeterminado)
`/no-symlink`	saltear los vínculos simbólicos
`/ads`	explorar ADS (predeterminado)
`/no-ads`	no explorar ADS
`/log-file=FILE`	registrar salida en FILE
`/log-rewrite`	sobrescribir archivo de salida (predeterminado: añadir)
`/log-console`	registrar resultados en la consola (predeterminado)
`/no-log-console`	no registrar resultados en la consola
`/log-all`	también incluir en el registro los archivos limpios
`/no-log-all`	no registrar los archivos limpios (predeterminado)
`/aind`	mostrar indicador de actividad
`/auto`	explorar y desinfectar todos los discos locales automáticamente

Opciones del módulo de exploración:

`/files`	explorar los archivos (predeterminado)
`/no-files`	no explorar los archivos
`/memory`	explorar la memoria
`/boots`	explorar los sectores de inicio
`/no-boots`	no explorar los sectores de inicio (predeterminado)
`/arch`	explorar los archivos comprimidos (predeterminado)
`/no-arch`	no explorar los archivos comprimidos
`/max-obj-size=SIZE`	solo explorar archivos menores que SIZE megabytes (predeterminado 0 = ilimitado)
`/max-arch-level=LEVEL`	subnivel máximo de archivos comprimidos dentro de los archivos comprimidos (anidados) que se van a explorar
`/scan-timeout=LIMIT`	explorar los archivos comprimidos durante LIMIT segundos como máximo

/max-arch-size=SIZE	solo explorar los archivos en un archivo comprimido si son menores que SIZE (predeterminado 0 = ilimitado)
/max-sfx-size=SIZE	solo explorar archivos dentro de un archivo comprimido de autoextracción si son menores que SIZE megabytes (predeterminado 0 = ilimitado)
/mail	explorar los archivos de correo electrónico (predeterminado)
/no-mail	no explorar los archivos de correo electrónico
/mailbox	explorar buzones de correo (predeterminado)
/no-mailbox	no explorar los buzones de correo
/sfx	explorar los archivos comprimidos de autoextracción (predeterminado)
/no-sfx	no explorar los archivos comprimidos de autoextracción
/rtp	explorar los empaquetadores de tiempo de ejecución (predeterminado)
/no-rtp	no explorar los empaquetadores de tiempo de ejecución
/unsafe	explorar en búsqueda de aplicaciones potencialmente no seguras
/no-unsafe	no explorar en búsqueda de aplicaciones potencialmente no seguras (predeterminado)
/unwanted	explorar en búsqueda de aplicaciones potencialmente no deseadas
/no-unwanted	no explorar en búsqueda de aplicaciones potencialmente no deseadas (predeterminado)
/suspicious	explorar en busca de aplicaciones sospechosas (predeterminado)
/no-suspicious	no explorar en busca de aplicaciones sospechosas
/pattern	usar firmas (predeterminado)
/no-pattern	no usar firmas
/heur	habilitar la heurística (predeterminado)
/no-heur	deshabilitar la heurística
/adv-heur	habilitar la heurística avanzada (predeterminado)
/no-adv-heur	deshabilitar la heurística avanzada
/ext-exclude=EXTENSIONS	excluir las EXTENSIONES de archivos delimitadas por dos puntos de la exploración
/clean-mode=MODE	usar el MODO de limpieza para objetos infectados Se encuentran disponibles las siguientes opciones: • none (predeterminado): no se realizará la limpieza automática. • standard: ecls.exe intentará limpiar o quitar automáticamente los archivos infectados. • strict: ecls.exe intentará limpiar o quitar automáticamente los archivos infectados sin intervención del usuario (no se le consultará antes de quitar los archivos). • rigorous: ecls.exe quitará los archivos sin intentar limpiarlos, sea cual sea el archivo. • delete: ecls.exe quitará los archivos sin intentar limpiarlos, pero no quitará archivos delicados como los archivos del sistema de Windows.
/quarantine	copiar archivos infectados (si se han limpio) a la cuarentena (complementa la acción realizada durante la limpieza)
/no-quarantine	no copiar los archivos infectados a cuarentena

Opciones generales:

/help	mostrar la ayuda y salir
/version	mostrar información de la versión y salir
/preserve-time	preservar el último acceso con su fecha y hora

Códigos de salida:

0	no se detectó ninguna amenaza
1	se detectó una amenaza y se desinfectó
10	algunos archivos no se pudieron explorar (pueden ser amenazas)
50	amenaza detectada
100	error (los códigos de salida superiores a 100 significan que no se ha explorado el archivo y que no se puede considerar limpio)

ESET CMD

Esta es una característica que permite comandos avanzados de ecmd. Le permite exportar e importar la configuración usando la línea de comandos (ecmd.exe). Hasta ahora, solo era posible exportar la configuración usando la interfaz gráfica de usuarioESET Mail Security Se puede exportar la configuración en un archivo *.xml*.

Cuando haya habilitado ESET CMD, encontrará dos métodos de autorización disponibles:

- **Ninguno**: sin autorización. No recomendamos este método porque permite la importación de cualquier configuración no firmada, lo cual es un riesgo potencial.

- **Contraseña de configuración avanzada**: se necesita una contraseña para importar una configuración desde un archivo .xml, este archivo debe estar firmado (consulte la configuración de firma del archivo .xml más adelante). La contraseña especificada en Configuración de acceso se debe brindar antes de poder importar una nueva configuración. Si no tiene acceso a la configuración habilitada, su contraseña no coincide o el archivo de configuración .xml no está firmado, la configuración no se importará.

Una vez habilitado ESET CMD, puede usar la línea de comandos para exportar/importar la configuración de ESET Mail Security. Puede hacerlo manualmente o crear un script con el propósito de la automatización.

Para utilizar comandos avanzados de ecmd, debe ejecutarlos con privilegios de administrador o abrir el Símbolo de comandos de Windows (cmd) utilizando **Ejecutar como administrador**. De lo contrario, verá un mensaje de **Error al ejecutar el comando**. Además, al exportar una configuración, debe existir la carpeta de destino. El comando de exportar sigue funcionando cuando la configuración CMD de ESET se encuentra apagada.

Comando de exportar la configuración:
```
ecmd /getcfg c:\config\settings.xml
```

Comando de importar la configuración:
```
ecmd /setcfg c:\config\settings.xml
```

Los comandos ecmd avanzados sólo se pueden ejecutar localmente. Ejecutar la tarea de cliente **Ejecutar comando** mediante ESET PROTECT no funcionará.

Firmar un archivo de configuración *.xml*:

1. Descargue el archivo ejecutable XmlSignTool.

2. Abra un símbolo de Windows Command Prompt (cmd) y seleccione **Ejecutar como administrador**.

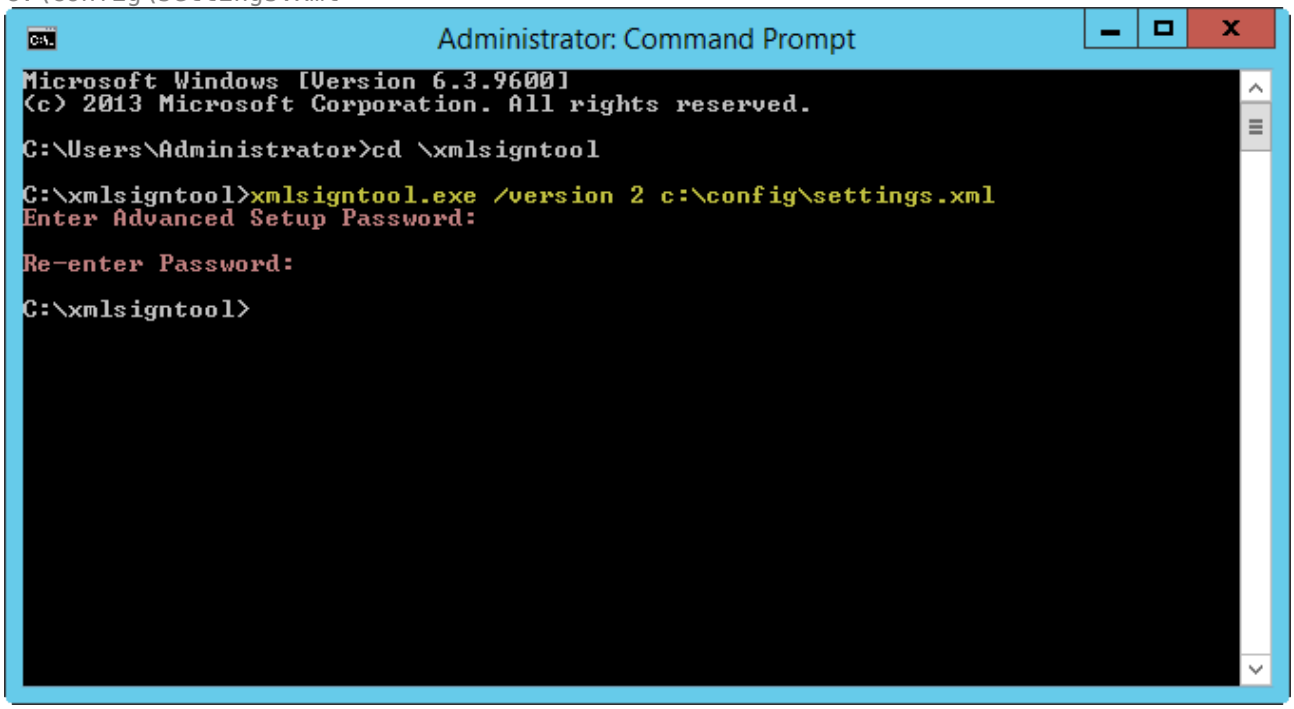
3. Diríjase hasta la ubicación del `xmlsigntool.exe`.

4. Ejecute un comando para firmar el archivo de configuración *.xml*, uso: `xmlsigntool /version 1|2 <xml_file_path>`

El valor del parámetro `/version` depende de la versión de su ESET Mail Security. Use `/version 2` para ESET Mail Security 7 y superior.

5. Ingrese y vuelva a ingresar la contraseña de Configuración avanzada cuando XmlSignTool lo solicite. Su archivo de configuración *.xml* ahora se encuentra firmado y se podrá utilizar para importar en otra instancia de ESET Mail Security con ESET CMD utilizando el método de autorización con contraseña.

Comando de archivo de configuración firmado y exportado: `xmlsigntool /version 2 c:\config\settings.xml`



Si modifica la contraseña de la Configuración de acceso y desea importar la configuración firmada anteriormente con una contraseña antigua, podrá volver a firmar el archivo de configuración *.xml* usando la contraseña actual. Esto le permite usar un archivo de configuración anterior sin exportarlo a otro equipo que ejecute ESET Mail Security antes de la importación.

ESET RMM

El control y la administración remotos (RMM) es el proceso de supervisión y control de sistemas de software (como los de escritorios, servidores y dispositivos móviles) por medio de un agente instalado de forma local al que puede acceder un proveedor de servicios de administración.

Habilitar RMM

El comando de control y la administración remotos es funcional. Es necesario tener privilegios de administrador para utilizar la utilidad RMM.

Modo de funcionamiento

Seleccione el modo de funcionamiento de RMM desde el menú desplegable.

- **Solo separación segura**: si quiere habilitar la interfaz RMM para operaciones seguras de solo lectura
- **Todas las operaciones**: si quiere habilitar la interfaz RMM para todas las operaciones

Método de autorización

Establezca el método de autorización de RMM desde el menú desplegable:

- **Ninguno**: No se efectuará ninguna comprobación de la ruta de aplicación, puede ejecutar ermm.exe desde cualquier aplicación
- **Ruta de aplicaciones**: Especifica qué aplicación tiene permitido ejecutar ermm.exe

La instalación predeterminada de ESET Mail Security contiene el archivo *ermm.exe* ubicado en ESET Mail Security (ruta predeterminada *c:\Program Files\ESET\ESET Mail Security*). *ermm.exe* de intercambio de datos con el complemento RMM, que se comunica con el Agente RMM, vinculado al servidor RMM.

- *ermm.exe*: Utilidad de línea de comandos desarrollada por ESET que posibilita la administración de productos de Endpoint y la comunicación con cualquier complemento RMM.
- Complemento RMM – Una aplicación de terceros que se ejecuta a nivel local en sistemas Endpoint de Windows. El complemento fue diseñado para comunicarse con un agente RMM específico (por ejemplo, solo Kaseya) y con *ermm.exe*.
- Agente RMM – Una aplicación de terceros (por ejemplo, Kaseya) ejecutada de forma local en el sistema Endpoint para Windows. El agente se comunica con un complemento RMM y con un servidor RMM.
- Servidor RMM – Se ejecuta como un servicio en un servidor de terceros. Los sistemas RMM compatibles son de Kaseya, Labtech, Autotask, Max Focus y Solarwinds N-able.

Visite nuestro Artículo de la base de conocimiento para obtener más información acerca de ESET RMM en ESET Mail Security.

Complementos de ESET Direct Endpoint Management para soluciones RMM de terceros

RMM se ejecuta como servicio en un servidor de terceros. Para más información, consulte las siguientes guías del usuario en línea de ESET Direct Endpoint Management:

- Complemento de ESET Direct Endpoint Management para ConnectWise Automate
- Complemento de ESET Direct Endpoint Management para DattoRMM
- ESET Direct Endpoint Management para Solarwinds N-Central
- ESET Direct Endpoint Management para NinjaRMM

Licencia

ESET Mail Security se conecta al servidor de Licencia de ESET algunas veces por hora para realizar verificaciones. El parámetro **Verificación de intervalo** se encuentra configurado como **Automático** de manera predeterminada. Si quiere reducir el tráfico de red que provocan las verificaciones de licencias, cambie la verificación de intervalo a **Limitada** y la verificación de licencias se realizará una sola vez por día (también luego del reinicio del servidor).

Cuando la verificación de intervalos está definida como **Limitada**, todos los cambios relacionados con las licencias que se realizan en ESET Mail Security a través de ESET Business Account y ESET MSP Administrator pueden demorar hasta un día en aplicarse.

Proveedor WMI

La Instrumentación para la administración de Windows (WMI) es la implementación de Microsoft de Web-Based Enterprise Management (WBEM, gestión de empresa basada en la web), una iniciativa de la industria para desarrollar una tecnología estándar para acceder a la información de gestión en un entorno empresarial.

Para obtener más información sobre WMI, consulte
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

Proveedor WMI de ESET

El propósito del Proveedor WMI de ESET es permitir la supervisión remota de los productos de ESET en un entorno empresarial sin necesitar ningún software o herramientas específicos de ESET. Al exponer la información del producto básico, el estado y las estadísticas a través de WMI, ampliamos considerablemente las posibilidades de los administradores empresariales en la supervisión de los productos de ESET.

Los administradores pueden aprovechar el número de métodos de acceso que WMI ofrece (línea de comandos, scripts y herramientas de supervisión empresarial de terceros) para supervisar el estado de sus productos de ESET.

La implementación actual proporciona acceso de solo lectura para la información básica del producto, las funciones instaladas y su estado de protección, las estadísticas de exploraciones individuales y los archivos de registro de los productos.

El proveedor de WMI permite el uso de la infraestructura y las herramientas estándar de Windows WMI para leer el estado del producto y de los registros del producto.

Datos proporcionados

Todas las clases de WMI relacionadas con el producto de ESET se encuentran en el espacio de nombres “raíz/ESET”. Las siguientes clases, que se describen en detalle a continuación, están implementadas actualmente:

General

- ESET_Product
- ESET_Features

- ESET_Statistics

Registros

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

Clase ESET_Product

Solo puede haber una instancia para la clase ESET_Product. Las propiedades de esta clase se refieren a la información básica sobre su producto de ESET instalado:

- ID: identificador del tipo de producto, por ejemplo, “emsl”
- Name: nombre del producto, por ejemplo, “ESET Mail Security”
- FullName: nombre completo del producto, por ejemplo, “ESET Mail Security para IBM Domino”
- Version: versión del producto, por ejemplo, "6.5.14003.0"
- VirusDBVersion: versión de la base de datos de virus, por ejemplo, “14533 (20161201)”
- VirusDBLastUpdate: fecha y hora de la última actualización de la base de datos de virus. La cadena contiene la fecha y la hora en el formato de fecha y hora de WMI, por ejemplo, “20161201095245.000000+060”
- LicenseExpiration: tiempo de expiración de la licencia. La cadena contiene la fecha y la hora en el formato de fecha y hora de WMI
- KernelRunning: Valor booleano que indica si el servicio ekrn se está ejecutando en la máquina, por ejemplo, "TRUE”

- StatusCode – el número que indica el estado de protección del producto: 0 – verde (correcto), 1 – amarillo (advertencia), 2 – rojo (error)

- StatusText: mensaje que describe la razón de un código de estado distinto de cero, de lo contrario es nulo

Clase ESET_Features

La clase ESET_Features tiene instancias múltiples, según el número de características del producto. Cada instancia contiene:

- Name: nombre de la característica (la lista de nombres se proporciona a continuación)

- Status: estado de la característica: 0 - inactiva, 1 - deshabilitada, 2 - habilitada

Una lista de cadenas que representan las características de productos reconocidas actualmente:

- CLIENT_FILE_AV: protección antivirus del sistema de archivos en tiempo real

- CLIENT_WEB_AV: protección antivirus del cliente de Internet

- CLIENT_DOC_AV: protección antivirus de los documentos del cliente

- CLIENT_NET_FW : firewall personal del cliente

- CLIENT_EMAIL_AV: protección antivirus de clientes de correo electrónico

- CLIENT_EMAIL_AS: protección antispam de clientes de correo electrónico

- SERVER_FILE_AV: protección antivirus en tiempo real de archivos en el producto de servidor de archivos protegido, por ejemplo, archivos de base de datos de contenido de SharePoint en el caso de ESET Mail Security

- SERVER_EMAIL_AV: protección antivirus de correos electrónicos de productos de servidores protegidos, por ejemplo, correos electrónicos en Microsoft Exchange o IBM Domino

- SERVER_EMAIL_AS: protección antispam de correos electrónicos de productos de servidores protegidos, por ejemplo, correos electrónicos en Microsoft Exchange o IBM Domino

- SERVER_GATEWAY_AV: protección antivirus de los protocolos de red protegidos en la puerta de enlace

- SERVER_GATEWAY_AS: protección antispam de los protocolos de red protegidos en la puerta de enlace

Clase ESET_Statistics

La clase ESET_Statistics tiene instancias múltiples, según el número de exploraciones en el producto. Cada instancia contiene:

- Scanner: código de cadena para la exploración específica, por ejemplo, “CLIENT_FILE”

- Total: número total de archivos explorados

- Infected: número de archivos infectados que se encontraron

- Cleaned: número de archivos desinfectados

- Fecha y hora: la fecha y la hora del último cambio de esta estadística. En un formato de fecha y hora de WMI, por ejemplo, “20130118115511.000000+060”

- ResetTime: fecha y hora en que se reinició por última vez el contador de estadísticas. En un formato de fecha y hora de WMI, por ejemplo, “20130118115511.000000+060”

Lista de cadenas que representan las exploraciones reconocidas actualmente:

- CLIENT_FILE

- CLIENT_EMAIL

- CLIENT_WEB

- SERVER_FILE

- SERVER_EMAIL

- SERVER_WEB

Clase ESET_ThreatLog

La clase ESET_ThreatLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Amenazas detectadas”. Cada instancia contiene:

- ID: identificación única de este historial de registros de exploración

- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)

- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

- Scanner: nombre de la exploración que creó este evento de registro

- ObjectType: tipo de objeto que produjo este evento de registro

- ObjectName: nombre del objeto que produjo este evento de registro

- Threat: nombre de la amenaza encontrada en el objeto descrito por las propiedades de ObjectName y ObjectType

- Action: acción realizada luego de identificar la amenazada

- User: cuenta de usuario que causó la generación de este evento de registro

- Information: descripción adicional del evento

- Hash: hash del objeto que produjo este registro de evento

ESET_EventLog

La clase ESET_EventLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Eventos”. Cada instancia contiene:

- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número en el intervalo de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Module: nombre del módulo que creó este evento de registro
- Event: descripción del evento
- User: cuenta de usuario que causó la generación de este evento de registro

ESET_ODFileScanLogs

La clase ESET_ODFileScanLogs tiene instancias múltiples, cada una de las cuales representa un registro de exploración de archivos a petición. Esto equivale a la lista de registros “Exploración del equipo a petición” de la GUI. Cada instancia contiene:

- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- Targets : carpetas/objetos de destino de la exploración
- TotalScanned: número total de objetos explorados
- Infected: número de objetos infectados encontrados
- Cleaned: número de objetos desinfectados
- Status: estado del proceso de exploración

ESET_ODFileScanLogRecords

La clase ESET_ODFileScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_ODFileScanLogs. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones a petición. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia de clase contiene:

- LogID: identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_ODFileScanLogs)
- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log: el mensaje de registro real

ESET_ODServerScanLogs

La clase ESET_ODServerScanLogs tiene instancias múltiples, cada una de las cuales representa una ejecución de la exploración del servidor a petición. Cada instancia contiene:

- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- Targets : carpetas/objetos de destino de la exploración
- TotalScanned: número total de objetos explorados
- Infected: número de objetos infectados encontrados
- Cleaned: número de objetos desinfectados
- RuleHits: número total de objetos explorados
- Status: estado del proceso de exploración

ESET_ODServerScanLogRecords

La clase ESET_ODServerScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_ODServerScanLogs. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones a petición. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia de clase contiene:

- LogID: identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_ ODServerScanLogs)
- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número en el intervalo de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log: el mensaje de registro real

ESET_SmtpProtectionLog

La clase ESET_SmtpProtectionLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Protección Smtp”. Cada instancia contiene:

- ID: identificación única de este historial de registros de exploración
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

- HELODomain: nombre del dominio HELO
- IP: dirección IP de origen
- Sender: remitente de correo electrónico
- Recipient: destinatario de correo electrónico
- Tipo de protección: tipo de protección utilizada
- Action: acción realizada
- Motivo: motivo de la acción
- TimeToAccept: número de minutos después de los que se aceptará el correo electrónico

ESET_HIPSLog

La clase ESET_HIPSLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “HIPS”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número en el intervalo de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Aplicación: aplicación de origen
- Destino: tipo de operación
- Acción: acción realizada por HIPS, por ejemplo, permitir, rechazar, etc.
- Regla: nombre de la regla responsable por la acción
- Información adicional

ESET_URLLog

La clase ESET_URLLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Sitios Web filtrados”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- URL: la URL

- Status – indica qué pasó con la URL, por ejemplo «Bloqueado por control web»
- Aplicación: aplicación que haya intentado acceder a la URL
- Usuario: cuenta de usuario en la que se estaba ejecutando la aplicación

ESET_DevCtrlLog

La clase ESET_DevCtrlLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Control de dispositivos”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Device: nombre del dispositivo
- User: nombre de la cuenta de usuario
- UserSID: cuenta de usuario SID
- Group: nombre del grupo de usuarios
- GroupSID: grupo de usuarios SID
- Status – indica qué le pasó al dispositivo, por ejemplo «Escritura bloqueada»
- DeviceDetails: información adicional sobre el dispositivo
- EventDetails: información adicional sobre el evento

ESET_MailServerLog

La clase ESET_MailServerLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Servidor de correo”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- IPAddr: dirección IP de origen
- HELODomain: nombre del dominio HELO
- Sender: remitente de correo electrónico

- Recipient: destinatario de correo electrónico
- Subject: asunto de correo electrónico
- ProtectionType: tipo de protección que ha realizado la acción descrita por el registro de registro actual, es decir, malware, antispam o reglas.
- Action: acción realizada
- Reason: la razón por la que se realizó la acción sobre el objeto por el tipo de protección dado.

ESET_HyperVScanLogs

La clase ESET_HyperVScanLogs tiene instancias múltiples, cada una de las cuales representa una ejecución de la exploración del archivo Hyper-V. Esto equivale a la lista de registros “Exploración Hyper-V” de la GUI. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- Targets: máquinas/discos/volúmenes de destino de la exploración
- TotalScanned: número total de objetos explorados
- Infected: número de objetos infectados encontrados
- Cleaned: número de objetos desinfectados
- Status: estado del proceso de exploración

ESET_HyperVScanLogRecords

La clase ESET_HyperVScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_HyperVScanLogRecords. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones de Hyper-V. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia de clase contiene:

- LogID: identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_HyperVScanLogs)
- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log: el mensaje de registro real

ESET_NetworkProtectionLog

La clase ESET_NetworkProtectionLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Protección de red”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Evento: Suceso que desencadena la acción de protección de la red
- Acción: acción que realiza la protección de la red
- Fuente: dirección fuente del dispositivo de red
- Objeto: dirección de destino del dispositivo de red
- Protocolo: protocolo de comunicación de red
- Regla o nombre del gusano: regla o nombre del gusano que se relaciona con el evento
- Aplicación: aplicación que inició la comunicación de red
- User: cuenta de usuario que causó la generación de este evento de registro

ESET_SentFilesLog

La clase ESET_SentFilesLog tiene instancias múltiples, cada una de las cuales representa un historial de registros del registro “Archivos enviados”. Cada instancia contiene:

- ID : identificación única de este historial de registros
- Timestamp: fecha y hora de la creación del historial de registros (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Sha1: Sha-1 hash de archivo enviado
- Archivo: archivo enviado
- Tamaño: tamaño del archivo enviado
- Categoría: catergoría del archivo enviado
- Motivo: motivo para enviar el archivo
- Enviado a: el departamento de ESET al que se envió el archivo
- User: cuenta de usuario que causó la generación de este evento de registro

ESET_OneDriveScanLogs

La clase ESET_OneDriveScanLogs tiene instancias múltiples, cada una de las cuales representa una ejecución de la exploración OneDrive. Esto equivale a la lista de registros “Exploración OneDrive” de la GUI. Cada instancia contiene:

- ID: identificación única de este registro de OneDrive
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- Targets : carpetas/objetos de destino de la exploración
- TotalScanned: número total de objetos explorados
- Infected: número de objetos infectados encontrados
- Cleaned: número de objetos desinfectados
- Status: estado del proceso de exploración

ESET_OneDriveScanLogRecords

La clase ESET_OneDriveScanLogRecords tiene instancias múltiples, cada una de las cuales representa un historial de registro en uno de los registros de exploración representados por las instancias de la clase ESET_OneDriveScanLogs. Las instancias de esta clase proporcionan historiales de registro de todos los registros y exploraciones OneDrive. Cuando solo se requiere una instancia de un historial de registro particular, se debe filtrar mediante la propiedad LogID. Cada instancia contiene:

- LogID: identificación del historial de registros al que pertenece este registro (ID de una de las instancias de la clase ESET_OneDriveScanLogs)
- ID: identificación única de este registro de OneDrive
- Timestamp: fecha y hora de la creación del registro (en el formato de fecha y hora de WMI)
- LogLevel: gravedad del historial de registros expresada como un número de [0-8]. Los valores corresponden a los siguientes niveles nombrados: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log: el mensaje de registro real

Acceso a los datos proporcionados

Aquí hay algunos ejemplos de cómo acceder a los datos WMI de ESET desde la línea de comandos de Windows y PowerShell, que deben funcionar desde cualquier sistema operativo actual de Windows. Sin embargo, hay muchas otras maneras de acceder a los datos desde otros lenguajes y herramientas de scripting.

Línea de comandos sin scripts

La `wmic` herramienta de línea de comandos puede usarse para acceder a cualquier clase de WMI personalizada o a algunas predefinidas.

Para mostrar toda la información sobre el producto en el equipo local:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Para mostrar el número de versión del producto solo del producto en el equipo local:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Para mostrar toda la información sobre el producto en un equipo remoto con IP 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Para mostrar y obtener toda la información sobre el producto en el equipo local:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Para mostrar y obtener toda la información sobre el producto en un equipo remoto con IP 10.1.118.180:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
cred $cred
```

Destinos de las exploraciones de la consola de administración de ESET

Esta funcionalidad permite que ESET PROTECT utilice objetivos de escaneo (Exploración de la base de datos de buzones de correo bajo demanda y Exploración de Hyper-V) cuando ejecuta la tarea del cliente de Exploración del servidor en un servidor con ESET Mail Security. La configuración de los objetivos de exploración de ESET PROTECT solo está disponible si tiene instalado ESET Management Agent, de lo contrario estará atenuado.

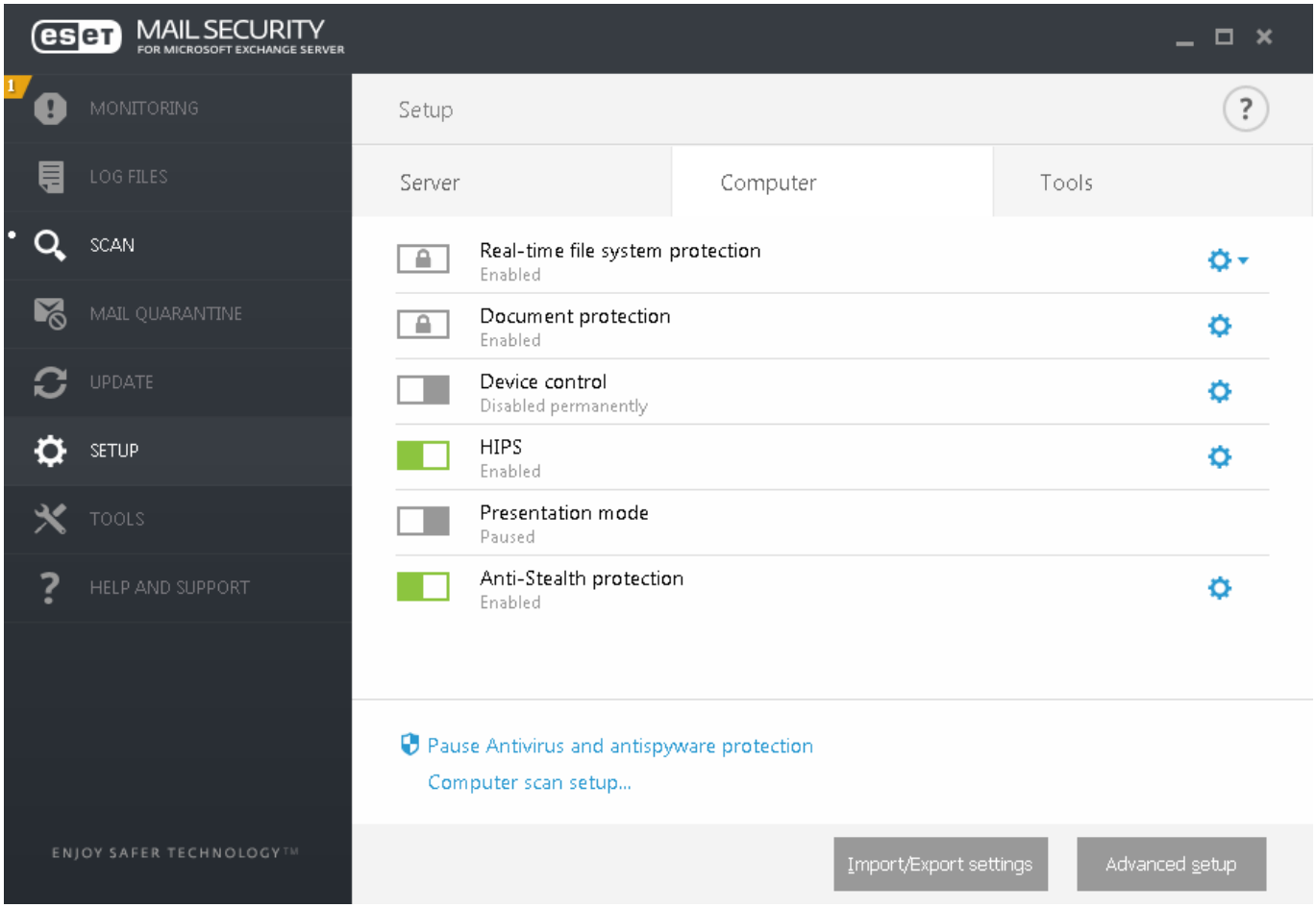
Cuando habilita la opción **Generar lista de objetivos**, ESET Mail Security crea una lista de los objetos disponibles para la exploración. Esta lista se genera periódicamente, según sus **Períodos de actualización**.

> Cuando habilita **Generar listado meta** por primera vez, ESET PROTECT lo adquiere en aproximadamente la mitad del **Período de actualización** especificado. Por lo que si el **Período de actualización** está establecido en 60 minutos, le llevará a ESET PROTECT unos 30 minutos para recibir el listado de objetivos escaneados. Si necesita que ESET PROTECT recolecte la lista antes, establezca el período de actualización en un valor menor. Siempre puede volver a aumentarlo.

Cuando ESET PROTECT ejecuta una tarea de cliente de **Exploración de servidor** recogerá la lista y se le pedirá que seleccione los objetivos de Exploración de Hyper-V en ese servidor particular.

Modo de anulación

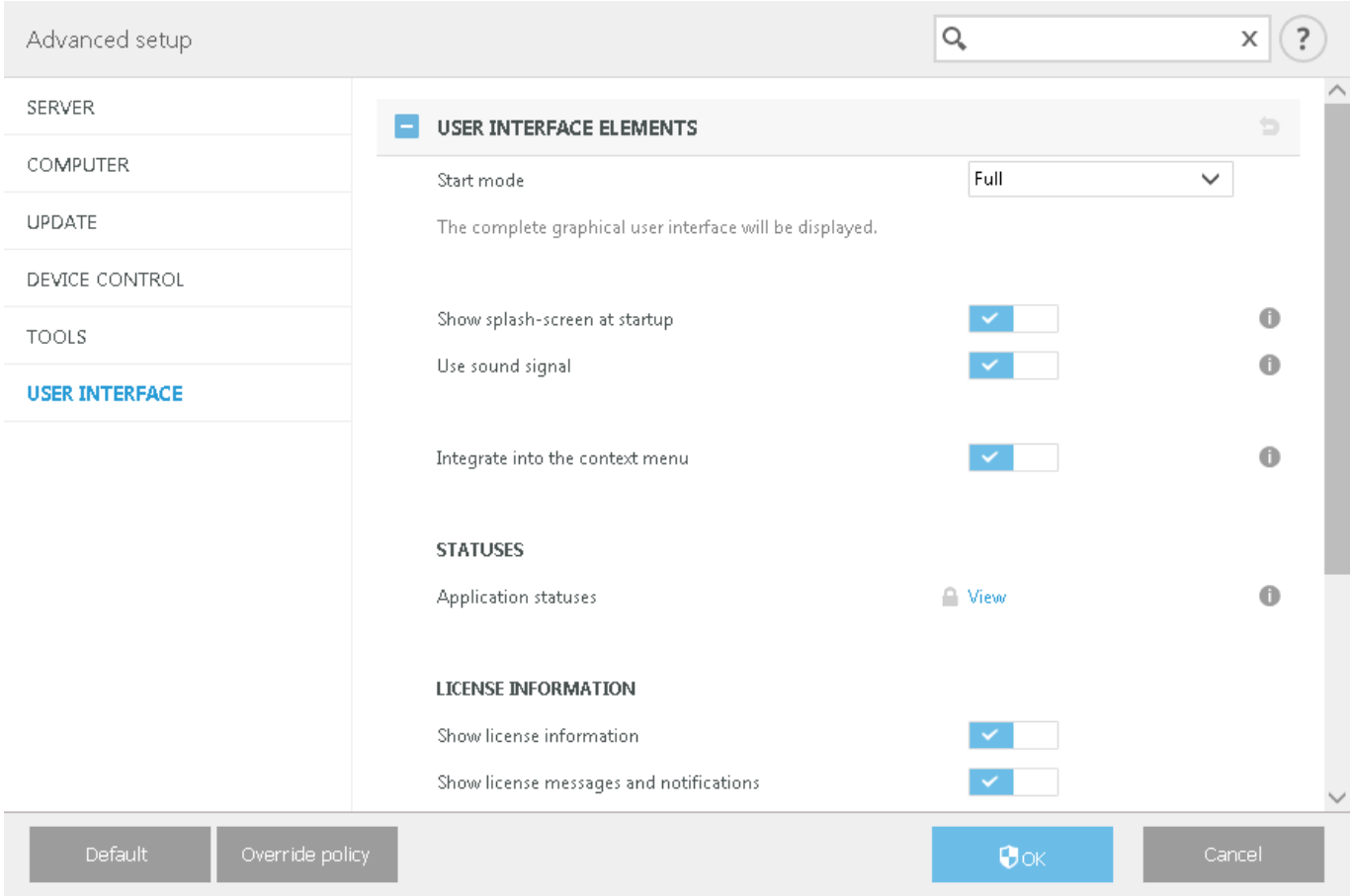
Si tiene una política ESET PROTECT aplicada a ESET Mail Security, verá un ícono de bloqueado en lugar del interruptor Habilitar/Deshabilitar en la Página de configuración y un ícono de bloqueo junto al interruptor en la ventana de **Configuración avanzada**.



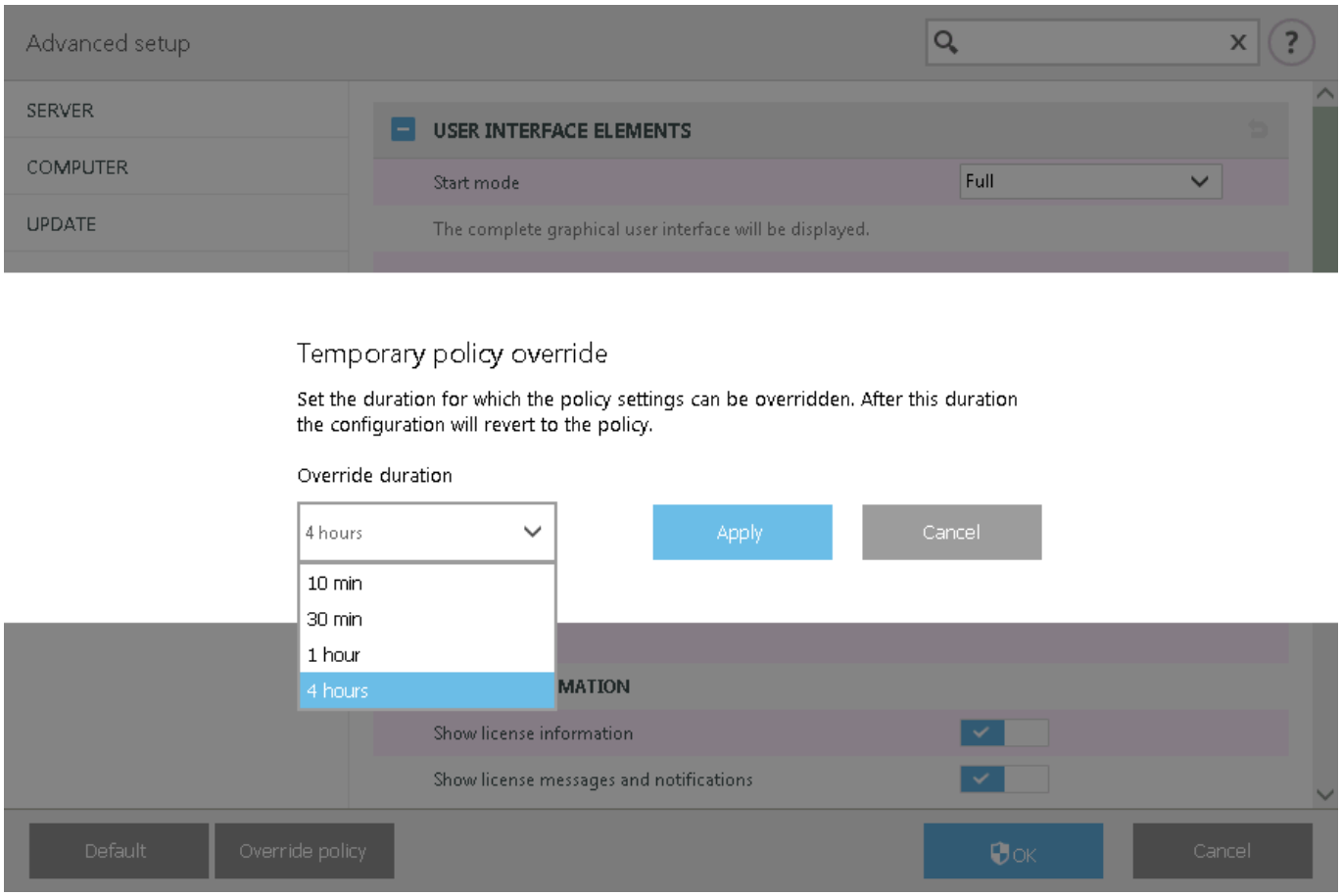
Normalmente, los ajustes configurador a través de una política ESET PROTECT no se pueden modificar. El modo de anulación le permite desbloquear temporalmente estos ajustes. Sin embargo, necesita habilitar el **Modo de anulación** con una política ESET PROTECT.

Inicie sesión en ESET PROTECT Web Console , vaya a **Políticas**, seleccione y edite la política existente que se aplica a ESET Mail Security, o bien, cree una nueva. En **Configuración**, haga clic en **Modo de anulación**, habilítelo y configure el resto de los ajustes, incluido el tipo de Autenticación (usuario de Active Directory o Contraseña).

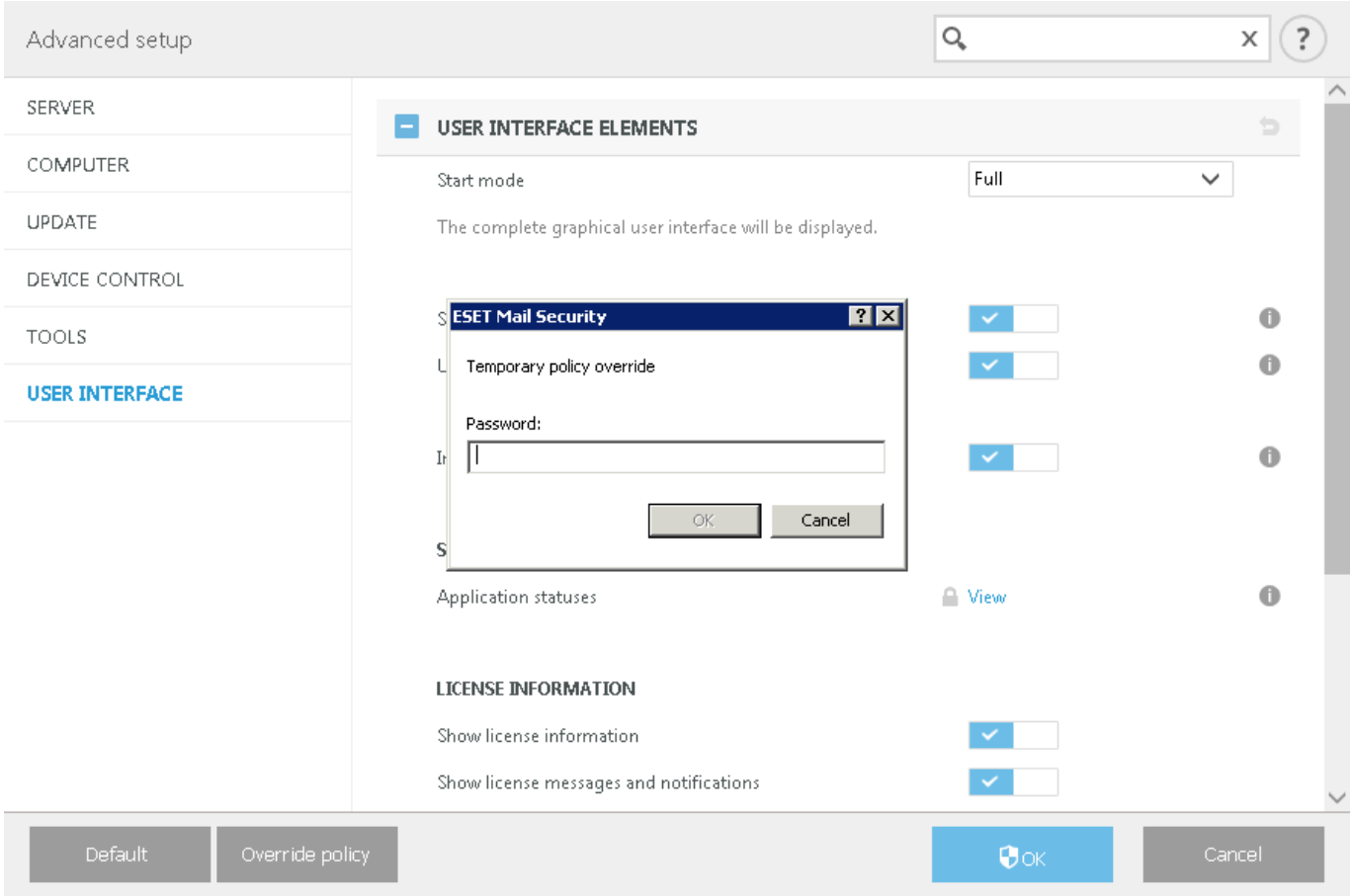
Una vez modificada la política, o aplicada la nueva política a ESET Mail Security, aparecerá el botón Anular política en la ventana **Configuración avanzada**.



Haga clic en el botón **Anular política**, establezca la duración y haga clic en **Aplicar**.



Si como tipo de autentificación seleccionó **Contraseña**, ingrese la contraseña de anulación de política.



Después de que venza el modo de anulación, todo cambio a la configuración que haya realizado volverá a su ajuste de política ESET PROTECT original. Recibirá una notificación antes del vencimiento de la anulación.

Puede **Finalizar el modo de anulación** en cualquier momento antes de su vencimiento en la Página de monitoreo o en la ventana de Configuración avanzada.

Archivos de registro

Esta sección le permite modificar la configuración del inicio de sesión de ESET Mail Security.

Historiales de registros

Los registros quedan asentados en el registro de Eventos (*C:\ProgramData\ESET\ESET Security\Logs*) y se pueden visualizar en el visor de Archivos de registro. Use los interruptores para activar o desactivar una función en particular.

Registrar errores de transporte de correo
Si esta opción está habilitada y hay problemas en la capa de transporte de correo, los mensajes de error se guardan en el registro de Eventos.

Registrar excepciones de transporte de correo
Si hay alguna excepción en el transporte de correo, los detalles correspondientes se guardan en el registro de Eventos.

Filtro de registros

Produce una cantidad significativa de datos porque todas las opciones de registro están habilitadas de forma predeterminada. Le recomendamos que desactive selectivamente el registro de los componentes que no sean útiles o no estén relacionados con el problema.

> Para iniciar el registro real que necesita para activar el **Registro de diagnósticos** general a nivel del producto en el menú principal, vaya a **Configuración** > Herramientas. Una vez que el mismo registro está activado, ESET Mail Security recopilará los registros detallados según las características que están habilitadas en esta sección.

Use los interruptores para activar o desactivar una función en particular. Estas opciones también se combinan según la disponibilidad de los componentes individuales en el ESET Mail Security.

• Registro de diagnósticos del transporte del correo

> Al resolver problemas con la exploración de la base de datos que se ejecuta en una operación normal, le recomendamos que deshabilite el **registro de diagnóstico de transporte de correo**. De lo contrario, esto podría obstruir el registro resultante y dificultar el análisis.

- **Registro de diagnósticos de la exploración de bases de datos a petición**: escribe información detallada en registros, en especial cuando es necesario solucionar problemas.
- **Registro de diagnóstico de clúster**: el registro de clúster se incluirá en el registro de diagnóstico general.
- **Registro de diagnóstico de OneDrive**: el registro de OneDrive se incluirá en el registro de diagnóstico general.
- **Registro de diagnóstico del motor antispam**: cuando necesite solucionar problemas, verá información detallada sobre el motor antispam en los registros. Escribe información detallada sobre el motor antispam en el archivo de registro para fines de diagnóstico. El motor Antispam no usa el Registro de eventos (warnlog.dat) y, por lo tanto, no se puede visualizar en el visor de Archivos de registro. Escribe registros directamente en un archivo de texto dedicado (por ejemplo C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log) para que todos los datos de diagnóstico del motor Antispam se mantengan en un solo lugar. De esta manera, no se pone en peligro el desempeño de ESET Mail Security en caso de un enorme tráfico de correo electrónico.

Archivos de registro

Define cómo se administrarán los registros. Esto es importante, principalmente, para evitar que se utilice el disco. Las configuraciones predeterminadas permiten la eliminación automática de registros antiguos para ahorrar espacio en el disco.

Eliminar registros automáticamente

Se eliminarán las entradas de registro anteriores a la cantidad de días especificados (a continuación).

Eliminar los registros más antiguas que (días)

Especificar la cantidad de días.

Elimine automáticamente los historiales antiguos, si se excede el tamaño de los registros

Cuando el tamaño de los registros excede el **Tamaño máx. de registros [MB]**, se eliminarán los historiales antiguos hasta que se alcance un **Tamaño de registros reducido [MB]**.

Realizar copias de seguridad de los historiales eliminados automáticamente

Se realizarán copias de seguridad de los archivos e historiales de registros eliminados automáticamente en un directorio especificado y con la opción de comprimirlo en archivos ZIP.

Realizar copias de seguridad de los registros de diagnóstico

Realizará copias de seguridad de registros de diagnóstico eliminados automáticamente. Si no están habilitados, no se harán copias de seguridad de los historiales de registros de diagnóstico.

Carpeta de copias de seguridad

Carpeta donde se almacenarán las copias de seguridad de los registros. Puede habilitar las copias de seguridad de los registros comprimidos con el uso de ZIP.

Optimizar archivos de registro automáticamente

Cuando estén activados, los archivos de registro se desfragmentarán si el porcentaje de fragmentación es mayor que el valor especificado en el campo **Si el número de registros no utilizados excede (%)**. Haga clic en **Optimizar** para comenzar la desfragmentación de los archivos de registro. Todas las entradas de registro vacías se eliminan para mejorar el rendimiento y la velocidad de procesamiento del registro. Esta mejora se observa más claramente cuanto mayor es el número de entradas de los registros.

Habilitar protocolo del texto

Para habilitar el almacenamiento de los registros en otro formato de archivo separado de los Archivos de registro:

- **Directorio de destino**: el directorio donde se almacenarán los archivos de registro (solo se aplica a **texto**/**CSV**). Cada sección de registro tiene su propio archivo con un nombre de archivo predefinido (por ejemplo, *virlog.txt* para la sección de archivos de registro Amenazas detectadas, si usa un formato de archivo de texto sin formato para almacenar los registros).
- **Tipo**: si selecciona el formato de archivo **Texto**, los registros se almacenarán en un archivo de texto; los datos se separarán mediante tabulaciones. Lo mismo se aplica para el formato del archivo **CSV** separado por comas. Si elige **Suceso**, los registros se almacenarán en el registro Windows Event (se puede ver mediante el Visor de sucesos en el Panel de control) en lugar del archivo.
- **Eliminar todos los archivos de registro:** borra todos los registros almacenados seleccionados en el menú desplegable **Tipo**.

> Para ayudar a resolver los problemas más rápidamente, Soporte técnico de ESET le puede solicitar que proporcione los registros de su equipo. El ESET Log Collector le facilita la recopilación de la información necesaria. Para obtener más información acerca del ESET Log Collector, vea nuestro artículo de la Base de conocimientos .

Registro de auditoría

Realiza un seguimiento de los cambios de configuración o protección. Debido a que las modificaciones que tienen lugar en la configuración del producto pueden afectar de manera significativa la forma de operar del producto, tal vez quiera llevar un registro de los cambios para los fines de las auditorías. Verá los registros de los cambios en la sección **Archivos de registro** > Registro de auditorías.

Exportar registro

Exportar a los registros de aplicaciones y servicios de Windows
Le permite duplicar archivos desde el Registro de protección del servidor del correo electrónico hasta registros de aplicaciones y servicios. Para ver el registro de protección del servidor de correo electrónico, abra Windows **Visor de eventos** y diríjase a **Registros de aplicaciones y servicios** > **ESET** > **Seguridad** > **ExchangeServer Protección de correo**. Los registros de aplicaciones y servicios son compatibles con Microsoft Windows Server 2012 o versiones más recientes.
Exportar a servidor syslog
Puede tener registros de protección del servidor de correo electrónico duplicados en el servidor syslog en el Formato de evento común (CEF). El CEF es un formato estandarizado, extensible y basado en el texto que se puede utilizar para facilitar la recopilación de datos y la combinación de ellos para que un sistema de gestión empresarial realice un análisis posterior. En este caso, puede usarlo junto con Información de seguridad y gestión de eventos (SIEM) y soluciones de gestión de registro, como Micro Focus ArcSight. Consulte Control de eventos en Syslog para obtener información detallada sobre las descripciones y los campos de eventos exportados.
Dirección del servidor
Ingrese la dirección IP o el nombre de host del servidor. En el caso de ArcSight, especifique el servidor con SmartConnector instalado.
Protocolo
Seleccione el protocolo que se utilizará, ya sea el protocolo TCP o UDP.
Puerto
El valor predeterminado es 514 para ambos protocolos.
Exportar a archivo
Permite que los registros se exporten a nivel local a un archivo en formato CEF. La capacidad de almacenamiento de registros es limitada. Por lo tanto, se utiliza un sistema de registro circular. Los registros se escriben en forma secuencial en los archivos (de `mailserver.0.log` a `mailserver.9.log`). Los últimos registros se almacenan en `mailserver.0.log`. Una vez que se llega al límite de tamaño, se quitan los archivos más antiguos `mailserver.9.log` y se le asigna un nuevo nombre a los archivos de registro en secuencia (`mailserver.0.log` cambia el nombre a `mailserver.1.log` y así sucesivamente).
Ruta al archivo
La ruta predeterminada es C:\ProgramData\ESET\ESET Security\Logs. Puede modificar la ubicación, si lo desea.

Asignación de eventos en Syslog

Las siguientes tablas muestran el mapeo de eventos de ESET Mail Security a campos de datos de ArcSight. Puede utilizar estas tablas como referencia de lo que se envía a ArcSight a través de SmartConnector.

Header		
Device Vendor	"ESET"	
Device Product	"EMSX"	"EMSX" or "ESET Mail Security for MS Exchange Server"
Device Version	e.g. "7.1.10005.0"	
Device Event Class ID	e.g. "101"	Device Event Category unique identifier: 100-199 malware 200-299 phish 300-399 spam 400-499 policy
Event Name	e.g. "MailScanResult: malware"	A brief description of what happened in the event: MailScanResult: malware MailScanResult: phishing link MailScanResult: spam MailScanResult: policy

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
rt	deviceReceiptTime	Time event was generated	The time at which the event was generated, in milliseconds since Jan 1st 1970
src	sourceAddress	Sender's IP	IP address of the sending mail server
shost	sourceHostName (1023)	Sender's HELO domain	HELO domain of the sending mail server
flexString1	flexString1	Message-ID	Message-ID header from the email
dhost	destinationHostName (1023)	Receiving server	Hostname of the machine that received the communication
msg	message (1023)	Message subject	Subject of the message, from the RFC5233 header "Subject:"
suser	sourceUserName (1023)	SMTP sender	SMTP sender of the email (MAIL FROM)
duser	destinationUserName (1023)	SMTP recipient(s)	SMTP recipient(s) of the email (RCPT TO)
act	deviceAction (63)	Action taken	Action taken (cleaned, quarantined, etc.)
cat	deviceEventCategory (1023)	Detection category	Most significant detection (malware >> phish >> spam >> SPF/DKIM >> policy)
sourceServiceName	sourceServiceName	Type of protection	SMTP Transport agent, On-demand database scan
deviceExternalId	deviceExternalId	Engine version	Anti-Malware engine version, Antispam engine version, e.g. "18620,7730"
cs1	deviceCustomString1	Anti-Malware result	Result of Anti-Malware scan, including threat name
cs1Label	deviceCustomString1Label	"Anti-Malware result"	
cs2	deviceCustomString2	Antispam result	Result of Antispam scan, including reason for marking as spam
cs2Label	deviceCustomString2Label	"Antispam result"	
cs3	deviceCustomString3	Anti-Phishing result	Result of Anti-Phishing scan, including detected URL
cs3Label	deviceCustomString3Label	"Anti-Phishing result"	
cs4	deviceCustomString4	SPF/DKIM/DMARC result	Result of SPF/DKIM/DMARC check, in RFC7601 format
cs4Label	deviceCustomString4Label	"SPF/DKIM/DMARC result"	
cs5	deviceCustomString5	"From:" sender	Sender address from RFC5322 header "From:"
cs5Label	deviceCustomString5Label	"From header"	
cs6	deviceCustomString6	"To:" and "Cc:" recipients	Recipients addresses from RFC5322 headers "To:" and "Cc:"
cs6Label	deviceCustomString6Label	"To and Cc headers"	
fname	filename (1023)	Attachment name	Name of the first detected attachment

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
fileHash	fileHash (255)	Attachment hash	Hash of the first detected attachment
fsize	fileSize	Attachment size	Size of the first detected attachment
reason	reason (1023)	Rule/policy activated	Name of the policy triggered by the email or it's content
ESETEMSXFileDetails	ESETEMSXFileDetails	File details	Information about all detected attachments, their names, hashes and sizes

Optional

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
end	endTime	Time event has ended	The time at which the activity ended, in milliseconds since Jan 1st 1970. Useful only if sand boxing technology is used ESET LiveGuard Advanced.
dtz	deviceTimeZone (255)	Timezone of the server	
request	requestURL	Detected URL	Malign or blacklisted URL extracted from mail body or mail headers. ESET Mail Security does not provide single URL in logs due to the fact that multiple URL's can be detected in email messages by various detection components.

Servidor proxy

En redes de área local muy extensas, la conexión del equipo a Internet puede tener como intermediario un servidor proxy. En tal caso, será necesario definir las siguientes opciones de configuración. Si no lo hace, el programa no podrá actualizarse en forma automática. En ESET Mail Security, la configuración del servidor proxy está disponible en dos secciones diferentes de la ventana de **Configuración avanzada** (**F5**):

1. **Configuración avanzada** (F5) > **Actualización** > **Perfiles** > **Actualizaciones** > **Opciones de conexión** > Proxy HTTP. Esta configuración se aplica al perfil de actualización dado y se recomienda para portátiles que reciben frecuentemente módulos desde diferentes ubicaciones.

2. **Configuración avanzada** (F5) > **Herramientas** > **Servidor proxy**. Al especificar el servidor proxy en este nivel define la configuración global del servidor proxy para todos los ESET Mail Security. Todos los módulos que requieran una conexión a Internet usarán los parámetros ingresados aquí.

Para especificar la configuración del servidor proxy en esta etapa, encienda el interruptor **Usar servidor proxy** y luego ingrese la dirección del servidor proxy en el campo **Servidor proxy**, junto con el número de **Puerto** del servidor proxy.

El servidor proxy requiere autenticación

En caso de que la comunicación de red a través del servidor proxy requiera autenticación, habilite esta opción y escriba su **Nombre de usuario** y **Contraseña**.

Detectar el servidor proxy

Haga clic en **Detectar** para detectar y llenar la configuración del servidor proxy en forma automática. Se copiarán los parámetros especificados en Internet Explorer.

> Esta característica no recupera los datos de autenticación (nombre de usuario y contraseña); usted debe ingresarlos.

Utilice una conexión directa si el proxy no está disponible

Si un producto está configurado para usar HTTP Proxy y no puede llegar al proxy, el producto evadirá el proxy y se comunicará directamente con los servidores ESET.

Modo de presentación

El modo de presentación es una característica para los usuarios que necesitan usar el software en forma ininterrumpida, que no desean que las ventanas emergentes los molesten y que quieren minimizar el uso de la CPU. El modo de presentación también se puede usar durante las presentaciones que la actividad de ESET Mail Security no puede interrumpir. Cuando está habilitado, todas las ventanas de notificación se deshabilitan y las tareas programadas no se ejecutan. La protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

Habilitar el modo de presentación automáticamente al ejecutar aplicaciones en modo de pantalla completa

El modo de presentación se activa automáticamente siempre que se ejecuta una aplicación de pantalla completa. Con el modo Presentación activado, no podrá ver las notificaciones o un cambio de estado de su ESET Mail Security.

Deshabilitar el modo de presentación automáticamente después de

Para definir la cantidad de tiempo en minutos después de la que el modo de presentación se deshabilitará automáticamente.

Diagnósticos

Los diagnósticos proporcionan el volcado de memoria de los procesos de ESET (por ejemplo, *ekrn*). Si una aplicación se bloquea, se generará un volcado. Esto puede ayudar a los desarrolladores a depurar y reparar distintos ESET Mail Security problemas.

Haga clic en el menú desplegable junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- **Deshabilitar**: para deshabilitar esta característica.
- **Mini**: (predeterminado) registra el grupo de datos útiles más reducido posible que pueda ayudar a identificar por qué se bloqueó la aplicación en forma inesperada. Este tipo de archivo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, debido a la cantidad limitada de información incluida, es posible que los errores que no se provocaron directamente por el subproceso activo en el momento del problema no se descubran al analizar este archivo.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene inesperadamente. Un volcado completo de memoria puede incluir datos de los procesos que estaban activos cuando se recopiló la memoria de volcado.

Directorio de destino

Directorio donde se va a generar la memoria de volcado durante el bloqueo.

Abrir carpeta de diagnósticos

Haga clic en **Abrir** para abrir este directorio dentro de una nueva ventana de *Windows Explorer*.

Crear volcado de diagnóstico

Haga clic en **Crear** para crear archivos de volcado de diagnóstico en el directorio de Destino.

Registro avanzado

Permitir el registro avanzado de exploración del equipo – Graba todos los eventos que se produzcan durante la exploración de archivos y carpetas mediante la exploración del equipo o la Protección del sistema de archivos en tiempo real.
Habilitar el registro avanzado del control del dispositivo – Grabar todos los eventos que ocurren en el control del dispositivo para permitir el diagnóstico y solucionar problemas.
Habilitar el registro avanzado de Direct Cloud – Registrar toda la comunicación del producto entre el producto y los servidores de Direct Cloud.
Habilitar el registro avanzado de protección de documentos – Graba todos los eventos que ocurren en la protección de documentos para diagnosticar y solucionar problemas.
Habilitar el registro avanzado de núcleo – Grabar todos los eventos que ocurren en el servicio de kernel de ESET (ekrn) para permitir la realización de diagnósticos y la resolución de problemas.
Habilitar el registro avanzado de licencias - Registre las comunicaciones del producto con el servidor de la licencia.
Habilitar seguimiento de memoria – Registre todos los eventos que ayudarán a los desarrolladores a diagnosticar pérdidas de memoria.
Habilitar el registro avanzado de protección de red – Registra todos los datos de red que pasan a través de la protección de red en formato PCAP, con el fin de que los desarrolladores diagnostiquen y corrijan los problemas relacionados con la protección de red.
Habilitar el registro de sistemas operativos – Se recopilará información adicional acerca del Sistema operativo como los procesos en ejecución, actividad del CPU y operaciones de disco. Esto puede ayudar a los desarrolladores para diagnosticar y solucionar problemas relacionados con el producto ESET ejecutado en su sistema operativo.
Habilitar el registro avanzado del filtro del Protocolo – Graba todos los datos que pasen por el motor de filtrado de protocolos en formato PCAP para ayudar a los desarrolladores a diagnosticar y corregir los problemas relacionados con el filtrado de protocolos.
Permitir el registro avanzado de envío de mensajes push – Graba todos los eventos que ocurren durante el envío de mensajes push para diagnosticar y solucionar problemas.
Habilitar el registro avanzado de la protección del sistema de archivos en tiempo real - Registre todos los eventos que ocurren en la protección del sistema de archivos en tiempo real para diagnosticar y solucionar problemas.
Habilitar el registro avanzado del motor de actualizaciones – Registra todos los eventos que ocurren durante el proceso de actualización, para ayudar a los desarrolladores a diagnosticar y solucionar los problemas relacionados con el motor de actualizaciones.

Ubicación de los archivos de registro

C:\ProgramData\ESET\ESET Security\Diagnostics

Soporte técnico

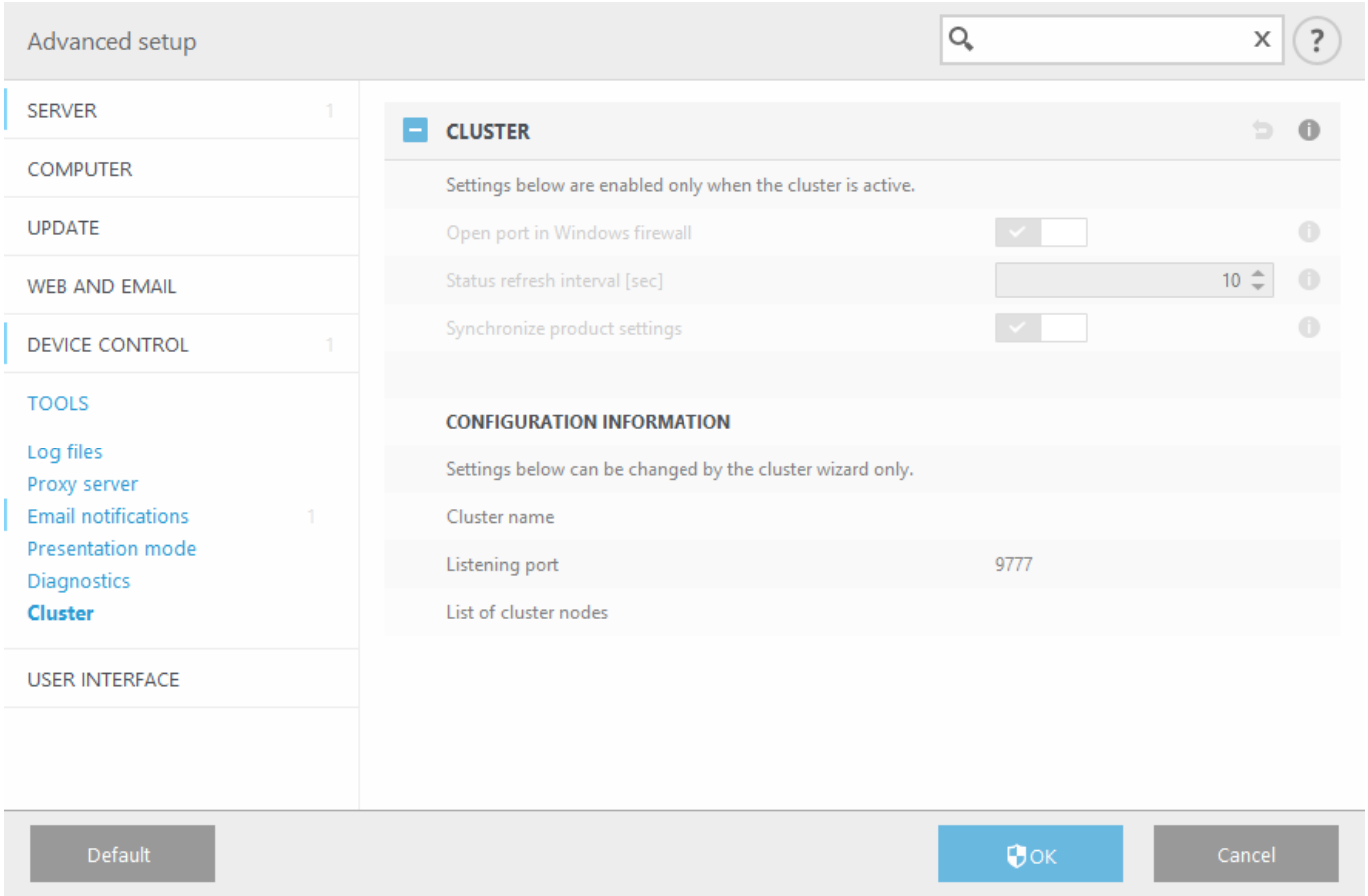
Enviar datos de configuración del sistema

Seleccione **Enviar siempre** para que no se le solicite enviar sus datos de configuración de ESET Mail Security a Atención al cliente, o use **Preguntar antes de enviar**.

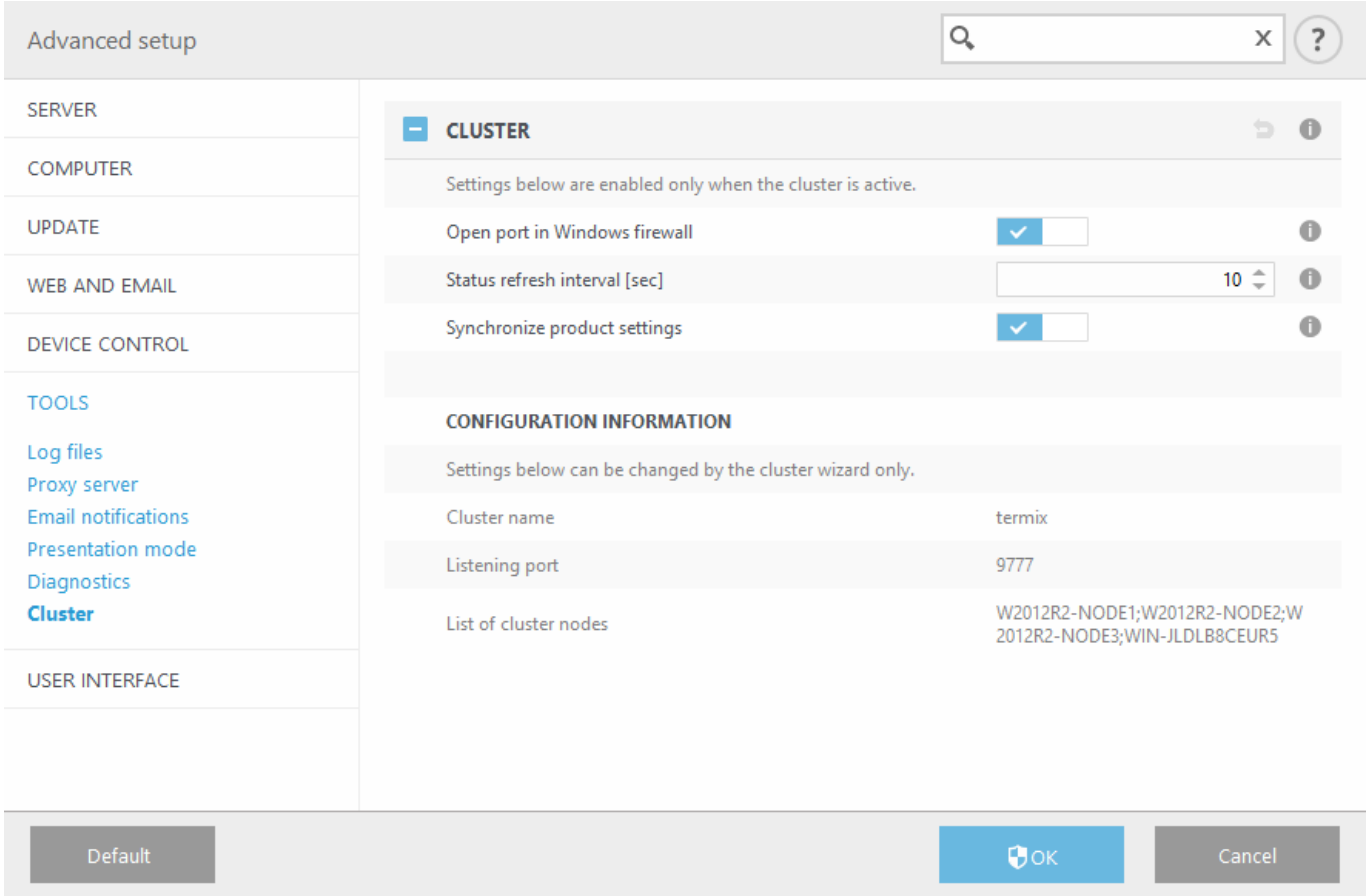
Clúster

La opción Habilitar clúster se habilita de forma automática al configurar el clúster de ESET. Es posible deshabilitarlo de forma manual en la ventana de **Configuración avanzada** (F5) con un clic en el ícono del interruptor (por ejemplo, cuando necesita cambiar la configuración sin afectar a otros nodos dentro del clúster de ESET). Este interruptor solo habilita o deshabilita la funcionalidad del clúster de ESET. Para configurar o eliminar el clúster, es necesario usar el Asistente de clúster o **Destruir clúster**, opción que se encuentra en la sección Herramientas > Clúster en la ventana principal del programa.

Clúster de ESET no configurado y deshabilitado:



Clúster de ESET configurado adecuadamente con sus detalles y opciones:



Interfaz de usuario

Configure la conducta de la interfaz del usuario (GUI) de ESET Mail Security. Es posible ajustar el aspecto visual del programa y los efectos.

Use el menú desplegable Modo de inicio de GUI para seleccionar alguno de los siguientes modos de inicio de Interfaz de usuario gráfica (GUI):

- **Completo**: Se mostrará la interfaz de usuario completa.
- **Terminal**: no se mostrará notificación o alerta alguna. La interfaz gráfica del usuario solo puede iniciarla el Administrador. La interfaz del usuario debe estar configurada en Terminal si los elementos gráficos ralentizan el rendimiento de su equipo o causan otros problemas. También es posible que desee deshabilitar la interfaz gráfica del usuario en un servidor Terminal. Para obtener más información acerca de ESET Mail Security instalado en un servidor Terminal, consulte el tema Desactivar interfaz gráfica del usuario en servidor Terminal.

Modo de color

Seleccione el esquema de colores de la interfaz gráfica de usuario (GUI) ESET Mail Security en el menú desplegable:

- **Igual que el color del sistema**: el esquema de colores ESET Mail Security se basa en la configuración del sistema operativo.
- **Oscuro**: ESET Mail Security usará un esquema de colores oscuros (modo oscuro).

- **Claro**: ESET Mail Security usará un esquema de color claro (estándar).

Mostrar la pantalla de bienvenida al iniciar el programa – Deshabilite esta opción si no desea que se muestre la pantalla de bienvenida al iniciar la ventana principal del programa de su ESET Mail Security, por ejemplo, al iniciar sesión en el sistema.

Usar señal sonora – ESET Mail Security reproduce un sonido cuando ocurren sucesos importantes durante una exploración; por ejemplo, cuando se descubre una amenaza o cuando finaliza la exploración.

Integrar al menú contextual - Al habilitarlos, los elementos de control de ESET Mail Security se integran al menú contextual. Éste aparece cuando se hace un clic con el botón secundario en un objeto (archivo). El menú muestra una lista de todas las acciones que puede realizar en un objeto.

Información de licencias

Cuando se activa esta opción, se mostrarán mensajes y notificaciones sobre su licencia.

Mostrar información de licencias – Cuando esta opción esté deshabilitada, no se mostrará la fecha de vencimiento de la licencia en el **estado de protección** ni en la pantalla **Ayuda y soporte técnico**.

Configurar los estados de las aplicaciones relacionadas con la licencia - Abre la lista de estados de la aplicación relacionados con la licencia.

Configurar las notificaciones de licencia – Cuando esta opción está deshabilitada, las notificaciones y los mensajes solo se mostrarán cuando la licencia esté vencida.

Configuración de acceso: puede evitar los cambios no autorizados con la herramienta **Configuración de acceso** para asegurar que la seguridad se mantenga alta.

Shell de ESET: puede configurar los derechos de acceso para la configuración del producto, las características y los datos a través de eShell al cambiar la Política de ejecución de Shell de ESET.

Ícono en el área de notificación de Windows

Revertir toda la configuración en esta sección

Configuración del acceso

Para la máxima seguridad de su sistema, es fundamental que ESET Mail Security esté correctamente configurado. Cualquier modificación no autorizada puede provocar problemas o incluso la pérdida de datos importantes. Para evitar modificaciones no autorizadas, puede proteger su contraseña de configuración de ESET Mail Security.

> Si está desinstalando ESET Mail Security al mismo tiempo que utiliza la protección de contraseña de configuración de acceso, se le pedirá que introduzca la contraseña. De lo contrario, no podrá desinstalar ESET Mail Security.

Configuración de la protección por contraseña

Bloquea o desbloquea los parámetros de configuración del programa. Haga clic para abrir la ventana de **Configuración de la contraseña**.

Establecer contraseña

Para establecer o cambiar una contraseña para proteger los parámetros de configuración, haga clic en **Configuración**. Para proteger los parámetros de configuración de ESET Mail Security con el fin de evitar la modificación no autorizada, es necesario configurar una nueva contraseña. Cuando quiera cambiar la contraseña existente, escriba su contraseña anterior en el campo **Contraseña anterior**, ingrese su nueva contraseña en los campos **Contraseña nueva** y **Confirmar contraseña** y luego, haga clic en **Aceptar**. Esta contraseña será necesaria para futuras modificaciones de ESET Mail Security.

Exigir derechos completos de administrador para cuentas de administrador limitadas

Seleccione esta opción para solicitarle al usuario actual (quién no dispone de derechos de administrador) que introduzca las credenciales de cuenta del administrador al modificar determinados parámetros del sistema, como deshabilitar los módulos de protección.

> Si cambia la contraseña de la Configuración del acceso y desea importar un archivo de configuración .xml existente (que se firmó antes del cambio de contraseña) utilizando la línea de comandos de ESET CMD, asegúrese de volver a firmarlo con su contraseña actual. Esto le permite usar un archivo de configuración anterior sin la necesidad de exportarlo a otra máquina que ejecute ESET Mail Security antes de la importación.

Shell de ESET

Puede configurar los derechos de acceso para la configuración del producto, las características y los datos a través de eShell al cambiar la **Política de ejecución del Shell de ESET**. La configuración predeterminada es **Cifrado limitado**, pero puede cambiarla a Deshabilitado, Solo lectura o Acceso completo de ser necesario.

Deshabilitado

eShell no puede usarse en lo absoluto. Solo se permite la configuración de eShell en el contexto ui eshell. Puede personalizar la apariencia de eShell, pero no puede acceder a las configuraciones ni a los datos de ningún producto.

Solo lectura

eShell se puede utilizar como una herramienta de monitoreo. Puede visualizar todas las configuraciones tanto en el modo interactivo como en el de procesamiento por lotes, pero no puede modificar las configuraciones, las funciones ni los datos.

Cifrado limitado

En modo interactivo, puede visualizar y modificar todas las configuraciones, las funciones y los datos. En el modo de Lote, eShell funcionará como si estuviera en modo de solo lectura, no obstante, si usa archivos de lotes firmados, podrá editar las configuraciones y modificar los datos.

Acceso completo

El acceso a todas las configuraciones es ilimitado tanto en modo interactivo como de procesamiento por lotes (al ejecutar archivos por lotes). Puede visualizar y modificar cualquier configuración. Debe usar una cuenta de administrador para ejecutar eShell con acceso completo. Si UAC está habilitado, también se requiere elevación.

Deshabilitación de la interfaz gráfica del usuario en Terminal Server

Este capítulo describe cómo deshabilitar la interfaz gráfica del usuario de ESET Mail Security cuando se ejecuta en Windows Terminal Server para sesiones de usuario.

Normalmente, la interfaz gráfica del usuario de ESET Mail Security se inicia cada vez que un usuario remoto se registra en el servidor y crea una sesión de terminal. Por lo general, esto no es deseable en servidores Terminal Server. Si desea deshabilitar la interfaz gráfica del usuario para sesiones terminales, puede hacerlo mediante eShell al ejecutar el comando `set ui ui gui-start-mode none`. Esto pondrá la interfaz gráfica del usuario en modo terminal. Estos son los dos modos disponibles para el inicio de la interfaz gráfica del usuario:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Si desea averiguar qué modo se usa actualmente, ejecute el comando `get ui ui gui-start-mode`.

> Si tiene instalado ESET Mail Security en un servidor con Citrix, le recomendamos usar las configuraciones descritas en nuestro artículo de la base de conocimiento .

Ícono en el área de notificación de Windows

Las opciones y funciones de configuración más importantes están disponibles al hacer clic con el botón secundario en el ícono de la bandeja del sistema (área de notificación de Windows).

> Para acceder al menú del ícono de la bandeja del sistema (área de notificación de Windows), asegúrese de que el modo de inicio de los elementos de la interfaz del usuario esté configurado como Completo.

Más información

Abre la página de Supervisión para mostrarle el actual estado de protección y mensajes.

Detener protección

Muestra el cuadro de diálogo de confirmación que deshabilita la Protección antivirus y antispyware, que protege ante ataques mediante el control de los archivos, las comunicaciones por medio de Internet y correo electrónico. En el menú desplegable **Intervalo de tiempo** puede especificar durante cuánto tiempo se deshabilitará la protección.

Configuración avanzada

Abre la Configuración avanzada de ESET Mail Security.

Archivos de registro

Contienen información sobre todos los eventos importantes del programa que se llevaron a cabo y proporcionan una descripción general de las amenazas detectadas.

Restablecer disposición de la ventana

Restablece la ventana de ESET Mail Security a su tamaño y posición predeterminados en la pantalla.

Modo de color

Abre la configuración de la interfaz del usuario, donde puede cambiar el color de la interfaz gráfica del usuario.

Buscar actualizaciones

Comienza a actualizar los módulos para garantizar su nivel de protección frente a un código malicioso.

Acerca de

Proporciona información del sistema, detalles sobre la versión instalada de ESET Mail Security y los módulos del programa instalados, como así también la fecha de vencimiento de su licencia. La información acerca de su sistema operativo y recursos del sistema se puede encontrar en la parte inferior de la página.

Notificaciones

Las notificaciones en el escritorio y los globos de sugerencias son solo informativos y no necesitan la interacción con el usuario. Se muestran en el área de notificaciones en la esquina inferior derecha de la pantalla. A continuación, se pueden modificar las opciones más detalladas, como el tiempo de visualización de las notificaciones y la transparencia de la ventana.

Administre las notificaciones de ESET Mail Security y abra **Configuración avanzada** (**F5**) > **Notificaciones**. Puede configurar los siguientes tipos:

Estados de la aplicación: haga clic en **Editar** para seleccionar los estados de la aplicación que se mostrarán en la sección de inicio de la ventana principal del programa.

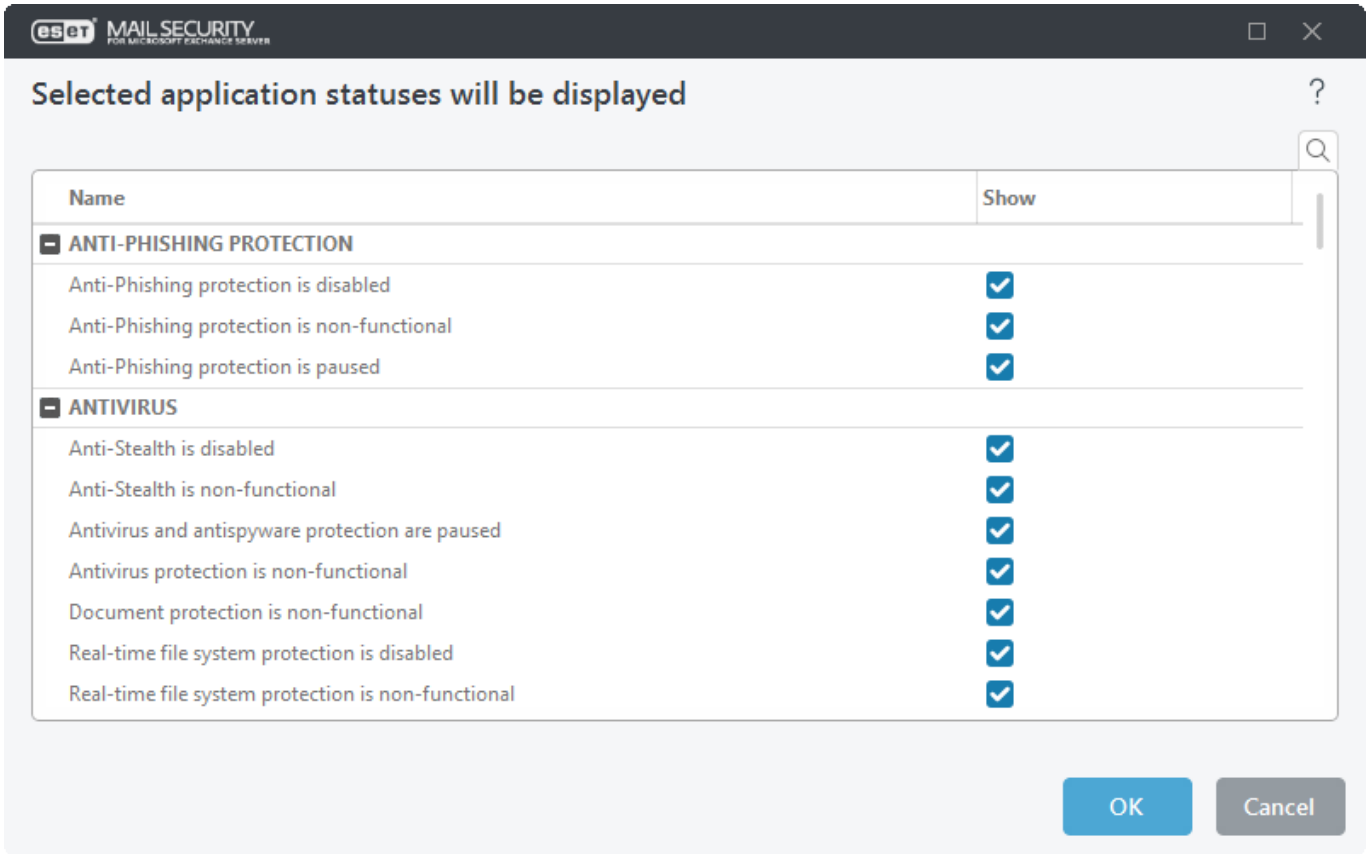
Notificaciones en el escritorio: pequeñas ventanas emergentes junto a la barra de tareas del sistema.

Alertas interactivas: ventanas de alerta y cuadros de mensajes que requieren la intervención del usuario.

Reenvío (notificaciones por correo electrónico): las notificaciones se envían a una dirección de correo electrónico especificada.

Estados de la aplicación

Esta ventana de diálogo le permite seleccionar o anular la selección de los estados de las aplicaciones que se mostrarán o no. Por ejemplo, cuando pause la protección del antivirus y antispyware que resultará en un cambio en el estado de protección que se mostrará en la página Supervisión. Si su producto no está activado o si su licencia ha caducado, también se mostrará el estado de la aplicación. Los estados de aplicación pueden administrarse mediante las ESET PROTECT políticas.



Mensajes y estados deshabilitados

Mensajes de confirmación

Le muestra una lista de mensajes de confirmación que puede seleccionar para que se muestren o no.

Estados de la aplicación

Le permite habilitar o deshabilitar el estado de visualización en la página Supervisión en el menú principal.

Notificaciones en el escritorio

La notificación en el escritorio se representa mediante una pequeña ventana de notificación junto a la barra de tareas del sistema. Está configurada de forma predeterminada para mostrarse durante 10 segundos y, a continuación, desaparece lentamente. ESET Mail Security se comunica con el usuario para informarle de actualizaciones correctas del producto, conexión de nuevos dispositivos, exploración de virus, finalización de tareas o detecciones nuevas encontradas.

Mostrar notificaciones de escritorio

Se recomienda mantener esta opción habilitada, para que el producto pueda informarle cuando tiene lugar un evento nuevo.

Notificaciones en el escritorio

Haga clic en **Editar** para seleccionar qué notificaciones del escritorio comunicarán diversos eventos.

Encienda el interruptor **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones no interactivas.

Tiempo de visualización en segundos

Defina la duración de la visibilidad de la notificación. El valor debe estar entre 3 y 30 segundos.

Transparencia

Defina el porcentaje de transparencia de la notificación. El intervalo admitido es de 0 (sin transparencia) a 80 (transparencia muy alta).

El menú desplegable **Cantidad mínima de detalle de sucesos para mostrar** le permite seleccionar el nivel de gravedad de las alertas y notificaciones. Se encuentran disponibles las siguientes opciones:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los historiales antes mencionados.
- **Informativo**: registra los mensajes de información, que incluyen los mensajes de actualizaciones correctas, y todos los historiales antes mencionados.
- **Advertencias**: registra los errores críticos y los mensajes de advertencia.
- **Errores**: se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico**: registra solo los errores críticos.

El campo **En sistemas con varios usuarios**, mostrar notificaciones en la pantalla de este usuario especifica qué usuario recibirá las notificaciones del sistema y otros tipos de notificaciones en los sistemas que permiten que se conecten varios usuarios al mismo tiempo. Normalmente, se trata de un administrador del sistema o de la red. Esta opción resulta especialmente útil para los servidores de terminal, siempre y cuando todas las notificaciones del sistema se envíen al administrador.

Permitir que las notificaciones se muestren en la pantalla: las notificaciones se mostrarán en la pantalla y podrá acceder a esta opción presionando Alt+Tab.

Personalización

En esta ventana, puede personalizar los mensajes que se usan en las notificaciones.

Mensaje de notificación – Un mensaje predeterminado que será mostrado en el pie de página de las notificaciones.

Detección

No cerrar notificaciones de detección de manera automática

Permite que las notificaciones de detección se mantengan en pantalla hasta que las cierre manualmente.

Utilizar mensaje predeterminado

Puede desactivar el mensaje predeterminado y especificar el mensaje de notificación de detección personalizado

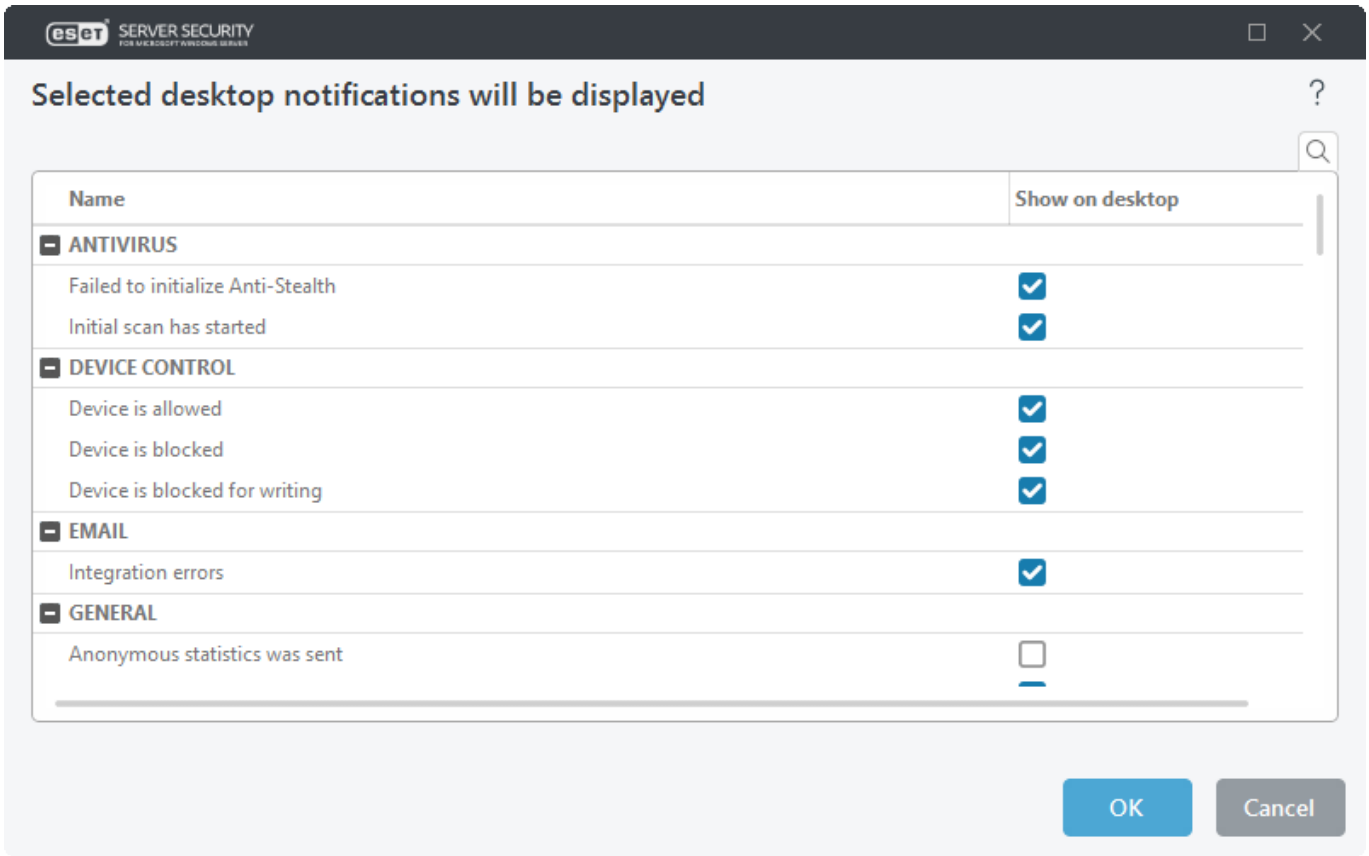
que se mostrará cuando se bloquee una detección.

Mensaje de notificación de detección

Ingrese un mensaje personalizado para mostrar cuando se bloquea una detección.

Notificaciones en el escritorio

Puede configurar las notificaciones de ESET Mail Security para que se muestren en el escritorio.



Alertas interactivas

Puede configurar la forma en que ESET Mail Security gestionará las alertas ante las amenazas y las notificaciones del sistema (como los mensajes sobre las actualizaciones correctas). Por ejemplo, la **duración** del tiempo de visualización y la **transparencia** en la área de notificación de Windows (esto solo se aplica a los sistemas que son compatibles con las notificaciones).

Mostrar alertas interactivas

Deshabilite esta función para evitar que ESET Mail Security muestre alertas en el área de notificación de Windows.

Lista de alertas interactivas

Útil para la automatización. Anule la selección de **Solicitar al usuario** para los elementos que desea automatizar y seleccione qué acción se llevará a cabo en lugar de la ventana de alerta que espera su interacción.

Los **cuadros de mensajes** se utilizan para mostrar preguntas o mensajes de texto corto.

Cerrar cuadros de mensajes automáticamente

Para cerrar las ventanas notificación automáticamente después de un período de tiempo determinado. Si no se cierran manualmente, las ventanas de alerta se cerrarán en forma automática una vez que transcurra el período especificado.

Mensajes de confirmación

Al hacer clic en **Editar**, se abrirá una ventana emergente con una lista de mensajes de confirmación que ESET Mail Security muestra antes de realizar una acción. Utilice las casillas de verificación para personalizar sus preferencias para los mensajes de confirmación.

Reenvío

ESET Mail Security puede enviar automáticamente correos electrónicos de notificación si ocurre un suceso con el nivel de detalle de los sucesos seleccionado.

Reenviar al correo electrónico

Habilite Reenviar notificaciones al correo electrónico para activar las notificaciones por correo electrónico.

Notificaciones reenviadas

Seleccione las notificaciones de escritorio que se reenvían al correo electrónico.

Configuración de correo electrónico

Nivel de detalle mínimo para las notificaciones: especifica el nivel mínimo de detalle de las notificaciones que se enviarán.

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros antes mencionados.
- **Informativo**: registra los mensajes de información como los eventos de red no estándar, que incluyen mensajes de actualizaciones correctas y todos los registros antes mencionados.
- **Advertencias**: registra errores graves y mensajes de advertencia (la tecnología Antistealth no se está ejecutando correctamente o el proceso de actualización ha fallado).
- **Errores**: se registrarán errores tales como “Error al descargar el archivo” y los errores críticos.
- **Crítico**: registra solo los errores críticos.

Enviar cada notificación en un correo electrónico por separado

Cuando se habilite, el destinatario recibirá un correo electrónico nuevo por cada notificación individual. Esto puede dar como resultado un gran número de correos electrónicos recibidos en un corto periodo de tiempo.

Intervalo luego del cual se enviarán correos electrónicos de notificación nuevos (min.)

Después del intervalo en minutos, se enviarán notificaciones nuevas por correo electrónico. Establezca el valor en 0 si desea enviar esas notificaciones inmediatamente.

Dirección del remitente

Ingrese la dirección del remitente que aparecerá en el encabezado de los correos electrónicos de notificación. Esto es lo que el destinatario verá en el campo **Desde**.

Dirección del destinatario

Especifique la dirección de correo electrónico del destinatario que se mostrará en el encabezado de los correos electrónicos de notificación. Use un punto y coma ";" para separar varias direcciones de correo electrónico.

Servidor SMTP

El nombre del servidor SMTP usado para enviar alertas y notificaciones. Este es normalmente el nombre de su Microsoft Exchange Server.

> Los servidores SMTP con cifrado TLS son admitidos por ESET Mail Security.

Nombre de usuario y contraseña

Si el servidor SMTP requiere autenticación, se deben completar estos campos con un nombre de usuario y una contraseña válidos para acceder al servidor SMTP.

Habilitar TLS

Habilita los mensajes de alertas y notificaciones admitidos por el cifrado TLS.

Probar conexión SMTP

Se enviará un mensaje de correo electrónico de prueba a la dirección de correo electrónico del destinatario.

Formato de mensajes

Las comunicaciones entre el programa y el usuario remoto o el administrador del sistema se llevan a cabo por medio de los correos electrónicos o los mensajes de la LAN (mediante el servicio de mensajería de Windows). Los mensajes de alerta predeterminados y el formato de notificación serán óptimos para la mayoría de situaciones. En ciertas circunstancias, es posible que necesite cambiar el formato de los mensajes de sucesos.

Formato de mensajes de sucesos

Especifique el formato de los mensajes de notificación de eventos de correo electrónico.

Formato de mensajes de advertencias sobre amenazas

Los mensajes de alerta y notificación de amenazas tienen un formato predeterminado predefinido. No es recomendable modificar dicho formato. No obstante, en ciertas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que necesite modificar el formato de los mensajes.

Las palabras clave (cadenas separadas por signos %) se reemplazan en el mensaje por la información real especificada. Se encuentran disponibles las siguientes palabras clave:

- %TimeStamp%: fecha y hora del evento.
- %Scanner%: módulo pertinente.
- %ComputerName%: nombre del equipo en el que se produjo la alerta.
- %ProgramName%: programa que generó la alerta.
- %DetectionObject%: nombre del archivo, mensaje, etc., infectado.
- %DetectionName%: identificación de la infección.
- %ErrorDescription%: descripción de un evento no causado por un virus.

Las palabras clave **%DetectionObject%** y **%DetectionName%** solo se usan en mensajes de alerta de amenazas, y **%ErrorDescription%** solo se usa en mensajes de sucesos.

Juego de caracteres

Puede elegir la codificación del menú desplegable. El mensaje de correo electrónico se convertirá de acuerdo con la codificación de caracteres seleccionada. Convierte un mensaje de correo electrónico en la codificación de caracteres ANSI que se basa en la configuración de Windows Regional (por ejemplo, windows-1250, Unicode (UTF-8), ACSII 7-bit, o Japonés (ISO-2022-JP)). Debido a esto, "á" se cambiará a "a" y un símbolo desconocido a "?".

Use la codificación de caracteres imprimibles

El origen del mensaje de correo electrónico se codificará en el formato Entrecomillado imprimible (QP) que utiliza los caracteres de ASCII y puede transmitir correctamente los caracteres nacionales especiales por correo electrónico en el formato de 8 bits (áéíóú).

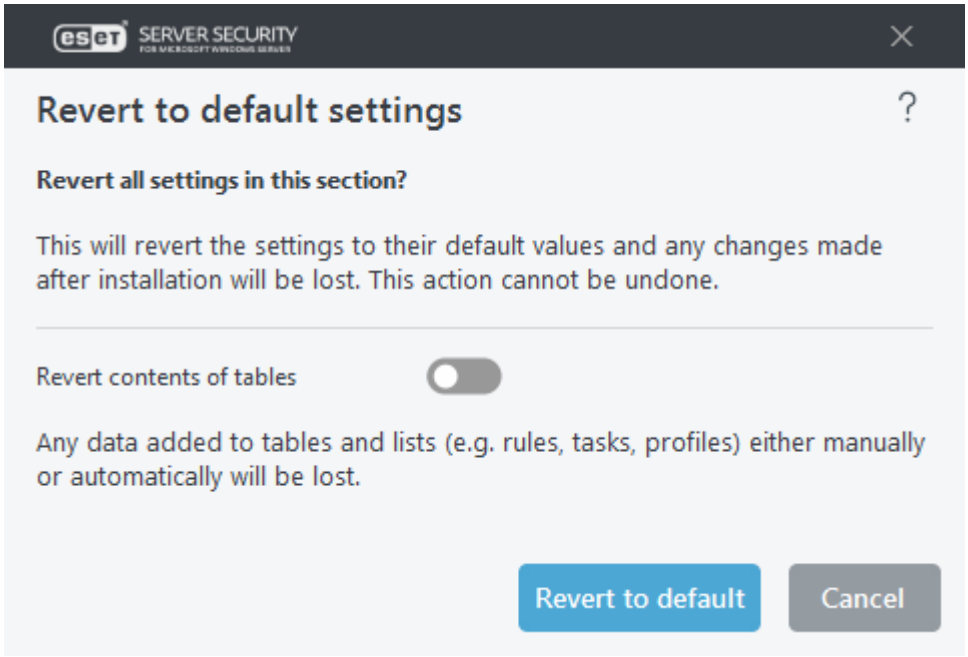
Revertir a la configuración predeterminada

Puede restaurar la configuración a sus valores predeterminados en **Configuración avanzada**. Hay dos opciones. Puede revertir todo a los ajustes predeterminados o revertir los ajustes sólo para una sección en particular (los ajustes en otras secciones permanecerán inalterados).

Restaurar todas las configuraciones – Todos los ajustes en todas las secciones de la configuración avanzada se restaurarán al estado en el que se encontraban después de haber instalado ESET Mail Security. Se puede considerar como una Restauración a los valores predeterminados de fábrica.

> i Una vez que haga clic en **Revertir a predeterminado**, todos los cambios que se hayan realizado se perderán y no se podrán deshacer. Esta acción no se puede deshacer.

Restablecer toda la configuración en esta sección - Restablece las configuraciones del módulo en la sección seleccionada a valores. Cualquier cambio que haya realizado en esta sección se perderá.



Revertir los contenidos de las tablas – Cuando se habilitan, las reglas, las tareas o los perfiles que se hayan agregado de manera manual o automática se perderán.

Ayuda y soporte

ESET Mail Security contiene herramientas de solución de problemas e información de soporte que lo ayudarán a resolver los problemas que puedan surgir.

Producto instalado

Información acerca del producto y la licencia

- Acerca de ESET Mail Security: muestra la información acerca de una copia de ESET Mail Security.
- Resolución de problemas del producto – Seleccione esta opción para buscar soluciones a los problemas más frecuentes. Es recomendable leer esta sección antes de ponerse en contacto con el equipo de soporte técnico.
- Resolución de problemas de licencia: para buscar soluciones a problemas con la activación o el cambio de licencia.
- Cambiar licencia: haga clic para abrir la ventana de activación y activar su producto.

Páginas de ayuda

Abre páginas de ayuda en línea para ESET Mail Security.

Base de conocimiento

Buscar en la base de conocimientos de ESET: la base de conocimiento de ESET contiene respuestas a las preguntas más frecuentes y soluciones recomendadas para varios problemas. La actualización regular por parte de los especialistas técnicos de ESET convierte a la base de conocimiento en la herramienta más potente para resolver varios tipos de problemas.

- Registro avanzado – Cree registros avanzados para todas las funciones disponibles con el fin de ayudar a los desarrolladores a diagnosticar y resolver problemas.

- Solicitar soporte: si no encuentra una respuesta a su problema, póngase en contacto con nuestro Departamento de Soporte Técnico.

- Detalles de soporte técnico – Muestra detalles de información (nombre del producto, versión del producto, etc.) para soporte técnico.

- ESET Log Collector – ESET Log Collector es una aplicación que recolecta la información en forma automática, tal como la configuración y los registros de su servidor para ayudar a resolver los problemas más rápidamente.

Enviar una solicitud de soporte

Con el fin de proporcionar asistencia lo más rápido posible y con la mayor exactitud, ESET solicita la información sobre la configuración de ESET Mail Security, la información detallada sobre el sistema, los procesos en ejecución (Registro de ESET SysInspector) y los datos de registro. ESET usará estos datos únicamente para proporcionar asistencia técnica al cliente. Este ajuste también se puede configurar desde **Configuración avanzada** (**F5**) > **Herramientas** > **Diagnósticos** > **Soporte técnico**.

> Si decide enviar los datos del sistema, debe completar y enviar el formulario web. De lo contrario, no se creará su comprobante y se perderán los datos de su sistema.

Cuando envía el formulario web, los datos de configuración de su sistema se enviarán a ESET. Seleccione **Enviar siempre esta información** para recordar esta acción para este proceso.

No enviar datos: Utilice esta opción si no desea enviar datos. Será redirigido a la página web de Soporte Técnico de ESET.

Acerca de ESET Mail Security

Esta ventana provee detalles sobre la versión instalada de ESET Mail Security. El sector superior de la ventana incluye la información sobre el sistema operativo y los recursos del sistema, el usuario actual y el nombre completo del equipo.

Componentes instalados

Contienen información sobre los módulos, para ver una lista de los componentes instalados y sus detalles. Haga clic en **Copiar** para copiar la lista al portapapeles. Puede resultar útil durante la solución de problemas o al ponerse en contacto con el soporte técnico.

Glosario

Visite la página Glosario para obtener más información acerca de los términos técnicos, amenazas y seguridad de internet.

Acuerdo de licencia de usuario final

Vigente a partir del 19 de octubre de 2021.

IMPORTANTE: Lea los términos y las condiciones del producto de aplicación que se especifican abajo antes de descargarlo, instalarlo, copiarlo o usarlo. **AL DESCARGAR, INSTALAR, COPIAR O UTILIZAR EL SOFTWARE, USTED DECLARA SU CONSENTIMIENTO CON LOS TÉRMINOS Y CONDICIONES Y RECONOCE QUE HA LEÍDO LA POLÍTICA DE PRIVACIDAD.**

Acuerdo de Licencia de Usuario Final

Los términos de este Acuerdo de licencia para el usuario final ("Acuerdo") ejecutado por y entre ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, registrado en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, n.° de entrada 3586/B, número de registro de negocio: 31333532 ("ESET" o el "Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tienen derecho a usar el Software definido en el Artículo 1 de este Acuerdo. El Software definido en este artículo puede almacenarse en un soporte digital, enviarse mediante correo electrónico, descargarse de Internet, descargarse de servidores del Proveedor u obtenerse de otras fuentes bajo los términos y condiciones mencionados más adelante.

ESTO ES UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL; NO UN CONTRATO DE COMPRA PARA ARGENTINA. El Proveedor sigue siendo el propietario de la copia del Software y del soporte físico en el que el Software se suministra en paquete comercial, así como de todas las demás copias a las que el Usuario final está autorizado a hacer en virtud de este Acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, descarga, copia o uso del Software, acepta los términos y condiciones de este Acuerdo y la Política de privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de privacidad, de inmediato haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE LA UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE CONSIENTE OBLIGARSE POR SUS TÉRMINOS Y CONDICIONES.

1. **Software.** Tal como se utiliza en este Acuerdo, el término "Software" significa: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todos los contenidos de los discos, CD-ROMs, DVDs, correos electrónicos y cualquier adjunto, u otros medios con los cuales se provee este Acuerdo, incluyendo el formulario del código objeto del software provisto en soporte digital, por medio de correo electrónico o descargado a través de la Internet; (iii) cualquier material escrito explicativo relacionado y cualquier otra documentación posible relacionada con el Software, sobre todo cualquier descripción del Software, sus especificaciones, cualquier descripción de las propiedades u operación del software, cualquier descripción del ambiente operativo en el cual se utiliza el Software, instrucciones de uso o instalación del Software o cualquier descripción del modo de uso del Software ("Documentación"); (iv) copias del Software, parches para posibles errores del Software, adiciones al Software, extensiones del Software, versiones modificadas del Software y actualizaciones de los componentes del Software, si existieran, con la autorización que le da a Usted el Proveedor con arreglo al Artículo 3 de este Acuerdo. El Software será provisto exclusivamente en la forma de código objeto ejecutable.

2. **Instalación, equipo y clave de licencia**. El Software suministrado en un soporte digital, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. El Software debe instalarse en un equipo correctamente configurado que cumpla, como

mínimo, con los requisitos especificados en la Documentación. La metodología de instalación se describe en la Documentación. No puede haber ningún programa informático ni Hardware que pudiera afectar al Software instalado en el equipo en el que instala el Software. El equipo hace referencia al Hardware que incluye, pero no se limita, a equipos personales, equipos portátiles, estaciones de trabajo, equipos de bolsillo, teléfonos inteligentes, dispositivos electrónicos portátiles o cualquier otro dispositivo para el que se diseñe el Software y en el que vaya a instalarse y/o utilizarse. La clave de licencia se refiere a una secuencia única de símbolos, letras números o caracteres especiales que se le brinda al Usuario final para permitirle el uso del Software de manera legal, así como de una versión específica de este o para brindarle una extensión de los términos de la Licencia en conformidad con el presente Acuerdo.

3. **Licencia**. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Usted tendrá el derecho no exclusivo y no transferible de instalar el Software en el disco rígido de un equipo o soporte similar para un almacenamiento permanente de datos, instalar y almacenar el Software en la memoria de un sistema informático e implementar, almacenar y mostrar el Software.

b) **Disposición sobre la cantidad de licencias.** El derecho a utilizar el Software estará sujeto a la cantidad de Usuarios finales. Un "Usuario final" se refiere a lo siguiente: (i) instalación del Software en un sistema informático, o (ii) si el alcance de una licencia está vinculado a la cantidad de buzones de correo, un Usuario final se referirá a un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("AUC"). Si un AUC acepta el correo electrónico y lo distribuye posteriormente en forma automática a varios usuarios, la cantidad de Usuarios finales se determinará conforme a la cantidad real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo cumple la función de una pasarela de correo, la cantidad de Usuarios finales será equivalente a la cantidad de usuarios de servidores de correo a los que dicha pasarela presta servicios. Si se envía una cantidad no especificada de direcciones de correo electrónico (por ejemplo, con alias) a un usuario y el usuario las acepta, y el cliente no distribuye automáticamente los mensajes a más usuarios, se requiere la Licencia únicamente para un equipo. No debe usar la misma Licencia en más de un equipo al mismo tiempo El Usuario final solo tiene derecho a introducir la Clave de licencia en el Software en la medida en que el Usuario final tenga derecho a usar el Software de acuerdo con la limitación derivada del número de Licencias otorgadas por el Proveedor. Se considera que la clave de Licencia es confidencial. No puede compartirla con terceros ni puede permitirles que la utilicen a menos que el presente Acuerdo o el Proveedor indique lo contrario. Si su clave de Licencia se encuentra en riesgo notifique al Proveedor de inmediato.

c) **Home/Business Edition.** La versión Home Edition del Software solo se usará en entornos privados o no comerciales para uso en el hogar y familiar exclusivamente. Debe obtener una versión Business Edition del software para poder usarla en un entorno comercial, así como en servidores, transmisores y puertas de enlace de correo o de Internet.

d) **Término de la Licencia.** El derecho a utilizar el Software tendrá un límite de tiempo.

e) **Software de OEM.** El software clasificado como "OEM" solo se puede usar en el equipo con el que se ha obtenido. No puede transferirse a otro equipo.

f) **Software NFR y versión de prueba.** Al Software clasificado como "No apto para la reventa", "NFR" o "Versión de prueba" no se le podrá asignar un pago y puede utilizarse únicamente para hacer demostraciones o evaluar las características del Software.

g) **Rescisión de la Licencia.** La Licencia se rescindirá automáticamente al finalizar el período para el cual fue otorgada. Si Usted no cumple con alguna de las disposiciones de este Acuerdo, el Proveedor tendrá el derecho de anular el Acuerdo, sin perjuicio de cualquier derecho o recurso judicial disponible para el Proveedor en dichas eventualidades. En el caso de cancelación de la Licencia, Usted deberá borrar, destruir o devolver de inmediato

por su propia cuenta el Software y todas las copias de seguridad a ESET o al punto de venta donde obtuvo el Software. Tras la finalización de la Licencia, el Proveedor podrá cancelar el derecho del Usuario Final a utilizar las funciones del Software que requieran conexión a los servidores del Proveedor o de terceros.

4. **Funciones con recopilación de información y requisitos para la conexión a Internet.** Para que funcione de manera correcta, el Software requiere conexión a Internet y debe conectarse a intervalos regulares a los servidores del Proveedor o de terceros y debe recopilar información en conformidad con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para llevar a cabo las siguientes funciones del Software:

a) **Actualizaciones del Software.** El Proveedor podrá publicar periódicamente actualizaciones o actualizaciones del Software ("Actualizaciones"), aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del Software y las Actualizaciones se instalan automáticamente, a menos que el Usuario final haya desactivado la instalación automática de Actualizaciones. Para aprovisionar Actualizaciones, es necesario verificar la autenticidad de la Licencia, lo que incluye información sobre el equipo o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La entrega de todas las actualizaciones puede estar sujeta a la Política de fin de la vida útil ("Política EOL"), disponible en https://go.eset.com/eol. No se proporcionarán actualizaciones una vez que el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil, como se define en la Política EOL.

b) **Envío de infiltraciones e información al Proveedor**. El Software contiene funciones que reúnen muestras de virus informáticos, otros programas informáticos dañinos y objetos sospechosos, problemáticos, potencialmente no deseados o potencialmente no seguros como archivos, URL, paquetes de IP y marcos de Ethernet (“Infiltraciones”) y luego los envía al Proveedor, incluidas, entre otras, la información sobre el proceso de instalación, el equipo o la plataforma en los cuales se instala el Software y la información sobre las operaciones y la funcionalidad del Software (“Información”). La Información y las Infiltraciones pueden contener datos (incluidos datos personales obtenidos aleatoriamente o accidentalmente) sobre el Usuario Final u otros usuarios del equipo en el cual se encuentra instalado el Software, y archivos afectados por Infiltraciones con metadatos asociados.

La Información y las Infiltraciones pueden ser recopiladas por las siguientes funciones del Software:

i. La función Sistema de reputación de LiveGride incluye la recopilación y el envío de hashes de una vía relacionados a Infiltraciones al Proveedor. Esta función se activa con la configuración estándar del Software.

ii. La función del sistema de comentarios de LiveGrid es recopilar información acerca de las infiltraciones con metadatos relacionados para enviársela al Proveedor. El Usuario final debe activar esta función durante la instalación del Software.

El proveedor solo debe hacer uso de la información y de las infiltraciones que recibe para analizar y para investigar las infiltraciones, para mejorar el Software y el proceso de verificación de la autenticidad de la Licencia. Asimismo, debe tomar las medidas correspondientes para garantizar la seguridad de las infiltraciones y de la información que recibe. Si se activa esta función del Software, el Proveedor deberá recopilar y procesar las infiltraciones y la información tal como se especifica en la Política de Privacidad y en conformidad con las normas legales vigentes. Puede desactivar estas funciones en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar información que permita al Proveedor identificarlo en conformidad con la Política de Privacidad. Por medio del presente, reconoce que el Proveedor utiliza sus propios medios para verificar si Usted hace uso del Software de acuerdo con las disposiciones del Acuerdo. Asimismo, reconoce que, a los efectos de este Acuerdo, es necesario que su información se transfiera durante las comunicaciones entre el Software y los sistemas informáticos del Proveedor o de sus socios comerciales como parte de la red de distribución y soporte del Proveedor a fin de garantizar la funcionalidad del Software, de autorizar el uso del Software y proteger los derechos del Proveedor.

Tras la finalización de este Acuerdo, el Proveedor o cualquiera de sus socios comerciales tendrán el derecho de transferir, procesar y almacenar datos esenciales que lo identifiquen, con el propósito de realizar la facturación y para la ejecución del presente Acuerdo y para transmitir notificaciones a su equipo.

Los detalles sobre la privacidad, la protección de la información personal y sus derechos como parte interesada pueden encontrarse en la Política de Privacidad, disponible en el sitio web del Proveedor y a la que se puede acceder de manera directa desde el proceso de instalación. También puede acceder a ella desde la sección de ayuda del Software.

5. **Ejercicio de los derechos del Usuario final**. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los sistemas informáticos para los que ha obtenido una Licencia.

6. **Restricciones de los derechos.** No puede copiar, distribuir, extraer componentes o crear versiones derivadas del Software. Al usar el Software, Usted tiene la obligación de cumplir con las siguientes restricciones:

a) Puede crear una copia del Software en un soporte de almacenamiento permanente de datos como una copia de seguridad para archivar, siempre que su copia de seguridad para archivar no esté instalada ni se utilice en ningún equipo. Cualquier otra copia que realice del Software constituirá un incumplimiento de este Acuerdo.

b) No puede utilizar, modificar, traducir ni reproducir el Software, o transferir los derechos de su uso o copias realizadas del Software de ninguna otra forma a lo establecido en este Acuerdo.

c) No puede vender, sublicenciar, arrendar o alquilar el Software, ni usarlo para suministrar servicios comerciales.

d) No puede aplicar técnicas de ingeniería inversa, descompilar o desmontar el Software, ni intentar obtener el código fuente del Software de ninguna otra forma, salvo en la medida en que esta restricción esté explícitamente prohibida por la ley.

e) Usted acepta que solo usará el Software de forma que se cumplan todas las leyes aplicables en la jurisdicción en la que lo utilice, incluyendo, pero sin limitarse a, las restricciones aplicables relacionadas con el copyright y otros derechos de propiedad intelectual.

f) Usted acepta que solamente usará el Software y sus funciones de una manera que no limite las posibilidades de otros Usuarios finales para acceder a estos servicios. El Proveedor se reserva el derecho de limitar el alcance los servicios proporcionados a Usuarios finales individuales, para activar el uso de los servicios por parte de la mayor cantidad posible de Usuarios finales. La limitación del alcance de los servicios también significará la terminación completa de la posibilidad de usar cualquiera de las funciones del Software y la eliminación de los Datos y de la información de los servidores de los Proveedores o de los servidores de terceros relacionados con una función específica del Software.

g) Usted acepta no ejercer ninguna actividad que implique el uso de la clave de Licencia de manera contraria a los términos de este Acuerdo ni que implique proporcionar la clave de Licencia a personas que no estén autorizadas a hacer uso del Software, como la transferencia de la clave de Licencia usada o no. en cualquier forma, así como la reproducción no autorizada, o la distribución de claves de Licencia duplicadas o generadas. Asimismo, no utilizará el Software como resultado del uso de una clave de Licencia obtenida de una fuente que no sea el Proveedor.

7. **Copyright**. El Software y todos los derechos, incluyendo, pero sin limitarse a, los derechos de propiedad y los derechos de propiedad intelectual, son propiedad de ESET y/o sus licenciatarios. Están protegidos por las disposiciones de tratados internacionales y por todas las demás leyes nacionales aplicables del país en el que se utiliza el Software. La estructura, la organización y el código del Software son valiosos secretos comerciales e información confidencial de ESET y/o sus licenciatarios. No puede copiar el Software, a excepción de lo especificado en el artículo 6 (a). Todas las copias que este Acuerdo le permita hacer deberán incluir el mismo

copyright y los demás avisos legales de propiedad que aparezcan en el Software. Si aplica técnicas de ingeniería inversa, descompila o desmonta el Software, o intenta obtener el código fuente del Software de alguna otra forma, en incumplimiento de las disposiciones de este Acuerdo, por este medio Usted acepta que toda la información obtenida de ese modo se considerará automática e irrevocablemente transferida al Proveedor o poseída por el Proveedor de forma completa desde el momento de su origen, más allá de los derechos del Proveedor en relación con el incumplimiento de este Acuerdo.

8. **Reserva de derechos**. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. **Versiones en varios idiomas, software en medios duales, varias copias**. En caso de que el Software sea compatible con varias plataformas o idiomas, o si Usted obtuvo varias copias del Software, solo puede usar el Software para la cantidad de sistemas informáticos y para las versiones correspondientes a la Licencia adquirida. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. **Comienzo y rescisión del Acuerdo.** Este Acuerdo es efectivo desde la fecha en que Usted acepta los términos de la Licencia. Puede poner fin a este Acuerdo en cualquier momento. Para ello, desinstale, destruya o devuelva permanentemente y por cuenta propia el Software, todas las copias de seguridad, y todos los materiales relacionados suministrados por el Proveedor o sus socios comerciales. Su derecho a usar el Software y cualquiera de sus funciones puede estar sujeto a la Política EOL. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de fin de su vida útil definida en la Política EOL, se terminará su derecho a usar el Software. Más allá de la forma de rescisión de este Acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán siendo aplicables por tiempo ilimitado.

11. **DECLARACIONES DEL USUARIO FINAL**. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA EN UNA CONDICIÓN "TAL CUAL ES", SIN UNA GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y HASTA EL ALCANCE MÁXIMO PERMITIDO POR LAS LEYES APLICABLES. NI EL PROVEEDOR, SUS LICENCIATARIOS, SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT PUEDEN HACER NINGUNA REPRESENTACIÓN O GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN ESPECÍFICO O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJIRÁ UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS. NO EXISTE NINGUNA GARANTÍA DEL PROVEEDOR NI DE NINGUNA OTRA PARTE DE QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE CUMPLIRÁN CON SUS REQUISITOS O DE QUE LA OPERACIÓN DEL SOFTWARE SERÁ ININTERRUMPIDA O ESTARÁ LIBRE DE ERRORES. USTED ASUME TODA LA RESPONSABILIDAD Y EL RIESGO POR LA ELECCIÓN DEL SOFTWARE PARA LOGRAR SUS RESULTADOS DESEADOS Y POR LA INSTALACIÓN, EL USO Y LOS RESULTADOS QUE OBTENGA DEL MISMO.

12. **Sin más obligaciones**. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciatarios, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. **LIMITACIÓN DE RESPONSABILIDAD**. EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O LICENCIADORES SERÁN RESPONSABLES DE PÉRDIDAS DE INGRESOS, GANANCIAS, VENTAS, DATOS O COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUIDOS, DAÑOS A LA PROPIEDAD, DAÑOS PERSONALES, INTERRUPCIÓN DEL NEGOCIO, PÉRDIDA DE INFORMACIÓN COMERCIAL O DE CUALQUIER VALOR ESPECIAL, DIRECTO, INSONDADO, ACCIDENTAL, ECONÓMICO, DE COBERTURA, DAÑOS PUNITIVOS, ESPECIALES O CONSECUENCIALES, QUE SIN EMBARGO DERIVEN O SURJAN POR CONTRATO, AGRAVIOS, NEGLIGENCIA U OTRA TEORÍA DE RESPONSABILIDAD QUE DERIVE DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USAR EL SOFTWARE, AUNQUE EL PROVEEDOR, SUS LICENCIADORES O FILIALES RECIBAN INFORMACIÓN DE LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE

RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Nada de lo contenido en este Acuerdo perjudicará los derechos estatutarios de ninguna parte que actúe en calidad de consumidor si infringe dicho Acuerdo.

15. **Soporte técnico**. ESET o los terceros autorizados por ESET suministrarán soporte técnico a discreción propia, sin ninguna garantía ni declaración. Cuando el software o cualquiera de sus funciones lleguen a la fecha de fin de la vida útil definida en la Política EOL, no se proporcionará soporte técnico. El Usuario final deberá crear una copia de seguridad de todos los datos existentes, software y prestaciones de los programas en forma previa al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET no pueden aceptar la responsabilidad por el daño o pérdida de datos, propiedad, software o hardware, o pérdida de beneficios debido al suministro de soporte técnico. ESET y/o los terceros autorizados por ESET se reservan el derecho de decidir si la solución del problema excede el alcance del soporte técnico. ESET se reserva el derecho de rechazar, suspender o dar por finalizado el suministro de soporte técnico a discreción propia. Se puede solicitar información sobre la Licencia y cualquier otro tipo de información a fin de brindar soporte técnico conforme a la Política de Privacidad.

16. **Transferencia de la Licencia**. El Software puede transferirse de un sistema informático a otro, a menos que esta acción infrinja los términos del presente Acuerdo. Si no infringe los términos del Acuerdo, el Usuario final solamente tendrá derecho a transferir en forma permanente la Licencia y todos los derechos derivados de este Acuerdo a otro Usuario final con el consentimiento del Proveedor, sujeto a las siguientes condiciones: (i) que el Usuario final original no se quede con ninguna copia del Software; (ii) que la transferencia de los derechos sea directa, es decir, del Usuario final original al nuevo Usuario final; (iii) que el nuevo Usuario final asuma todos los derechos y obligaciones pertinentes al Usuario final original bajo los términos de este Acuerdo; (iv) que el Usuario final original le proporcione al nuevo Usuario final la Documentación que habilita la verificación de la autenticidad del Software, como se especifica en el artículo 17.

17. **Verificación de la autenticidad del Software.** El Usuario final puede demostrar su derecho a usar el Software en una de las siguientes maneras: (i) a través de un certificado de licencia emitido por el Proveedor o por un tercero designado por el Proveedor; (ii) a través de un acuerdo de licencia por escrito, en caso de haberse establecido dicho acuerdo; (iii) a través de la presentación de un correo electrónico enviado por el Proveedor donde se incluyan los detalles de la Licencia (nombre de usuario y contraseña). Se puede solicitar información sobre la Licencia y datos sobre el Usuario final a para llevar a cabo la verificación de la autenticidad del Software conforme a la Política de Privacidad.

18. **Licencias para autoridades públicas y el gobierno de los Estados Unidos**. Se deberá suministrar el Software a las autoridades públicas, incluyendo el gobierno argentino, con los derechos de la Licencia y las restricciones descritas en este Acuerdo.

19. **Cumplimiento del control comercial**.

a) Usted no podrá, ya sea directa o indirectamente, exportar, reexportar o transferir el Software, o de alguna otra forma ponerlo a disposición de ninguna persona, o utilizarlo de ninguna manera, o participar de ningún acto, que pueda ocasionar que ESET o sus compañías controladoras, sus empresas subsidiarias y las subsidiarias de cualquiera de sus compañías controladoras, así como también las entidades controladas por sus compañías controladoras ("Afiliadas") violen, o queden sujetas a las consecuencias negativas de las Leyes de Control Comercial, las cuales incluyen

i. toda ley que controle, restrinja o imponga requisitos de licencia a la exportación, reexportación o transferencia de productos, software, tecnología o servicios, establecida o adoptada por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas y

ii. cualquier sanción, restricción, embargo, prohibición de exportación o importación, prohibición de transferencia de fondos o activos o prohibición de prestación de servicios, ya sea de índole económica, financiera, comercial o de otro tipo, o toda medida equivalente impuesta por cualquier gobierno, estado o autoridad reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados Miembro, o cualquier país donde deban cumplirse las obligaciones conforme al Acuerdo, o donde ESET o cualquiera de sus Afiliadas operen o estén constituidas.

(actos legales mencionados en los puntos i y ii. anteriormente, denominados "Leyes de control comercial").

b) ESET tendrá el derecho de suspender sus obligaciones conforme a estos Términos o terminar el Acuerdo, con efecto inmediato, en los siguientes casos:

i. ESET determina que, en su razonable opinión, el Usuario ha violado o podría violar la disposición del Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software quedan sujetos a las Leyes de Control Comercial y, en consecuencia, ESET determina que, en su razonable opinión, el cumplimiento continuo de sus obligaciones conforme al Acuerdo podría ocasionar que ESET o sus Afiliadas incurriesen en la violación de las Leyes de Control Comercial o quedasen sujetas a las consecuencias negativas de estas.

c) Ninguna de las estipulaciones del Acuerdo tiene por objeto inducir o exigir, ni debe interpretarse como una intención de inducir o exigir a ninguna de las partes actuar o abstenerse de actuar (o acordar actuar o abstenerse de actuar) de ninguna manera que resulte inconsistente con las Leyes de Control Comercial aplicables, o se encuentre penalizada o prohibida por estas.

20. **Avisos**. Todos los avisos y devoluciones de software o documentación deben entregarse a: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle cualquier cambio de este Acuerdo, las Políticas de privacidad, la Política de EOL y la Documentación de acuerdo con el artículo. 22 del Acuerdo. ESET puede enviarle correos electrónicos, notificaciones en la aplicación a través del Software o publicar la comunicación en nuestro sitio web. Acepta recibir comunicaciones legales de ESET de forma electrónica, lo que incluye comunicaciones sobre cambios de Términos, Términos especiales o Políticas de privacidad, cualquier contrato de trabajo o aceptación o invitación a tratar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. **Legislación aplicable**. Este Acuerdo se regirá e interpretará conforme a la legislación de la República Eslovaca. En el presente Acuerdo, el Usuario final y el Proveedor aceptan que los principios del conflicto de leyes y la Convención de las Naciones Unidas sobre los Contratos de Venta Internacional de Bienes no serán aplicables. Acepta expresamente que cualquier disputa o demanda derivada del presente Acuerdo con respecto al Proveedor o relativa al uso del Software deberá resolverse por el Tribunal del Distrito de Bratislava I., Eslovaquia; asimismo, Usted acepta expresamente el ejercicio de la jurisdicción del Tribunal mencionado.

22. **Disposiciones generales**. Si alguna disposición de este Acuerdo no es válida o aplicable, no afectará la validez de las demás disposiciones del Acuerdo, que seguirán siendo válidas y ejecutables bajo las condiciones aquí estipuladas. Este acuerdo se ha ejecutado en inglés. En el caso de que se prepare cualquier traducción del acuerdo para su comodidad o con cualquier otro fin, o en caso de discrepancia entre las versiones en diferentes idiomas de este acuerdo, prevalecerá la versión en inglés.

ESET se reserva el derecho de realizar cambios en el Software, así como de revisar los términos de este Acuerdo, sus Anexos, la Política de privacidad, la Política y la Documentación de EOL o cualquier parte de ellos, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar cambios del Software o el comportamiento comercial de ESET, (ii) por cuestiones legales, normativas o de seguridad; o (iii) para evitar abusos o daños. Se le notificará cualquier revisión del Acuerdo por correo electrónico, notificación en la aplicación

o por otros medios electrónicos. Si no está de acuerdo con los cambios de texto del Acuerdo, puede rescindirlo de acuerdo con el Artículo 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios de texto se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el acuerdo entero entre el proveedor y Usted relacionado con el Software y reemplaza a cualquier representación, discusión, garantía, comunicación o publicidad previa relacionadas con el Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Política de privacidad

La protección de los datos personales reviste especial importancia para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrita en el Registro comercial del Tribunal de Distrito de Bratislava I, Sección Sro, Registro N.º 3586/B, Número de registro de empresa: 31333532 como controlador de datos (“ESET” o “Nosotros”). Queremos cumplir con el requisito de transparencia de acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (“RGPD”). A fin de cumplir con el objetivo, publicamos la presente Política de privacidad con el único propósito de informar a nuestros clientes (“Usuario final” o “Usted”), en carácter de interesados, acerca de los siguientes temas relativos a la protección de los datos personales:

- Fundamento jurídico para el procesamiento de datos personales.
- Intercambio y confidencialidad de los datos.
- Seguridad de los datos.
- Sus derechos como interesado.
- Procesamiento de sus datos personales.
- Información de contacto.

Procesamiento de sus datos personales

Los servicios prestados por ESET implementados en nuestro producto se prestan de acuerdo con los términos del EULA, pero algunos pueden requerir atención especial. Quisiéramos brindarle más detalles sobre la recolección de datos relacionada a la provisión de nuestros servicios. Prestamos diversos servicios descritos en el EULA y la documentación. Para hacer que todo funcione, necesitamos recolectar la siguiente información:

- Estadísticas sobre actualizaciones y de otro tipo con información relativa al proceso de instalación y a su ordenador, lo que incluye la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos, como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto.
- Funciones hash unidireccionales relativas a infiltraciones como parte del sistema de reputación de ESET LiveGrid®, que mejora la eficiencia de nuestras soluciones de protección frente a programas malignos comparando archivos analizados con una base de datos de elementos puestos en listas blancas y negras en la nube.
- Muestras y metadatos sospechosos de la circulación, parte del sistema de realimentación de ESET LiveGrid®, que permite a ESET reaccionar de forma inmediata ante las necesidades de sus usuarios finales y responder a las amenazas más recientes. Nosotros dependemos de que Usted nos envíe:
    - infiltraciones como muestras potenciales de virus y otros programas malignos y sospechosos; objetos problemáticos o potencialmente no deseados o inseguros, como archivos ejecutables, mensajes de correo electrónico que haya clasificado, como correo no deseado o que nuestro producto haya marcado;

- información sobre dispositivos de la red local, como el tipo, el proveedor, el modelo o el nombre del dispositivo;
- información relativa al uso de Internet, como dirección IP e información geográfica, paquetes IP, URL y marcos de Ethernet;
- archivos de volcado de memoria y la información que contienen.

No necesitamos recopilar datos por fuera de este ámbito. Sin embargo, en algunas ocasiones no podemos evitarlo. Los datos recopilados accidentalmente pueden incluirse como malware y Nosotros no pretendemos que sean parte de nuestros sistemas o procesarlos para el cumplimiento de los objetivos detallados en la presente Política de privacidad.

- Para fines de facturación, verificación de autenticidad de la licencia y prestación de nuestros servicios, se requiere información de licencia como identificación de licencia y datos personales, como nombre, apellido, dirección y dirección de correo electrónico.
- Pueden ser necesarios datos de contacto y datos contenidos en sus solicitudes de soporte para el servicio técnico. Basados en el medio que Usted eligió para comunicarse con Nosotros, podemos recopilar su correo electrónico, número de teléfono, datos de licencia, detalles del producto y descripción de su caso de asistencia. Podemos solicitarle que proporcione información adicional para facilitar la prestación del servicio de soporte.

Intercambio y confidencialidad de los datos

No compartimos sus datos con terceros. Sin embargo, ESET es una compañía que opera globalmente a través de entidades afiliadas o socios como parte de nuestra red de venta, servicio y soporte. La información sobre licencias, facturación y soporte técnico que procesa ESET puede ser transferida desde las entidades afiliadas o los socios o hacia ellos a fin de ejecutar el EULA, por ejemplo, para la prestación de servicios o soporte.

ESET prefiere procesar sus datos en la Unión Europea (UE). Sin embargo, según su ubicación (el uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transmitir sus datos a un país ubicado fuera de la UE. Por ejemplo, usamos servicios de terceros en conexión con la informática en la nube. En estos casos, seleccionamos cuidadosamente a nuestros proveedores de servicios y garantizamos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por regla general, pactamos las cláusulas contractuales estándar de la UE, si es necesario, con normas contractuales complementarias.

En el caso de algunos países fuera de la UE, como Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos equivalente. Debido a este nivel de protección de datos equivalente, la transferencia de datos hacia estos países no requiere ninguna autorización ni acuerdo especial.

Derechos de la persona registrada

Los derechos de los Usuarios finales son importantes. Queremos informarle que cada Usuario final (de cualquier país, dentro y fuera de la Unión Europea) tiene los siguientes derechos, que ESET garantiza. Para ejercer los derechos de los interesados, puede comunicarse con nosotros a través del formulario de soporte o por correo electrónico a la siguiente dirección: dpo@eset.sk. A fin de poder identificarlo, le solicitamos la siguiente información: Nombre, dirección de correo electrónico y, de estar disponible, clave de licencia o número de cliente y empresa de afiliación. No debe enviarnos ningún otro dato personal, como la fecha de nacimiento. Queremos señalar que, para poder procesar su solicitud, así como con fines de identificación, procesaremos sus datos personales.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento resulta aplicable únicamente cuando nuestro procesamiento requiera su consentimiento. Si procesamos sus datos personales en razón de su

consentimiento, tiene derecho a retirarlo en cualquier momento sin expresión de causa. Solo podrá retirar su consentimiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad.

Derecho a oponerse. El derecho a oponerse al procesamiento resulta aplicable únicamente cuando nuestro procesamiento esté basado en el interés legítimo de ESET o un tercero. Si procesamos sus datos personales en pos de un interés legítimo, Usted, como interesado, tiene derecho a oponerse, en cualquier momento, al interés legítimo que designemos y al procesamiento de sus datos personales. Solo podrá oponerse al procesamiento con efectos para el futuro, lo que no afectará la legitimidad de los datos procesados con anterioridad. Si procesamos sus datos personales con fines de marketing directo, no es necesario que exprese una causa. Esto también se aplica a la elaboración de perfiles, ya que se relaciona con el marketing directo. En todos los demás casos, le solicitamos que nos informe, de forma breve, sus quejas en contra del interés legítimo de ESET para el procesamiento de sus datos personales.

Tenga en cuenta que, en algunos casos, a pesar de que haya retirado su consentimiento, tenemos derecho a continuar procesando sus datos personales en función de algún otro fundamento jurídico, por ejemplo, para el cumplimiento de un contrato.

Derecho de acceso. En carácter de interesado, Usted tiene derecho a obtener información de los datos que almacene ESET sobre usted de forma gratuita, en cualquier momento.

Derecho a solicitar una rectificación. En caso de que procesemos de forma involuntaria datos personales incorrectos sobre Usted, tiene derecho a que se corrija esta información.

Derecho a solicitar el borrado de los datos y la restricción en el procesamiento. En carácter de interesado, Usted tiene derecho a solicitar el borrado de sus datos personales o una restricción en su procesamiento. Si procesamos sus datos personales, por ejemplo, con su consentimiento, Usted lo retira y no hay ningún otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. También eliminaremos sus datos personales en cuanto ya no sean necesarios para los fines indicados cuando finalice nuestro período de retención.

Si usamos sus datos personales únicamente con el fin de marketing directo y Usted ha retirado su consentimiento o se ha opuesto al interés legítimo subyacente de ESET, restringiremos el procesamiento de sus datos personales, lo que implicará que sus datos de contacto se incluyan en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales serán eliminados.

Tenga en cuenta que podemos tener la obligación de almacenar sus datos hasta que finalicen los períodos y las obligaciones de retención determinados por el legislador o las autoridades supervisoras. La legislación eslovaca también podría determinar períodos y obligaciones de retención. A partir de su finalización, los datos correspondientes se eliminarán de forma rutinaria.

Derecho a la portabilidad de datos. Nos complace proporcionarle a Usted, en carácter de interesado, los datos personales que procese ESET en formato xls.

Derecho a presentar una queja. Como interesado, Usted tiene el derecho de presentar una queja a una autoridad supervisora en cualquier momento. ESET se encuentra sujeto a la regulación de las leyes eslovacas y Nosotros cumplimos con la ley de protección de datos como parte de la Unión Europea. La autoridad supervisora competente en materia de datos es la Oficina de Protección de Datos Personales de la República de Eslovaquia, con sede en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Información de contacto

Si desea ejercer su derecho como persona registrada o tiene una consulta o preocupación, envíenos un mensaje

a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk