TREND MICRO

XG

OfficeScan™

Manual del administrador

Para empresas grandes y medianas

Endpoint Security

Protected Cloud

Web Security

Trend Micro Incorporated se reserva el derecho de efectuar cambios en este documento y en el producto que en él se describe sin previo aviso. Antes de instalar y empezar a utilizar el producto, consulte los archivos Léame, las notas de la versión y la última versión de la documentación correspondiente que encontrará disponible en el sitio Web de Trend Micro en:

http://docs.trendmicro.com/es-es/enterprise/officescan.aspx

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs son marcas comerciales o marcas comerciales registradas de Trend Micro Incorporated. El resto de nombres de productos o empresas pueden ser marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.

Copyright © 2016. Trend Micro Incorporated. Reservados todos los derechos.

Nº de documento: OSSMXG7606/161028

Fecha de publicación: Octubre de 2016

Protegido por las patentes de Estados Unidos: 5,951,698

Esta documentación presenta las características principales del producto y proporciona instrucciones de instalación para un entorno de producción. Léala detenidamente antes de instalar o utilizar el producto.

También encontrará información pormenorizada sobre cómo utilizar funciones específicas del producto en el Centro de ayuda en línea de Trend Micro y en la Base de conocimientos de Trend Micro.

Trend Micro trata constantemente de mejorar la documentación. Si tiene alguna duda, comentario o sugerencia con relación a este o a cualquier otro documento de Trend Micro, póngase en contacto con nosotros a través de la dirección de correo electrónico docs@trendmicro.com.

Evalúe esta documentación en el siguiente sitio Web:

http://www.trendmicro.com/download/documentation/rating.asp

Tabla de contenidos

Prefacio

Prefacio xiii

Documentación de OfficeScan xiv

Audiencia xv

Convenciones del documento xv

Terminología xvi

Parte I: Introducción y cómo empezar

Capítulo 1: Presentación de OfficeScan

Acerca de OfficeScan 1-2

Novedades de OfficeScan XG 1-2

Funciones y ventajas principales 1-5

El servidor de OfficeScan 1-9

El agente de OfficeScan 1-11

Integración con los productos y servicios de Trend Micro 1-11

Capítulo 2: Introducción a OfficeScan

La consola Web 2-2

El Panel 2-5

Server Migration Tool 2-37

Integración con Active Directory 2-42

Árbol de agentes de OfficeScan 2-45

Dominios de OfficeScan 2-61

Capítulo 3: Introducción a la protección de datos

Instalación de la protección de datos 3-2
Licencia de protección de datos 3-4
Implementación de la protección de datos en los agentes de OfficeScan 3-6
Carpeta forense y base de datos de DLP 3-9
Desinstalación de la protección de datos 3-15

Parte II: Protección de los agentes de OfficeScan

Capítulo 4: Uso de la Smart Protection de Trend Micro

Acerca de la Smart Protection de Trend Micro 4-2
Servicios de Smart Protection 4-3
Fuentes de Smart Protection 4-6
Archivos de patrones de Smart Protection 4-8
Configuración de los Servicios de Smart Protection 4-13
Uso de los Servicios de Smart Protection 4-33

Capítulo 5: Instalación del agente de OfficeScan

Instalaciones nueva del agente de OfficeScan 5-2
Consideraciones sobre la instalación 5-2
Consideraciones sobre la implementación 5-13
Migración al agente de OfficeScan 5-71
Posterior a la instalación 5-75
Desinstalación del Agente de OfficeScan 5-78

Capítulo 6: Mantener actualizada la protección

Componentes y programas de OfficeScan 6-2
Información general de actualizaciones 6-13
Actualizaciones del servidor de OfficeScan 6-16
Actualizaciones del Smart Protection Server Integrado 6-29
Actualizaciones del agente de OfficeScan 6-30
Agentes de actualización 6-59
Resumen de la actualización de componentes 6-68

Capítulo 7: Buscando riesgos de seguridad

Acerca de los riesgos de seguridad 7-2
Tipos de métodos de exploración 7-9
Tipos de exploración 7-15
Configuración común para todos los tipos de exploración 7-28
Derechos y otras configuraciones de la exploración 7-59
Configuración general de la exploración 7-75
Notificaciones de riesgos de seguridad 7-87
Registros de riesgos de seguridad 7-98
Epidemias de riesgos de seguridad 7-114

Capítulo 8: Protección frente a amenazas desconocidas

Aprendizaje automático predictivo 8-2
Servicio de conexión sospechosa 8-5
Envío de muestras 8-9
Registros de amenazas desconocidas 8-11

Capítulo 9: Uso de Supervisión del comportamiento

Supervisión del comportamiento 9-2

Configuración de las opciones de supervisión de comportamiento global 9-13

Privilegios de supervisión de comportamiento 9-15

Notificaciones de la supervisión del comportamiento para usuarios del agente de OfficeScan 9-16

Registros de supervisión del comportamiento 9-18

Capítulo 10: Uso del Control de dispositivos

Control de dispositivos 10-2

Permisos para dispositivos de almacenamiento 10-4

Permisos para dispositivos sin almacenamiento 10-11

Administración del acceso a dispositivos externos (protección de datos activada) 10-11

Administración del acceso a dispositivos externos (protección de datos no activada) 10-15

Modificación de las notificaciones de Control de dispositivos 10-19

Registros de control de dispositivos 10-19

Capítulo 11: Uso de la Prevención de pérdida de datos

Acerca de la prevención de pérdida de datos (DLP) 11-2

Políticas de prevención de pérdida de datos 11-3

Tipos de identificadores de datos 11-6

Plantillas de prevención de pérdida de datos 11-21

Canales de la DLP 11-26

Acciones de la prevención de pérdida de datos 11-41

Excepciones de la prevención de pérdida de datos 11-44

Configuración de las políticas de prevención de pérdida de datos 11-50

Notificaciones de la prevención de pérdida de datos 11-56

Registros de prevención de pérdida de datos 11-60

Capítulo 12: Uso de Web Reputation

Acerca de las amenazas Web 12-2
Servicios de Command & Control Contact Alert 12-2
Reputación Web 12-4
Políticas de reputación Web 12-5
Notificaciones de amenazas Web para usuarios del agente 12-14
Notificaciones de rellamadas de C&C para administradores 12-15
Notificaciones de C&C Contact Alert para los usuarios del agente ... 12-19
Epidemias de rellamada de C&C 12-20
Registros de amenazas Web 12-22

Capítulo 13: Uso de OfficeScan Firewall

Acerca de OfficeScan Firewall 13-2
Activar o desactivar OfficeScan Firewall 13-6
Perfiles y políticas del cortafuegos 13-8
Derechos del cortafuegos 13-24
Configuración general del cortafuegos 13-26
Notificaciones de infracciones del cortafuegos para los usuarios del agente de OfficeScan 13-29
Registros del cortafuegos 13-30
Epidemias de infracciones del cortafuegos 13-32
Comprobar OfficeScan Firewall 13-34

Parte III: Administración del servidor y los agentes de OfficeScan

Capítulo 14: Administrar el servidor de OfficeScan

Role-based Administration 14-3
Trend Micro Control Manager 14-26
Configuración de la lista de objetos sospechosos 14-34
Servidores de referencia 14-36
Configuración de las notificaciones del administrador 14-39
Registros de sucesos del sistema 14-41
Administración de registros 14-43
Licencias 14-47
Copia de seguridad de la base de datos de OfficeScan 14-50
Herramienta de migración de SQL Server 14-52
Configuración de la conexión del servidor Web y el agente de OfficeScan 14-56
Comunicación entre servidor y agente 14-57
Contraseña de la consola Web 14-64
Configuración de la Consola Web 14-64
Administrador de cuarentena 14-65
Server Tuner 14-66
Smart Feedback 14-69

Capítulo 15: Administración del agente de OfficeScan

Ubicación del Endpoint 15-2
Administración del programa del agente de OfficeScan 15-7
Conexión agente-servidor 15-28
Configuración del proxy del agente de OfficeScan 15-54
Visualización de información sobre agentes de OfficeScan 15-60
Importación y exportación de la configuración de los agentes 15-61

Conformidad con las normas de seguridad 15-62
Compatibilidad con Trend Micro Virtual Desktop 15-82
Configuración global para los agentes 15-97
Configuración de derechos y otras configuraciones de los agentes ... 15-99

Parte IV: Protección adicional

Capítulo 16: Protección de los agentes fuera de las instalaciones

Edge Relay Server 16-2
Requisitos del sistema de Edge Relay Server 16-3
Instalación de Edge Relay Server 16-4
Conexión con Edge Relay Server 16-13
Administración de la conexión de Edge Relay Server 16-14
Administración de certificados de Edge Relay Server 16-16

Capítulo 17: Uso de Plug-in Manager

Acerca de Plug-in Manager 17-2
Instalación de Plug-in Manager 17-3
Administrar las características nativas de OfficeScan 17-4
Administración de Programas de complemento 17-5
Desinstalación de Plug-in Manager 17-12
Solución de problemas de Plug-in Manager 17-13

Capítulo 18: Recursos de solución de problemas

Soporte de sistema de inteligencia 18-2
Herramienta de diagnóstico de casos 18-2
Herramienta de ajuste del rendimiento de Trend Micro 18-2

Registros del servidor de OfficeScan 18-3
Registros de agentes de OfficeScan 18-15

Capítulo 19: Asistencia técnica

Recursos de solución de problemas 19-2
Ponerse en contacto con Trend Micro 19-3
Enviar contenido sospechoso a Trend Micro 19-4
Otros recursos 19-5

Apéndices

Apéndice A: Compatibilidad con IPv6 en OfficeScan

Compatibilidad de IPv6 con el servidor y los agentes de OfficeScan ... A-2
Configuración de direcciones IPv6 ..... A-6
Pantallas que muestran direcciones IP A-7

Apéndice B: Compatibilidad de Windows Server Core

Compatibilidad de Windows Server Core B-2
Métodos de instalación para Windows Server Core B-2
Funciones del agente de OfficeScan en Windows Server Core B-6
Comandos de Windows Server Core B-7

Apéndice C: Compatibilidad con Windows 8/8.1/10 y Windows Server 2012/2016

Acerca de Windows 8/8.1/10 y Windows Server 2012/2016 ..... C-2
Compatibilidad de la característica OfficeScan por parte del modo de interfaz de usuario C-5
Internet Explorer 10/11 y Microsoft Edge C-6

Apéndice D: Recuperación de OfficeScan

Recuperación del servidor de OfficeScan y los Agentes de OfficeScan mediante el paquete de copia de seguridad del servidor D-2

Apéndice E: Glosario

ActiveUpdate E-2
Archivo comprimido E-2
Cookie E-2
Ataque de denegación de servicio E-2
DHCP E-2
DNS E-3
Nombre del dominio E-3
Dirección IP dinámica E-3
ESMTP E-4
Contrato de licencia para usuario final E-4
Falso positivo E-4
FTP E-4
GeneriClean E-4
Revisión E-5
HTTP E-5
HTTPS E-6
ICMP E-6
IntelliScan E-6
IntelliTrap E-7
IP E-7
Archivo Java E-7
LDAP E-8
Puerto de escucha E-8
Agente de MCP E-8

Ataque de amenazas mixtas E-9
NAT E-9
NetBIOS E-9
Comunicación unidireccional E-9
Parche E-10
Ataques de phishing E-10
Ping E-11
POP3 ..... E-11
Servidor proxy E-11
RPC E-11
Revisión de seguridad E-11
Service Pack E-12
SMTP E-12
SNMP E-12
Captura SNMP E-12
SSL E-12
Certificado SSL E-13
TCP E-13
Telnet E-13
Puerto de troyano E-13
Puerto de confianza E-15
Comunicación bidireccional E-16
UDP E-16
Archivos que no se pueden limpiar E-16

Índice

Índice IN-1

Prefacio

Prefacio

Este documento contiene información introductoria, procedimientos de instalación de agentes e instrucciones para la administración de servidores y agentes de OfficeScan.

Los temas que se incluyen son:

- *Documentación de OfficeScan en la página xiv*
- *Audiencia en la página xv*
- *Convenciones del documento en la página xv*
- *Terminología en la página xvi*

Documentación de OfficeScan

La documentación de OfficeScan incluye:

TABLA 1. Documentación de OfficeScan

DOCUMENTACIÓN	DESCRIPCIÓN
Manual de instalación y actualización	Un documento PDF que contiene los requisitos y los procedimientos para la instalación del servidor de OfficeScan, así como para la actualización del servidor y los agentes.
Requisitos del sistema	Un documento PDF que describe los requisitos del sistema mínimos y recomendados para la instalación del servidor de OfficeScan, así como para la actualización del servidor y los agentes.
Manual del administrador	Un documento PDF que contiene información introductoria, procedimientos de instalación del Agente de OfficeScan y la administración del servidor y el agente de OfficeScan.
Ayuda	Los archivos HTML compilados en formato WebHelp o CHM que proporcionan información sobre procedimientos, consejos de uso e información específica de los campos. Se puede acceder a la Ayuda desde las consolas del servidor y los agentes de OfficeScan, así como desde la instalación maestra de OfficeScan.
Archivo Léame	contiene una lista de los problemas conocidos y los pasos básicos para la instalación. También puede contener la información más reciente del producto, no disponible en la Ayuda o en la documentación impresa.
Base de conocimientos	Una base de datos en línea que contiene información para solucionar problemas. Incluye la información más reciente acerca de los problemas conocidos de los productos. Para acceder a la base de conocimientos, vaya al siguiente sitio Web: http://esupport.trendmicro.com

Puede descargar la versión más recientes de los documentos PDF y el archivo Léame desde:

http://docs.trendmicro.com/es-es/enterprise/officescan.aspx

Audiencia

Los destinatarios de la documentación de OfficeScan son:

- Administradores de OfficeScan: responsables de la administración de OfficeScan, incluidas la instalación y la administración de los servidores y los agentes de OfficeScan. . Se presupone que estos usuarios cuentan con conocimientos avanzados sobre administración de redes y de servidores.
- Usuarios finales: usuarios que tienen instalado el Agente de OfficeScan en los endpoints. El nivel de destreza de endpoint de estos usuarios va desde el inicial hasta el avanzado.

Convenciones del documento

Este documento utiliza las siguientes convenciones:

TABLA 2. Convenciones del documento

CONVENCIÓN	DESCRIPCIÓN
MAYÚSCULAS	Acrónimos, abreviaciones y nombres de determinados comandos y teclas del teclado
Negrita	Menús y comandos de menú, botones de comandos, pestañas y opciones
Cursiva	Referencias a otros documentos
`Monoespacio`	Líneas de comandos de ejemplo, código de programa, direcciones URL, nombres de archivos y mensajes del programa.
Navegación > **Ruta**	La ruta de navegación a una determinada pantalla. Por ejemplo, **Archivo** > **Guardar** significa hacer clic en **Archivo** y, a continuación, en **Guardar** en la interfaz.
Nota	Notas sobre la configuración

CONVENCIÓN	DESCRIPCIÓN
Consejo	Recomendaciones o sugerencias
Importante	Información relativa a configuración requerida o predeterminada y limitaciones del producto
¡ADVERTENCIA!	Acciones críticas y opciones de configuración

Terminología

En la siguiente tabla se muestra la terminología oficial que se utiliza en la documentación de OfficeScan:

TABLA 3. Terminología de OfficeScan

TERMINOLOGÍA	DESCRIPCIÓN
Agente de OfficeScan	El programa del agente de OfficeScan.
Agente endpoint	El endpoint en el que está instalado el Agente de OfficeScan.
Usuario del agente (o usuario)	La persona que administra el Agente de OfficeScan en el endpoint del agente.
Servidor	El programa servidor de OfficeScan.
Equipo servidor	El endpoint en el que está instalado el servidor de OfficeScan.
Administrador (o administrador de OfficeScan)	La persona que administra el servidor de OfficeScan.

TERMINOLOGÍA	DESCRIPCIÓN
Consola	La interfaz de usuario en la que se configura y se administra el servidor de OfficeScan y la configuración del agente. La consola del programa del servidor de OfficeScan se denomina "consola Web", mientras que la del programa del Agente de OfficeScan se denomina "consola del agente".
Riesgo de seguridad	Término global referido a virus/malware, spyware/grayware y amenazas Web.
Servicio de licencias	Incluye antivirus, Damage Cleanup Services, reputación Web y antispywarelos, los cuales se activan durante el proceso de instalación del servidor de OfficeScan.
Servicio de OfficeScan	Servicios alojados por Microsoft Management Console (MMC). Por ejemplo, `ofcservice.exe`, el servicio maestro de OfficeScan.
Programa	Incluye el Agente de OfficeScan y Plug-in Manager.
Componentes	Responsables de explorar, detectar y tomar las medidas oportunas frente a los riesgos de seguridad.

`Carpeta de instalación del agente`	La carpeta del endpoint que contiene los archivos del Agente de OfficeScan. Si acepta la configuración predeterminada durante la instalación, puede encontrar la carpeta de instalación en cualquiera de las siguientes ubicaciones:
	
	`C:\Archivos de programa\Trend Micro\OfficeScan Client`
	
	`C:\Program Files (x86)\Trend Micro\OfficeScan Client`

TERMINOLOGÍA	DESCRIPCIÓN

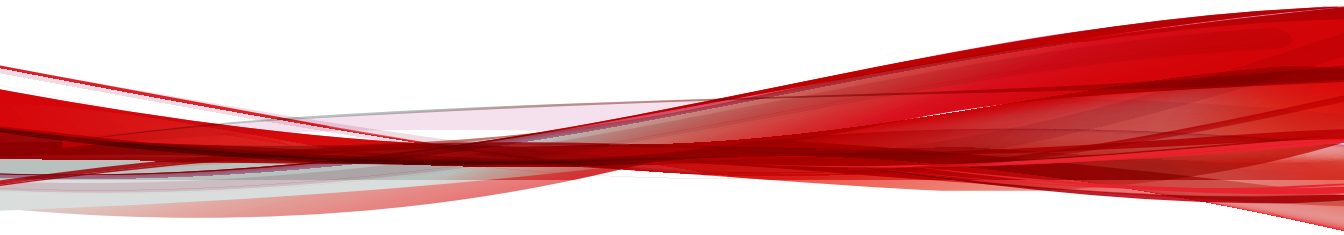
`Carpeta de instalación del servidor`	La carpeta del endpoint que contiene los archivos del servidor de OfficeScan. Si acepta la configuración predeterminada durante la instalación, puede encontrar la carpeta de instalación en cualquiera de las siguientes ubicaciones:
	`C:\Archivos de programa\Trend Micro\OfficeScan`
	`C:\Program Files (x86)\Trend Micro\OfficeScan`
	Por ejemplo, si un archivo se encuentra en la carpeta `\PCCSRV` dentro de la carpeta de instalación del servidor, la ruta completa del archivo es:
	`C:\Archivos de programa\Trend Micro\OfficeScan \PCCSRV\<Nombre_de_archivo>`.

Agente de Smart scan	Cualquier Agente de OfficeScan que se haya configurado para utilizar Smart Scan.
Agente de exploración convencional	Cualquier Agente de OfficeScan que se haya configurado para utilizar la exploración convencional.
Doble pila	Entidades que tienen direcciones IPv4 e IPv6. Por ejemplo: • Endpoints con direcciones IPv4 e IPv6 • Agentes de OfficeScan instalados en endpoints de doble pila • Agentes de actualización que distribuyen actualizaciones a los agentes • Un servidor proxy de doble pila, como DeleGate, puede realizar conversiones entre direcciones IPv4 e IPv6
Solo IPv4	Una entidad que solo tiene direcciones IPv4.
Solo IPv6	Una entidad que solo tiene direcciones IPv6.

TERMINOLOGÍA	DESCRIPCIÓN
Soluciones de complemento	Características nativas de OfficeScan y programas de complemento proporcionados a través de Plug-in Manager

Parte I

Introducción y cómo empezar



Capítulo 1

Presentación de OfficeScan

En este capítulo se presenta Trend Micro™ OfficeScan™ y se ofrece información general sobre sus características y funciones.

Los temas que se incluyen son:

- *Acerca de OfficeScan en la página 1-2*
- *Novedades de OfficeScan XG en la página 1-2*
- *Funciones y ventajas principales en la página 1-5*
- *El servidor de OfficeScan en la página 1-9*
- *El agente de OfficeScan en la página 1-11*
- *Integración con los productos y servicios de Trend Micro en la página 1-11*

Acerca de OfficeScan

Trend Micro™ OfficeScan™ protege las redes empresariales frente a malware, virus de red, amenazas basadas en Web, spyware y ataques de amenazas mixtas. Como solución integrada, OfficeScan consta del programa de Agente de OfficeScan que se encuentra en el endpoint y de un programa servidor que gestiona todos los agentes. El Agente de OfficeScan protege el endpoint e informa sobre su estado de seguridad al servidor. El servidor, mediante la consola de administración basada en Web, simplifica la aplicación de políticas de seguridad coordinada y la implementación de actualizaciones en todos los agentes.

OfficeScan cuenta con la tecnología de Trend Micro Smart Protection Network™, una infraestructura de clientes por Internet de última generación que proporciona una seguridad más inteligente que los planteamientos convencionales. La exclusiva tecnología en la nube y un agente más ligero reducen la dependencia en descargas de patrones convencionales y eliminan los retrasos que usualmente se asocian con las actualizaciones de los equipos de escritorio. Las ventajas para las empresas son un mayor ancho de banda de la red, una potencia de procesamiento de consumo reducido y ahorros en los costes asociados. Los usuarios obtienen acceso inmediato a la protección más reciente desde cualquier ubicación desde la que estén conectados (dentro de la red de la empresa, desde su domicilio o en movimiento).

Novedades de OfficeScan XG

Esta versión de OfficeScan incluye las siguientes funciones nuevas y mejoras.

Característica	Descripción
Mejoras en la protección de ransomware	La protección frente a ataques de ransomware se ha mejorado aún más para permitir que los Agentes de OfficeScan recuperen archivos cifrados a causa de amenazas de ransomware, bloqueen procesos asociados con ransomware y eviten que archivos ejecutables comprometidos infecten la red. Para obtener más información, consulte *Protección frente al ransomware en la página 9-3*.

Característica	Descripción
Mejora en la protección de programas recién encontrados	Para maximizar la política de seguridad de protección de ransomware en agentes individuales con mayor facilidad, la característica de detección de programas recién encontrados se ha movido a la pantalla de ajustes de la supervisión de comportamiento. Para obtener más información, consulte *Proteger frente a programas recién encontrados en la página 9-6*. También puede personalizar el mensaje que se muestra en los endpoints del agente después de que un usuario descargue y ejecute un programa recién encontrado. Para obtener más información, consulte *Modificación del contenido del mensaje de notificación en la página 9-17*.
Aprendizaje automático predictivo	El motor de aprendizaje automático predictivo puede proteger la red de amenazas nuevas, desconocidas o que no se hayan identificado con anterioridad mediante el análisis avanzado de características de archivo y la supervisión de procesos heurística. El aprendizaje automático predictivo puede determinar la probabilidad de que una amenaza exista en un archivo o un proceso, así como el tipo de amenaza probable, para protegerle de ataques de día cero.
OfficeScan Edge Relay Server	OfficeScan Edge Relay Server le ofrece una mayor visibilidad y una protección mejorada para los endpoints que abandonan la intranet local gracias a las siguientes características: • Sincronización de listas de objetos sospechosos • Envío de muestras • Envío de registros • Envío de información del estado del agente, como versiones actuales de patrones y componentes Para obtener más información, consulte *Edge Relay Server en la página 16-2*.

Característica	Descripción
Envío de muestras de archivos sospechosos	Para mejorar aún más la integración con Analizador virtual de Deep Discovery, ahora los Agentes de OfficeScan pueden detectar y enviar archivos sospechosos que puedan contener amenazas que no se conocían con anterioridad directamente a Analizador virtual para su análisis. Tras comprobar la existencia de una amenaza, las listas de objetos sospechosos se actualizan de forma inmediata y se sincronizan en todos los agentes, lo que evita que la amenaza se propague por la red. Para obtener más información, consulte *Envío de muestras en la página 8-9*.
Mejoras de la interfaz de usuario de la consola	La consola se ha rediseñado para ofrecer una mejor visibilidad del estado de protección de la red.
Mejoras de integración de Control Manager	Para evitar comunicaciones no autorizadas entre los servidores de OfficeScan y Control Manager, el registro en el servidor de Control Manager requiere autenticación de certificado y la administración de las políticas del servidor de Control Manager se gestiona mediante cifrado de clave pública. Para obtener más información, consulte *Autorización con certificado de Control Manager en la página 14-31*.
Protección frente a explotación	La exploración en tiempo real le permite detectar y bloquear amenazas mediante las explotaciones de la lista de vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE). Para obtener más información, consulte *Configuración de la exploración en la página 7-29*. La supervisión de comportamiento también puede detectar comportamiento de programas anómalo que se suele ver en ataques de explotación. Para obtener más información, consulte *Protección frente a explotación en la página 9-5*.

CARACTERÍSTICA	DESCRIPCIÓN
Mejora de las conexiones sospechosas	Ahora puede configurar la característica de conexiones sospechosas para que registre o bloquee conexiones de red detectadas por la lista IP de C&C global y las huellas de red de malware. Para obtener más información, consulte *Definir la configuración de conexión sospechosa en la página 8-7*.
Mejoras de cortafuegos	El filtro de aplicaciones del cortafuegos de OfficeScan ahora es compatible con Windows 8 y plataformas posteriores. Puede otorgar a los usuarios de los Agentes de OfficeScan derechos para configurar el nivel de seguridad del cortafuegos y la lista de excepciones. Para obtener más información, consulte *Agregar un perfil del cortafuegos en la página 13-21*.
Modo independiente	Se ha cambiado el nombre del modo «En itinerancia» por «Independiente». Para obtener más información, consulte *Estado de conexión del agente en la página 2-46*.
Plataformas y exploradores compatibles	Esta versión de OfficeScan es compatible con: • Microsoft™ Windows™ Server 2016 **Nota** Esta versión de OfficeScan ya no es compatible con el servidor Web Apache.

Funciones y ventajas principales

OfficeScan ofrece las funciones y ventajas siguientes.

TABLA 1-1. Funciones y ventajas principales

CARACTERÍSTICA	VENTAJAS
Protección de ransomware	Las características de exploración mejoradas pueden identificar y bloquear programas de ransomware cuyo objetivo son los documentos que se ejecutan en endpoints mediante la identificación de patrones de comportamiento comunes y el bloqueo de procesos asociados a este tipo de programas.
Defensa de amenazas conectada	Configure OfficeScan para suscribirse a las listas de objetos sospechosos desde el servidor de Control Manager. Mediante la consola de Control Manager se pueden crear acciones personalizadas para los objetos que detecten las listas de objetos sospechosos. De este modo, se podrá proporcionar una estrategia de defensa personalizada frente a las amenazas que identifiquen los endpoints protegidos por los productos de Trend Micro específicos del entorno. Puede configurar los agentes de OfficeScan para que envíen objetos de archivo que puedan contener amenazas que no se hayan identificado con anterioridad a Analizador virtual para su análisis. Tras evaluar los objetos, Analizador virtual añadirá aquellos que contengan amenazas desconocidas a las listas de objetos sospechosos de Analizador virtual y las distribuirá a los demás agentes de OfficeScan de la red.
Plug-in Manager y soluciones de complemento	Plug-in Manager facilita la instalación, implementación y administración de las soluciones de complemento. Los administradores pueden instalar dos tipos de solución de complemento: • Programas de complemento • Características nativas de OfficeScan

Característica	Ventajas
Administración centralizada	Una consola de administración basada en Web permite a los administradores acceder a todos los agentes y servidores de la red con facilidad. La consola Web coordina la implementación automática de políticas de seguridad, archivos de patrones y actualizaciones de software en cada agente y servidor. Junto con los servicios de prevención de epidemias, la consola Web desconecta los vectores de infección y rápidamente implementa políticas de seguridad específicas para cada ataque con el fin de prevenir o contener epidemias antes de que los archivos de patrones estén disponibles. OfficeScan también realiza una supervisión en tiempo real, envía notificaciones de sucesos y crea informes detallados. Los administradores pueden realizar una administración remota, definir políticas personalizadas para equipos de escritorio o grupos específicos, así como bloquear la configuración de seguridad del agente.
Protección frente a riesgos de seguridad	OfficeScan protege los equipos frente a los riesgos de seguridad mediante la exploración de archivos y, a continuación, lleva a cabo una acción específica por cada riesgo de seguridad detectado. La detección de un número desbordante de riesgos de seguridad en un corto período de tiempo es señal de epidemia. Para contener las epidemias, OfficeScan aplica políticas de prevención de epidemias y aísla los equipos infectados hasta que se encuentran completamente fuera de peligro. OfficeScan utiliza la exploración inteligente para que el proceso de exploración sea más eficaz. Esta tecnología redirecciona un gran número de firmas, previamente almacenadas en el endpoint local, a orígenes de Smart Protection. Al utilizar este enfoque, se reduce considerablemente el impacto en el sistema y en la red del siempre creciente volumen de actualizaciones de firmas a sistemas de endpoint. Para obtener más información sobre Smart Scan y su implementación en los agentes, consulte *Tipos de métodos de exploración en la página 7-9*.

Característica	Ventajas
Damage Cleanup Services	Damage Cleanup Services™ limpia los equipos de virus basados en archivos y de red, además de restos de virus y gusanos (troyanos, entradas del registro, archivos víricos) mediante un proceso totalmente automatizado. Para hacer frente a las amenazas y problemas que causan los troyanos, Damage Cleanup Services lleva a cabo las acciones siguientes: • Detecta y elimina troyanos activos. • Elimina los procesos creados por los troyanos. • Repara los archivos del sistema modificados por los troyanos. • Elimina los archivos y aplicaciones depositados por los troyanos. Como Damage Cleanup Services se ejecuta automáticamente en segundo plano, no es necesario configurarlo. Los usuarios no perciben la ejecución del programa. No obstante, es posible que, de vez en cuando, OfficeScan solicite que el usuario reinicie el endpoint para completar el proceso de eliminación de un troyano.
Reputación Web	La tecnología de reputación Web protege los equipos de los agentes de forma proactiva, tanto dentro como fuera de la red empresarial, frente a ataques de sitios Web malintencionados y potencialmente peligrosos. La reputación Web rompe la cadena de infección e impide la descarga de código malicioso. Verifique la credibilidad de los sitios y páginas Web integrando OfficeScan con Smart Protection Server o Trend Micro Smart Protection Network.
Cortafuegos de OfficeScan	El cortafuegos de OfficeScan protege a los agentes y los servidores de la red mediante inspecciones de estado y exploraciones de virus de red de alto rendimiento. Cree reglas para filtrar las conexiones por aplicación, dirección IP, número de puerto o protocolo, y aplicarlas a continuación a diferentes grupos de usuarios.

CARACTERÍSTICA	VENTAJAS
Prevención de pérdida de datos	El servicio de prevención de pérdida de datos protege los activos digitales de la organización frente a fugas accidentales o intencionadas. La prevención de pérdida de datos permite a los administradores: • Identificar los activos digitales que se deben proteger • Crear políticas que limiten o prevengan la transmisión de activos digitales a través de los medios más habituales, como los dispositivos de correo electrónico y los dispositivos de almacenamiento externo • Aplicar la conformidad a estándares de privacidad establecidos
Control de dispositivos	Control de dispositivos regula el acceso a los dispositivos de almacenamiento externo y a los recursos de red conectados a los equipos. El control de dispositivos ayuda a evitar la pérdida y la fuga de datos y, junto con la exploración de archivos, ayuda a protegerse frente a los riesgos de seguridad.
Supervisión del comportamiento	El componente de supervisión de comportamiento controla constantemente los agentes en busca de modificaciones inusuales en el sistema operativo o el software que se ha instalado.

El servidor de OfficeScan

El servidor de OfficeScan es el repositorio central de todas las configuraciones de agentes, los registros de riesgos de seguridad y las actualizaciones.

El servidor lleva a cabo dos funciones importantes:

- Instala, supervisa y gestiona los Agentes de OfficeScan.
- Descarga muchos de los componentes que necesitan los agentes. El servidor de OfficeScan descarga componentes desde Trend Micro ActiveUpdate Server y los distribuye a los agentes.

Nota

Algunos componentes los descargan las fuentes de Smart Protection. Consulte *Fuentes de Smart Protection en la página 4-6* para obtener más información.

FIGURA 1-1. Funcionamiento del servidor de OfficeScan

El servidor de OfficeScan es capaz de ofrecer comunicación bidireccional en tiempo real entre el servidor y los Agentes de OfficeScan. Gestiona los agentes desde una consola Web basada en explorador, a la que los administradores pueden acceder desde casi cualquier punto de la red. El servidor se comunica con el agente (y el agente con el servidor) mediante el protocolo de transferencia de hipertexto (HTTP).

El agente de OfficeScan

Proteja los equipos Windows de los riesgos de seguridad mediante la instalación del Agente de OfficeScan en cada endpoint.

El Agente de OfficeScan informa al servidor principal desde el que se haya instalado. Configure los agentes para que envíen informes a otro servidor mediante la herramienta Agent Mover. El agente envía sucesos e información de estado al servidor en tiempo real. Algunos ejemplos de sucesos pueden ser la detección de virus/malware, el inicio del agente, la desconexión del agente, el inicio de una exploración o la finalización de una actualización.

Integración con los productos y servicios de Trend Micro

OfficeScan se integra con los productos y servicios de Trend Micro que aparecen en la siguiente tabla. Para conseguir una integración perfecta, asegúrese de que los productos ejecuten las versiones necesarias o recomendadas.

TABLA 1-2. Productos y servicios que se integran con OfficeScan

PRODUCTO/ SERVICIO	DESCRIPCIÓN	VERSIÓN
Servidor ActiveUpdate	Proporciona todos los componentes que el Agente de OfficeScan necesita para proteger los endpoints frente a amenazas de seguridad.	No aplicable
Smart Protection Network	Proporciona servicios de File Reputation y servicios de reputación Web a los agentes. Trend Micro aloja la Red de Smart Protection.	No aplicable

PRODUCTO/ SERVICIO	DESCRIPCIÓN	VERSIÓN
Smart Protection Server Independiente	Proporciona los mismos Servicios de Reputación de Ficheros y Servicios de Reputación Web que la Red de Smart Protection. Un Smart Protection Server independiente tiene como función localizar el servicio en la red de empresa a fin de optimizar la eficacia. **Nota** Se instala un Smart Protection Server Integrado con el servidor de OfficeScan. Tiene las mismas funciones que la versión independiente, pero cuenta con capacidad limitada.	• 3.0
Control Manager	Una solución de administración de software que proporciona la capacidad de controlar los programas antivirus y de seguridad de contenidos desde una ubicación central, independientemente de la plataforma o ubicación física de dichos programas.	• 6.0 SP3 revisión 2 (recomendado) • 6.0 SP3 • 6.0 SP2 • 6.0 SP1
Deep Discovery Analyzer	Deep Discovery ofrece supervisión en toda la red con tecnología de espacios aislados personalizados e inteligencia en tiempo real para permitir la detección precoz de ataques, permitir la relación de contenido rápido y ofrecer actualizaciones de seguridad personalizadas que mejoren de forma inmediata la protección frente a futuros ataques.	5.1 y posterior

Capítulo 2

Introducción a OfficeScan

En este capítulo se ofrece una introducción de OfficeScan y se describe su configuración inicial.

Los temas que se incluyen son:

- *La consola Web en la página 2-2*
- *El Panel en la página 2-5*
- *Server Migration Tool en la página 2-37*
- *Integración con Active Directory en la página 2-42*
- *Árbol de agentes de OfficeScan en la página 2-45*
- *Dominios de OfficeScan en la página 2-61*

La consola Web

La consola Web es el punto central para supervisar OfficeScan a través de la red empresarial. La consola incluye un conjunto de valores y parámetros de configuración predeterminados que pueden configurarse en función de los requisitos y especificaciones de seguridad de la empresa. La consola Web utiliza las tecnologías de Internet estándar, como JavaScript, CGI, HTML y HTTPS.

Nota

Defina la configuración de tiempo de espera desde la consola Web. Consulte el apartado *Configuración de la Consola Web en la página 14-64*.

Use la consola Web para realizar las acciones siguientes:

- Administrar agentes que se han instalado en equipos en red.
- Agrupar agentes en dominios lógicos para realizar una configuración y administración simultáneas.
- Definir configuraciones de exploración e iniciar la exploración manual en uno o varios equipos conectados en red
- Configurar notificaciones sobre riesgos de seguridad en la red y ver los registros que envían los agentes.
- Configurar criterios y notificaciones de epidemia
- Delegar tareas de administración de la consola Web en otros administradores de OfficeScan mediante la configuración de funciones y cuentas de usuario.
- Garantizar que los agentes cumplen las directrices de seguridad.

Nota

La consola Web no admite Windows 8, 8.1, 10 ni Windows Server 2012 en el modo de interfaz de usuario de Windows.

Requisitos para abrir la consola Web

Abra la consola Web desde cualquier endpoint de la red que disponga de los siguientes recursos:

- Procesador Intel™ Pentium™ a 300MHz o equivalente
- 128MB de memoria RAM
- Al menos 30 MB de espacio disponible en disco
- Monitor con una resolución de 1366 x 768 de 256 colores o superior
- Compatibilidad del explorador Web:
  - Microsoft Internet Explorer™ 10.0 o posterior
  - Microsoft Edge
  - Chrome

Nota

OfficeScan solo es compatible con tráfico HTTPS cuando se visualiza la consola Web.

En el explorador Web, escriba una de las opciones siguientes en la barra de direcciones según el tipo de instalación de servidor de OfficeScan:

TABLA 2-1. URL de la consola OfficeScan Web

TIPO DE INSTALACIÓN	URL
Con SSL en un sitio predeterminado	`https://<FQDN o dirección IP del servidor de OfficeScan>/OfficeScan`
Con SSL en un sitio virtual	`https://<FQDN o dirección IP del servidor de OfficeScan>:<número de puerto>/OfficeScan`

Nota

Si ha realizado una actualización desde una versión anterior de OfficeScan, es posible que los archivos de caché del explorador de Internet y el servidor proxy impidan que se cargue correctamente la consola Web de OfficeScan. Libere la memoria caché del explorador y de los servidores proxy ubicados entre el servidor de OfficeScan y el endpoint que utiliza para permitir el acceso a la consola Web.

Cuenta de inicio de sesión

Durante la instalación del servidor de OfficeScan se crea una cuenta raíz y se le solicita que introduzca una contraseña para dicha cuenta. Cuando abra la consola Web por primera vez, escriba "raíz" como nombre de usuario e introduzca la contraseña de la cuenta raíz. Si olvida la contraseña, póngase en contacto con su proveedor de servicios para que le ayude a restablecerla.

Defina las funciones de usuario y configure las cuentas de usuario para permitir a otros usuarios acceder a la consola Web sin utilizar la cuenta raíz. Cuando los usuarios inicien sesión en la consola, podrán utilizar las cuentas de usuario que ha configurado para ellos. Para obtener más información, consulte *Role-based Administration en la página 14-3*.

El banner de la consola Web

La zona de banner de la consola Web ofrece las siguientes opciones:

FIGURA 2-1. Zona de banner de la consola Web

- **<nombre de la cuenta>**: Haga clic en el nombre de la cuenta (por ejemplo, raíz) para modificar los detalles de la cuenta, como la contraseña.
- **Cerrar sesión**: le desconecta de la consola Web.

Obtener ayuda

El menú **Ayuda** permite acceder a la siguiente información de asistencia:

- **Contenido e índice**: abre la ayuda en línea.
- **Novedades**: muestras algunas características clave nuevas de la versión.
- **Soporte**: muestra la página Web de Trend Micro Support, en la que puede plantear preguntas y obtener respuesta a preguntas frecuentes sobre los productos de Trend Micro.
- **Enciclopedia de amenazas**: muestra el sitio Web de la enciclopedia de amenazas, que es el repositorio de información sobre malware de Trend Micro. Los expertos en amenazas de Trend Micro publican regularmente detecciones de malware, spam, URL maliciosas y vulnerabilidades. La enciclopedia de amenazas también explica ataques a páginas Web destacadas y proporciona información relacionada.
- **Ponerse en contacto con Trend Micro**: muestra el sitio Web Trend Micro **Contacto** que contiene información sobre nuestras oficinas en todo el mundo.
- **Acerca de**: Proporciona un resumen del producto, instrucciones para comprobar detalles sobre la versión del componente y un enlace al Sistema de inteligencia de compatibilidad.

  Para conocer más detalles, consulte *Soporte de sistema de inteligencia en la página 18-2*.

El Panel

El **Panel** aparece cada vez que se abre la consola Web de OfficeScan o hace clic en **Panel** en el menú principal.

Cada cuenta de usuario de la consola Web cuenta con un panel completamente independiente. Los cambios realizados en el panel de una cuenta de usuario no afectan a los paneles de las otras cuentas de usuario.

Si una consola contiene datos de agente de OfficeScan, los datos se mostrarán en función de los permisos del dominio del agente para la cuenta de usuario. Por ejemplo, si concede permisos a una cuenta de usuario para que administre los dominios A y B, la

consola de la cuenta de usuario solo mostrará datos de aquellos agentes que pertenezcan a los dominios A y B.

Para obtener información detallada acerca de las cuentas de usuario, consulte *Role-based Administration en la página 14-3*.

La pantalla **Panel** contiene lo siguiente:

- Sección Estado de las licencias de los productos
- Componentes
- Pestañas

Sección Estado de las licencias de los productos

Esta sección se encuentra en la parte superior del panel y muestra el estado de las licencias de OfficeScan.

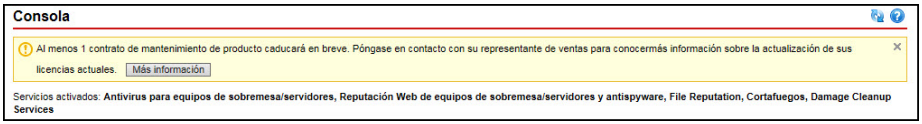


FIGURA 2-2. Sección Estado de las licencias de los productos

Durante los casos siguientes aparecen recordatorios sobre el estado de las licencias:

- Si cuenta con una licencia de versión completa:
  - 60 días antes de que caduque una licencia.
  - Durante el periodo de gracia del producto. La duración del periodo de gracia puede varía entre una zona y otra. Consulte con su representante de Trend Micro para comprobar la duración de su periodo de gracia.
  - Cuando la licencia caduca y finaliza el periodo de gracia. Durante este tiempo no podrá obtener asistencia técnica ni actualizar componentes. Los motores de exploración seguirán explorando los equipos con componentes obsoletos. Es posible que estos componentes obsoletos no puedan protegerle completamente frente a los riesgos de seguridad más recientes.

- Si cuenta con una licencia de versión de evaluación:
  - 14 días antes de que caduque una licencia.
  - Cuando caduca la licencia. Durante este tiempo, OfficeScan desactiva las actualizaciones de componentes, la exploración y todas las funciones del agente.

Si ha obtenido un código de activación, renueve la licencia en **Administración** > **Configuración** > **Licencia del producto**.

Barras de información del producto

OfficeScan muestra una serie de mensajes en la parte superior de la pantalla **Panel** que proporcionan información adicional a los administradores.

La información que se muestra incluye:

- Los últimos Service Pack o revisiones disponibles para OfficeScan.

  Nota

  Haga clic en **Más información** para descargar la revisión del Centro de descarga de Trend Micro (http://downloadcenter.trendmicro.com/index.php?regs=ES).

- Nuevos componentes disponibles.
- Notificaciones sobre el contrato de mantenimiento cuando este está a punto de caducar.
- Notificaciones sobre el modo de valoración.
- Notificaciones sobre autenticidad.

  Nota

  Si la licencia de OfficeScan no es original, se mostrará un mensaje informativo. Si no obtiene una licencia original, OfficeScan mostrará una advertencia y dejará de realizar actualizaciones.

Pestañas y componentes

Los componentes son el elemento principal del panel. Los componentes proporcionan información específica acerca de distintos eventos relacionados con la seguridad. Algunos componentes permiten realizar ciertas tareas como la actualización de elementos.

La información que muestran los componentes proviene de:

- El servidor y los agentes de OfficeScan
- Las soluciones de complemento y sus agentes
- Trend Micro Smart Protection Network

Nota

Active el Smart Feedback para mostrar los datos desde la Red de Smart Protection. Para obtener información detallada acerca del Smart Feedback, consulte *Smart Feedback en la página 14-69*.

Las pestañas constituyen un área para los componentes. El **Panel** puede contener hasta 30 pestañas.

Trabajar con las pestañas

Administre las pestañas con acciones de adición, cambio de nombre, cambio de diseño, eliminación y cambio automático de vistas de pestaña.

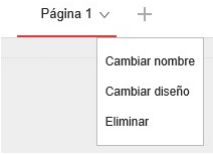
Procedimiento

1. Vaya **Panel**.
2. Para agregar una nueva pestaña:
   a. Haga clic en el icono de adición.

b. Escriba un nombre para la nueva pestaña.

3. Para cambiar el nombre de una pestaña:

a. Sitúe el puntero del ratón sobre el nombre de la pestaña y haga clic en la flecha hacia abajo.



b. Haga clic en **Cambiar nombre** y escriba el nuevo nombre de la pestaña.

4. Para cambiar el diseño de los componentes de una pestaña:

a. Sitúe el puntero del ratón sobre el nombre de la pestaña y haga clic en la flecha hacia abajo.

b. Haga clic en **Cambiar diseño**.

c. Seleccione el nuevo diseño en la pantalla que aparecerá.

d. Haga clic en **Guardar**.

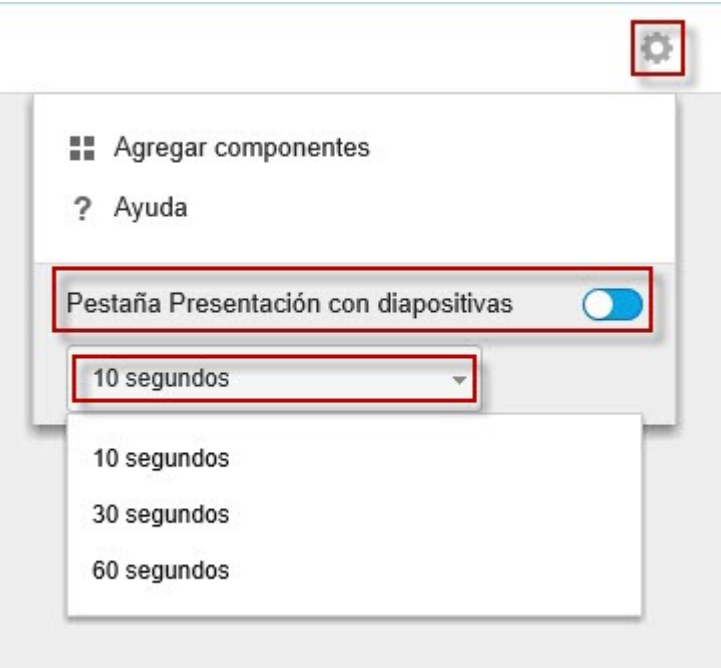
5. Para eliminar una pestaña:

a. Sitúe el puntero del ratón sobre el nombre de la pestaña y haga clic en la flecha hacia abajo.

b. Haga clic en **Eliminar** y, a continuación, confirme la acción.

6. Para reproducir una presentación con diapositivas de pestañas:

a. Haga clic en el botón **Configuración** a la derecha de la visualización de pestañas.



b. Active el control **Presentación con diapositivas de pestañas**.

c. Seleccione el tiempo que se mostrará cada pestaña antes de pasar a la siguiente.

Trabajar con los componentes

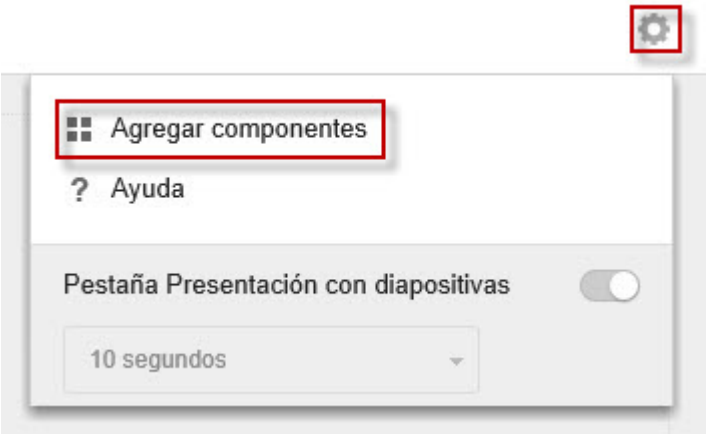
Administre los componentes con acciones de adición, transferencia, cambio de tamaño, cambio de nombre y eliminación de elementos.

Procedimiento

1. Vaya **Panel**.
2. Haga clic en una pestaña.

3. Para agregar un componente:

   a. Haga clic en el botón **Configuración** a la derecha de la visualización de pestañas.



   b. Haga clic en **Agregar componentes**.

   c. Seleccione los componentes que desea agregar.

      - En el menú desplegable en la parte superior de los componentes, seleccione una categoría para limitar las selecciones.
      - Utilice el cuadro de texto de búsqueda de la parte superior de la pantalla para buscar un componente concreto.

   d. Haga clic en **Agregar**.

4. Para mover un componente a una nueva ubicación de la misma pestaña, arrastre y coloque el componente en la nueva ubicación.

5. Cambie el tamaño de un componente de una pestaña con varias columnas colocando el cursor en el extremo derecho del componente y moviéndolo hacia la izquierda o hacia la derecha.

6. Para cambiar el nombre de un componente:

a. Haga clic en el icono de configuración (>).

b. Escriba el nuevo título.

Nota

En el caso de algunos componentes, como **OfficeScan y Plug-ins Mashup**, se pueden modificar los elementos relacionados con los componentes.

c. Haga clic en **Guardar**.

7. Para eliminar un componente, haga clic en el icono de eliminación (>).

Componentes de la pestaña Resumen

La pestaña **Resumen** ofrece un resumen del estado de seguridad de todos los Agentes de OfficeScan en la red.

Nota

Los componentes que aparecen en la pestaña **Resumen** no se pueden eliminar ni modificar, y tampoco es posible añadir componentes.

Componentes disponibles:

- *Componente de detecciones de amenazas e infracciones de políticas generales en la página 2-13*
- *Componente de estado del endpoint en la página 2-14*
- *Componente de detecciones de riesgos de seguridad en un periodo de tiempo en la página 2-20*

Componente de detecciones de amenazas e infracciones de políticas generales

Este componente proporciona información general de todas las detecciones de amenazas y de las infracciones de políticas de la red en las últimas 24 horas.

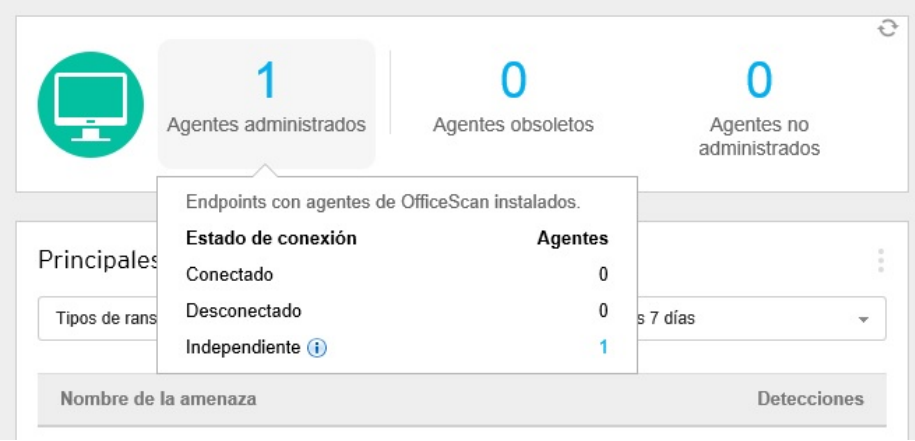
Sitúe el puntero del ratón sobre el recuento de amenazas o infracciones para ver un desglose de los tipos específicos de detecciones que se han producido para cada grupo. Para ver los registros de una característica concreta, haga clic en el recuento de la derecha.

TABLA 2-2. Categorías de detección

CATEGORÍA	DESCRIPCIÓN
Amenazas conocidas	Muestra todas las características que detectan amenazas de seguridad confirmadas por Trend Micro. • Virus/Malware • Spyware/Grayware • Reputación Web

CATEGORÍA	DESCRIPCIÓN
Amenazas desconocidas	Muestra todas las características que detectan amenazas potenciales mediante heurística avanzada, análisis o modelos de características. • Aprendizaje automático predictivo • Supervisión del comportamiento • Conexiones sospechosas • Objetos de archivos sospechosos
Infracciones de políticas	Muestra todas las características que contienen infracciones de políticas específicas de sus estándares de seguridad empresariales. • Cortafuegos • Control de dispositivos • Prevención de pérdida de datos

Componente de estado del endpoint



Este componente proporciona información general del estado de conexión y de actualización de los Agentes de OfficeScan en la red, así como del recuento de

cumplimiento de seguridad más reciente de endpoints no administrados que no informan al servidor de OfficeScan.

Sitúe el puntero del ratón sobre un recuento para ver el desglose de los diferentes estados. Para ver los registros de un estado concreto, haga clic en el recuento de la derecha.

TABLA 2-3. Grupos de agentes/endpoints

GRUPO	DESCRIPCIÓN
Agentes administrados	Muestra el último estado de conexión transmitido de los Agentes de OfficeScan de la red. • Conectado • Desconectado • Independiente
Agentes obsoletos	Muestra una lista de categorías de componente y el recuento de los Agentes de OfficeScan con un componente obsoleto en cada categoría.
Endpoints no administrados	Muestra una lista de todos los endpoints que OfficeScan puede detectar, pero que no tienen el programa del Agente de OfficeScan instalado o que no informan al servidor de OfficeScan. **Nota** Para asegurarse de que el servidor de OfficeScan actualice el recuento de endpoints no administrados con frecuencia: 1. Defina el alcance de Active Directory/dirección IP de una valoración. Para obtener más información, consulte *Integración con Active Directory en la página 2-42*. 2. Configure una valoración programada. Para obtener más información, consulte *Conformidad con las normas de seguridad para Endpoints no administrados en la página 15-76*.

Componente de resumen de ransomware

FIGURA 2-3. Una vista predeterminada que muestra todos los datos de ransomware y una vista ampliada del gráfico de barras "Intentos de ransomware detectados".

Este widget ofrece un resumen de todos los ataques de ransomware perpetrados en un intervalo de tiempo específico.

La vista predeterminada muestra un resumen de todas las detecciones de ransomware y aplica categorías más específicas a los intentos en función del canal de infección.

- Haga clic en el recuento de detecciones de ransomware de la vista predeterminada para abrir la pantalla de registros **Riesgos de seguridad: ransomware** que incluye los detalles de detecciones de ransomware.

Haga clic en cualquiera de los gráficos a la derecha del componente para mostrar una vista ampliada de los datos del gráfico.

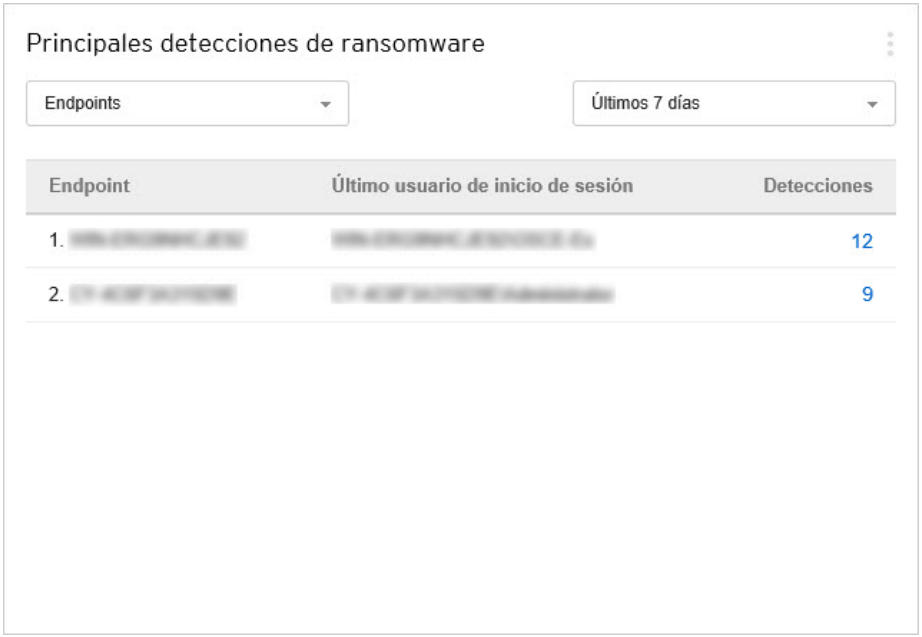
- Sitúe el puntero del ratón sobre los nodos de cualquiera de los días para ver la cantidad total de detecciones de la categoría de detección mostrada. Haga clic en un nodo para volver a la pantalla de registros **Riesgos de seguridad: ransomware**, que incluye los detalles de detección de ransomware de ese día concreto.

TABLA 2-4. Canales de detección de ransomware

CANAL	DESCRIPCIÓN	DETECTADO POR
Web	Archivos descargados mediante un cliente Web (por ejemplo, un explorador o un cliente FTP)	• Reputación Web • Exploración en tiempo real • Supervisión del comportamiento
Tráfico de red	Ransomware detectado por la característica de conexiones sospechosas	• Conexiones sospechosas
Correo electrónico	Archivos adjuntos de correo electrónico abiertos con Microsoft Outlook o Windows Live Mail **Nota** OfficeScan clasifica todos los archivos adjuntos abiertos con otras aplicaciones cliente de correo electrónico en el canal **Disco local o de red**.	• Exploración en tiempo real • Supervisión del comportamiento
Archivos de AutoRun	Programas ubicados en unidades de almacenamiento extraíbles y ejecutados por archivos de ejecución automática **Nota** OfficeScan clasifica los demás archivos o programas que no haya ejecutado el programa de ejecución automática en dispositivos de almacenamiento extraíble en el canal **Disco local o de red**.	• Exploración en tiempo real • Supervisión del comportamiento

CANAL	DESCRIPCIÓN	DETECTADO POR
Disco local o de red	Ransomware detectado en unidades locales o de red, incluidos: • Archivos adjuntos de correo electrónico abiertos con clientes de correo electrónico que no sean Microsoft Outlook o Windows Live Mail • Archivos en dispositivos de almacenamiento extraíble que el programa de ejecución automática no haya ejecutado	• Exploración en tiempo real • Exploración manual • Exploración programada • Explorar ahora • Supervisión del comportamiento

Componente de principales detecciones de ransomware

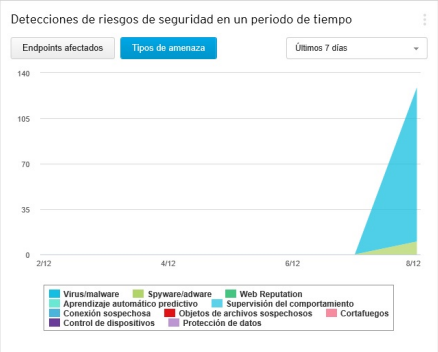


Este widget ofrece un resumen de las principales detecciones de ransomware en un intervalo de tiempo específico.

Use el menú desplegable para seleccionar el tipo de datos de ransomware que se mostrará.

MOSTRAR	DESCRIPCIÓN
Endpoints	Muestra los endpoints con el mayor número de detecciones de ransomware de la red. Haga clic en el recuento de detecciones de ransomware para abrir la pantalla de registros **Riesgos de seguridad: ransomware** que incluye los detalles de detecciones de ransomware.
Tipos de ransomware	Muestra los tipos de ransomware con el mayor número de detecciones de la red. Haga clic en el enlace **Nombre de la amenaza** para abrir la enciclopedia de amenazas de Trend Micro a fin de obtener más información sobre el tipo de amenaza específico.
Dominios	Muestra los dominios de ransomware con el mayor número de detecciones de la red. Haga clic en el enlace **Nombre de la amenaza** para abrir la enciclopedia de amenazas de Trend Micro a fin de obtener más información sobre el dominio específico.

Componente de detecciones de riesgos de seguridad en un periodo de tiempo



Este widget proporciona un resumen de los endpoints en la red con las detecciones de amenazas y los tipos de amenazas que afectan a su red en un intervalo de tiempo determinado.

Haga clic en los botones **Endpoints afectados** o **Tipos de amenaza** para cambiar las vistas.

MOSTRAR	DESCRIPCIÓN
Endpoints afectados	Muestra el recuento de endpoints con detecciones de amenazas o infracciones de políticas para un intervalo de tiempo determinado. Haga clic en el nodo de un día concreto para ir a la pantalla **Administración de agentes**, donde se muestran los endpoints afectados de ese día en el árbol de agentes.

MOSTRAR	DESCRIPCIÓN
Tipos de amenaza	Muestra un gráfico que expone la cantidad de amenazas y de infracciones de políticas registradas en un intervalo de tiempo concreto. • Haga clic en los nombres de los tipos de amenaza de la parte inferior del gráfico para mostrar u ocultar la información de detección en el mismo. • Sitúe el puntero del ratón sobre los nodos de cualquiera de los días para ver la cantidad total de detecciones de los tipos de amenaza mostrados. Haga clic en un nodo para ir a la pantalla de registros del tipo de amenaza resaltado en la lista.

Consejo

Puede agregar este componente varias veces para mostrar ambas vistas. Encontrará el componente en el tipo de componente **OfficeScan** cuando agregue componentes a otras pestañas.

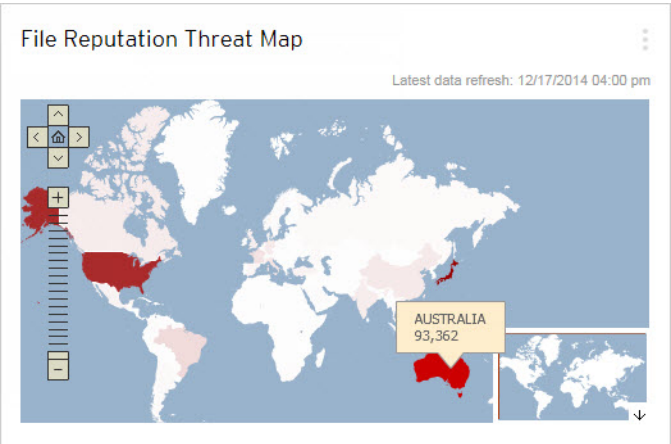
Componentes de Smart Protection Network

OfficeScan incluye una pestaña predeterminada que contiene información de Trend Micro Smart Protection Network, que proporciona servicios de File Reputation y Web Reputation a los Agentes de OfficeScan.

Componentes disponibles:

- *Componente Fuentes de amenazas más destacadas de Web Reputation en la página 2-24*
- *Componente Usuarios amenazados más destacados de Web Reputation en la página 2-23*
- *Componente de Complemento de mapa de amenazas de reputación de archivo en la página 2-22*

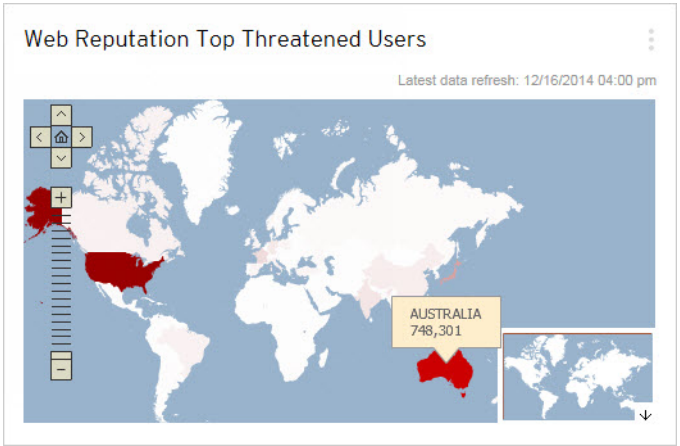
Componente de Complemento de mapa de amenazas de reputación de archivo



Este componente muestra el número total de detecciones de amenazas de seguridad realizadas por los Servicios de Reputación de Ficheros. La información se muestra en un mapa mundial por ubicación geográfica.

Coloque el puntero del ratón sobre las diferentes regiones del mapa para ver el número total de detecciones de amenazas a la seguridad de cada región.

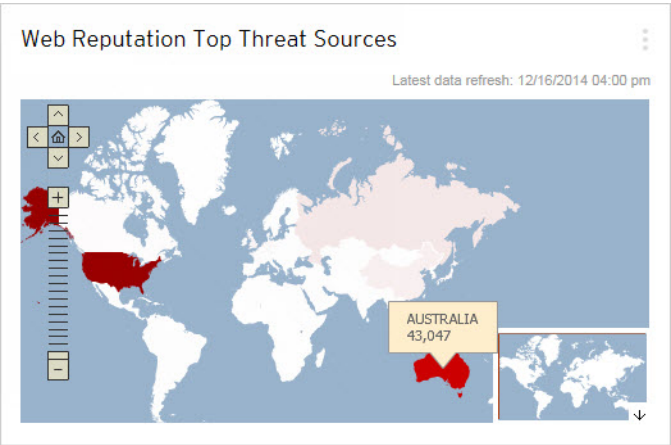
Componente Usuarios amenazados más destacados de Web Reputation



Este componente muestra el número de usuarios afectados por las URL maliciosas detectadas por los Servicios de Reputación Web. La información se muestra en un mapa mundial por ubicación geográfica.

Coloque el puntero del ratón sobre las diferentes partes del mapa para ver el número total de usuarios afectados de cada región.

Componente Fuentes de amenazas más destacadas de Web Reputation



Este componente muestra el número total de detecciones de amenazas de seguridad realizadas por los Servicios de Reputación web. La información se muestra en un mapa mundial por ubicación geográfica.

Coloque el puntero del ratón sobre las diferentes regiones del mapa para ver el número total de detecciones de amenazas a la seguridad de cada región.

Componentes de protección de datos

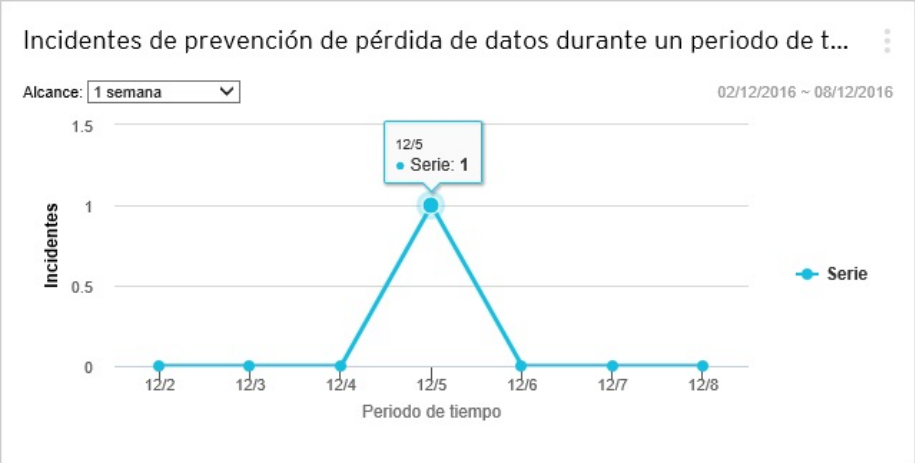
Nota

Los componentes de protección de datos estarán disponibles tras la activación de la protección de datos de OfficeScan.

Componentes disponibles:

- *Componente Incidentes de prevención de pérdida de datos durante un periodo de tiempo en la página 2-25*
- *Componente Incidentes principales de prevención de pérdida de datos en la página 2-26*

Componente Incidentes de prevención de pérdida de datos durante un periodo de tiempo

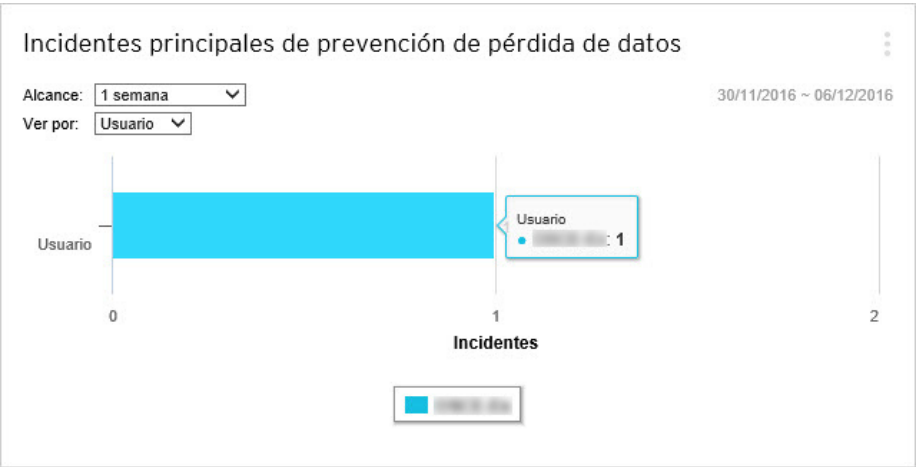


Este componente muestra la cantidad total de incidentes de prevención de pérdida de datos durante un periodo de tiempo concreto.

Nota

Las detecciones incluyen todos los incidentes de la prevención de pérdida de datos, sin importar la acción que se haya realizado («Bloquear» u «Omitir»).

Componente Incidentes principales de prevención de pérdida de datos



Este componente muestra los principales usuarios, canales, plantillas o endpoints que activaron incidentes de prevención de pérdida de datos en un intervalo de tiempo determinado.

Nota

- Este componente muestra un máximo de 10 usuarios, canales, plantillas o endpoints.
- Las detecciones incluyen todos los incidentes de la prevención de pérdida de datos, sin importar la acción que se haya realizado («Bloquear» u «Omitir»).

En el menú desplegable **Ver por**, seleccione el tipo de datos de prevención de pérdida de datos que se mostrará.

TABLA 2-5. Vistas de prevención de pérdida de datos

MOSTRAR	DESCRIPCIÓN
Usuario	Usuarios que transmitieron la mayor cantidad de activos digitales • Haga clic en los nombres de usuario de la parte inferior del gráfico para mostrar u ocultar la información de detección en el mismo. • Sitúe el puntero del ratón sobre las barras de detección para ver el nombre de usuario y la cantidad de incidentes de prevención de pérdida de datos de este.
Canal	canales de uso más frecuente para la transmisión de activos digitales • Haga clic en los nombres de canal de la parte inferior del gráfico para mostrar u ocultar la información de detección en el mismo. • Sitúe el puntero del ratón sobre las barras de detección para ver el nombre de canal y la cantidad de incidentes de prevención de pérdida de datos de este.
Plantilla	plantillas de activos digitales que activaron el mayor número de detecciones • Haga clic en los nombres de plantilla de la parte inferior del gráfico para mostrar u ocultar la información de detección en el mismo. • Sitúe el puntero del ratón sobre las barras de detección para ver el nombre de plantilla y la cantidad de incidentes de prevención de pérdida de datos de esta.
Endpoints	Endpoints que transmitieron la mayor cantidad de activos digitales • Haga clic en los nombres de endpoint de la parte inferior del gráfico para mostrar u ocultar la información de detección en el mismo. • Sitúe el puntero del ratón sobre las barras de detección para ver el nombre de endpoint y la cantidad de incidentes de prevención de pérdida de datos de este.

Componentes de OfficeScan

Los componentes de OfficeScan proporcionan una referencia rápida de las detecciones y los estados de seguridad del Agente de OfficeScan, así como información de los programas de complemento y los incidentes de epidemias.

Componentes disponibles:

- *Componente Eventos de rellamada de C&C en la página 2-28*
- *Componente Detecciones de riesgos de seguridad en la página 2-30*
- *Componente OfficeScan y Plug-ins Mashup en la página 2-31*
- *Componente Conectividad del agente antivirus en la página 2-32*
- *Agentes conectados al componente Edge Relay Server en la página 2-34*
- *Componente Epidemias en la página 2-34*
- *Componente Actualizaciones del agente en la página 2-36*

Componente Eventos de rellamada de C&C

Este componente muestra toda la información sobre los sucesos de rellamada de C&C, entre la que se incluyen el destino del ataque y la dirección de rellamada de origen.

Puede ver la información sobre las rellamadas de C&C en una lista de servidores de C&C específica. Para seleccionar el origen de la lista (Inteligencia global, Analizador virtual), haga clic en el icono de edición (>) y seleccione la lista del menú desplegable **Origen de lista de C&C**.

Use el menú desplegable **Ver por** para seleccionar el tipo de datos de rellamada de C&C que se muestran:

- **Host comprometido**: muestra la información de C&C más reciente por endpoint de destino.

  TABLA 2-6. Información de Host comprometido

COLUMNA	DESCRIPCIÓN
Host comprometido	El nombre del endpoint que es destino del ataque de C&C
Direcciones de rellamada	El número de direcciones de rellamada con las que el endpoint ha intentado contactar
Última dirección de rellamada	La última dirección de rellamada con la que el endpoint ha intentado contactar
Intentos de rellamada	El número de veces que el endpoint de destino ha intentado contactar con la dirección de rellamada **Nota** Haga clic en el hipervínculo para abrir la pantalla **Registros de rellamada C&C** y ver información más detallada.

- **Dirección de rellamada**: muestra la información de C&C más reciente por dirección de rellamada de C&C.

  TABLA 2-7. Información de dirección de C&C

COLUMNA	DESCRIPCIÓN
Dirección de rellamada	La dirección de las rellamadas de C&C que se originan en la red.
Nivel de riesgo de C&C	El nivel de riesgo de la dirección de rellamada que determina la lista Global Intelligence o Analizador virtual
Hosts comprometidos	El número de Endpoints que son destinos de la dirección de rellamada

Columna	Descripción
Último host comprometido	El nombre del endpoint con el que la dirección de rellamada de C&C ha intentado contactar por última vez.
Intentos de rellamada	El número de rellamadas que se han intentado realizar a la dirección desde la red **Nota** Haga clic en el hipervínculo para abrir la pantalla **Registros de rellamada C&C** y ver información más detallada.

Componente Detecciones de riesgos de seguridad

Este componente muestra la cantidad de riesgos de seguridad detectados y la cantidad de endpoints afectados.

Haga clic en el recuento de endpoints para abrir la pantalla **Administración de agentes**, donde se enumeran los Agentes de OfficeScan afectados del árbol de agentes.

Componente OfficeScan y Plug-ins Mashup

Este componente combina los datos de los Agentes de OfficeScan con los de los programas de complemento instalados y los presenta en el árbol de agentes. Este componente permite valorar rápidamente la cobertura de protección de los agentes y reduce la sobrecarga para la administración de los programas de complemento individuales.

Este componente muestra los datos de los siguientes programas de complemento:

- Compatibilidad con Trend Micro Virtual Desktop

Importante

Debe activar un programa de complemento compatible antes de que el componente Mashup pueda mostrar los datos correspondientes. Si existen nuevas versiones de los programas de complemento, actualícelas.

Para seleccionar las columnas que se muestran en el árbol de agentes, haga clic en el botón **Más opciones** de la esquina superior derecha del componente y, a continuación, haga clic en el botón **Configuración**.

Haga clic en los datos de cualquier columna para abrir la consola del programa de complemento correspondiente o la pantalla **Administración de agentes** de OfficeScan. La pantalla que se abra dependerá del tipo de datos en el que haya hecho clic.

Componente Conectividad del agente antivirus

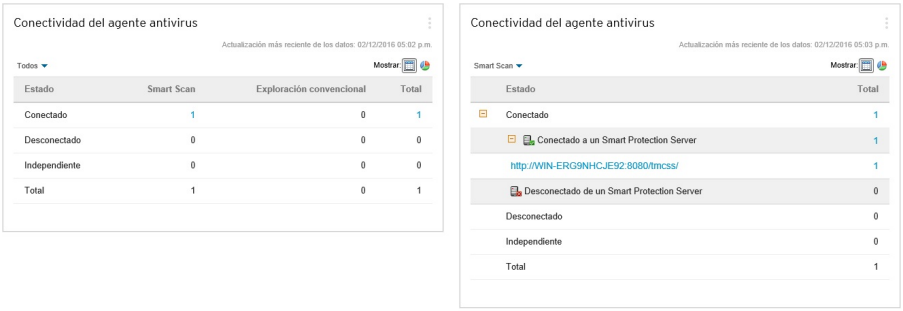


FIGURA 2-4. Vista predeterminada que muestra todos los agentes de Smart Scan y de exploración convencional, así como la vista ampliada del agente de Smart Scan con Smart Protection Servers

Este componente muestra el estado de conexión de los Agentes de OfficeScan al servidor de OfficeScan en relación con el método de exploración configurado (Smart Scan y exploración convencional).

Puede elegir si desea mostrar los datos en una tabla o un gráfico de pastel al hacer clic en los iconos de visualización ( ).

Use la lista desplegable que se encuentra sobre la tabla o el gráfico para cambiar el tipo de datos que se muestran. Haga clic en el recuento de cualquier estado para abrir la pantalla **Administración de agentes** que enumera los Agentes de OfficeScan relacionados en el árbol de agentes.

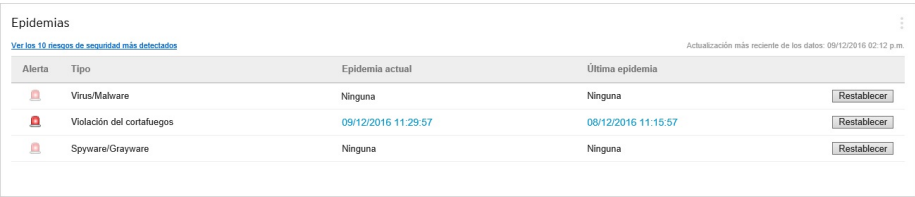
MOSTRAR	DESCRIPCIÓN
Todo	Muestra el estado de conexión de todos los Agentes de OfficeScan para ambos métodos de exploración.
Exploración convencional	Muestra el estado de conexión de todos los Agentes de OfficeScan que usan el método de exploración convencional.

MOSTRAR	DESCRIPCIÓN
Smart Scan	Muestra el estado de conexión de todos los Agentes de OfficeScan que usan el método Smart Scan. Cuando se visualiza el estado de conexión del agente en una tabla: • Expanda la información del agente «conectado» para ver el estado de conexión de los agentes con Smart Protection Server. • Haga clic en la URL para abrir la consola de administración de Smart Protection Server. **Nota** Solo los agentes conectados (que informan al servidor de OfficeScan) pueden informar de su estado de conexión con servidores Smart Protection Server. Para restaurar la conexión de un agente desconectado con Smart Protection Server, consulte *Soluciones a los problemas que se indican en los iconos del agente de OfficeScan en la página 15-44*.

Agentes conectados al componente Edge Relay Server

Este componente muestra el número de Agentes de OfficeScan conectados a OfficeScan Edge Relay Server durante un periodo de tiempo concreto.

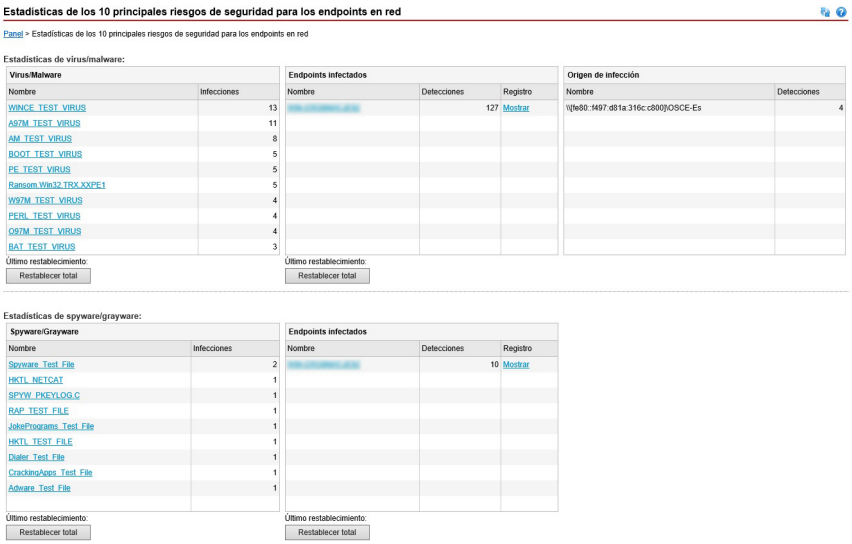
Componente Epidemias



El componente **Epidemias** muestra el estado de cualquier epidemia de riesgo de seguridad actual que exista en el sistema y la última alerta de epidemia.

- Haga clic en el enlace de fecha y hora de la alerta para obtener más información sobre la epidemia.
- **Restablezca** el estado de la información de alerta de epidemia y aplique medidas de prevención de epidemias de manera inmediata cuando OfficeScan detecte una.

  Para obtener información detallada acerca de la aplicación de medidas de prevención de epidemias, consulte *Políticas de prevención de epidemias en la página 7-120*.
- Haga clic en **Ver los 10 riesgos de seguridad más detectados** para ver los riesgos de seguridad más recurrentes, los endpoints con mayor número de riesgos de seguridad y los principales orígenes de infecciones.

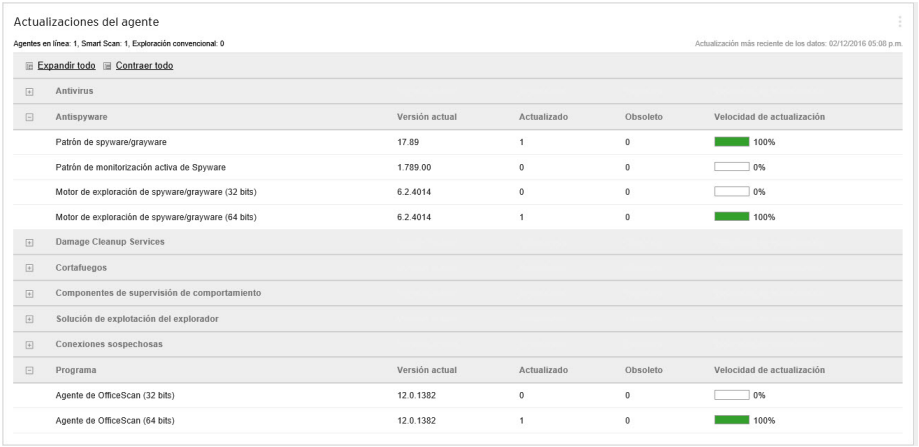


En la pantalla **Estadísticas de los 10 principales riesgos de seguridad**, puede:

- Ver información detallada sobre un riesgo de seguridad haciendo clic en su nombre.

- Ver el estado general de un endpoint concreto haciendo clic en el Nombre del Endpoint.
- Ver los registros de riesgos de seguridad del endpoint haciendo clic en **Ver** junto al nombre del endpoint.
- Restablecer la estadística de cada tabla haciendo clic en **Restablecer recuento**.

Componente Actualizaciones del agente



Este componente muestra los componentes y los programas disponibles que protegen a los Agentes de OfficeScan frente a los riesgos de seguridad.

Haga clic en el recuento con el estado «Obsoleto» para abrir la pantalla **Administración de agentes**, donde se enumeran los Agentes de OfficeScan que requieren actualizaciones en el árbol de agentes.

Componente de administración

El componente de administración muestra el estado de conexión de los Agentes de OfficeScan con el servidor de OfficeScan.

Componentes disponibles:

- *Componente Conectividad entre agente y servidor en la página 2-37*

Componente Conectividad entre agente y servidor

Este componente muestra el estado de conexión de todos los agentes con un servidor de OfficeScan.

Puede alternar entre la tabla y el gráfico de sectores haciendo clic en los iconos de pantalla ( ).

Haga clic en el recuento de cualquier estado para abrir la pantalla **Administración de agentes** que enumera los Agentes de OfficeScan relacionados en el árbol de agentes.

Server Migration Tool

OfficeScan ofrece Server Migration Tool, que permite a los administradores copiar la configuración de OfficeScan de versiones anteriores de OfficeScan a la versión actual. Server Migration Tool migra la siguiente configuración:

CARACTERÍSTICA	CONFIGURACIONES MIGRADAS
Administración de agentes	• Configuración de la exploración manual* • Configuración de la exploración programada* • Configuración de la exploración en tiempo real* • Configuración de Explorar ahora* • Configuración de la reputación Web* • Configuración de la supervisión del comportamiento* • Configuración de control de dispositivos* • Configuración de la prevención de pérdida de datos* • Derechos y otras configuraciones* • Configuración de servicios adicionales* • Lista de spyware/grayware permitido* **Nota** • La herramienta de migración de servidor no migra los directorios de copia de seguridad en los procesos de Exploración manual, Exploración programada, Exploración en tiempo real o Explorar ahora. • La configuración conserva los ajustes tanto a nivel de raíz como a nivel de dominio.
Agrupación de agentes	Todas las configuraciones **Nota** Las estructuras de los dominios de Active Directory se muestran tras sincronizar con Active Directory por primera vez.
Configuración general del agente	Todas las configuraciones

Característica	Configuraciones migradas
Ubicación del Endpoint	• Configuración de conocimiento de ubicación • Listas de direcciones IP y MAC del gateway
Prevención de pérdida de datos	• Identificadores de datos • Plantillas
Cortafuegos	• Políticas • Perfiles
Mantenimiento de los registros	Todas las configuraciones
Origen de actualización del agente	• Fuente de actualización del agente • Lista de orígenes de actualización personalizados
Fuentes de Smart Protection	Lista de fuentes de Smart Protection personalizadas
Notificaciones	• Configuración de notificaciones generales • Configuración de las notificaciones del administrador • Configuración de las notificaciones de epidemias • Configuración de las notificaciones de agentes
Proxy	Todas las configuraciones
Agentes inactivos	Todas las configuraciones
Administrador de cuarentena	Todas las configuraciones
Consola Web	Todas las configuraciones
Configuración de `ofcscan.ini`	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: Todas las configuraciones

CARACTERÍSTICA	CONFIGURACIONES MIGRADAS
Configuración de `ofcserver.ini`	[INI_SERVER_DISK_THRESHOLD]: Todas las configuraciones

Nota

- La herramienta no realiza una copia de seguridad de las listas de los Agente de OfficeScan del servidor de OfficeScan, sino únicamente de las estructuras de los dominios.
- El Agente de OfficeScan solo migra las características disponibles en la versión anterior del servidor del Agente de OfficeScan. En el caso de las características que no están disponibles en el servidor anterior, el Agente de OfficeScan aplica la configuración predeterminada.

Usar Server Migration Tool

Nota

Esta versión de OfficeScan es compatible con migraciones desde la versión 10.6 SP3 y posteriores de OfficeScan.

Las versiones de OfficeScan más antiguas no pueden contener toda la configuración disponible en la versión más reciente. OfficeScan aplica automáticamente la configuración predeterminada para cualquier función que no se ha migrado de la versión anterior del servidor de OfficeScan.

Procedimiento

1. En el equipo del servidor de OfficeScan XG, vaya a la <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\ServerMigrationTool`.
2. Copie la herramienta Server Migration Tool en el equipo del servidor de OfficeScan de origen.

Importante

Debe utilizar la herramienta de migración de servidor de OfficeScan XG en la versión del servidor de OfficeScan de origen para garantizar que todos los datos tengan el formato adecuado para el nuevo servidor de destino. OfficeScan XG no es compatible con versiones anteriores de la herramienta de migración de servidor.

3. Haga doble clic en `ServerMigrationTool.exe` para iniciar Server Migration Tool.

   Server Migration Tool se abre.

4. Para exportar la configuración desde el servidor origen de OfficeScan:

   a. Especifique la carpeta de destino mediante el botón **Examinar**.

   Nota

   El nombre predeterminado del paquete de exportación es `OsceMigrate.zip`.

   b. Haga clic en **Exportar**.

      Aparecerá un mensaje de confirmación.

   c. Copie el paquete de exportación a la carpeta de destino del servidor de OfficeScan.

5. Para importar la configuración al servidor de OfficeScan de destino:

   a. Busque el paquete de exportación mediante el botón **Examinar**.

   b. Haga clic en **Importar**.

      Aparece un mensaje de advertencia.

   c. Haga clic en **Sí** para continuar.

      Aparecerá un mensaje de confirmación.

6. Compruebe que el servidor contiene toda la configuración de la versión anterior de OfficeScan.

7. Mueva los Agentes de OfficeScan antiguos al nuevo servidor.

Para obtener más información sobre cómo mover los Agentes de OfficeScan, consulte *Mover agentes de OfficeScan a otro dominio o servidor de OfficeScan en la página 2-70* o *Agent Mover en la página 15-24*.

Integración con Active Directory

Integre OfficeScan con la estructura de Microsoft™ Active Directory™ para administrar Agentes de OfficeScan de manera más eficiente, asignar permisos de la consola Web mediante cuentas de Active Directory y determinar los agentes que no tienen instalado ningún software de seguridad. Todos los usuarios en el dominio de la red pueden tener acceso seguro a la consola de OfficeScan. Si lo desea, puede configurar un acceso limitado para usuarios específicos, incluso para los que se encuentran en otro dominio. El proceso de autenticación y la clave de cifrado ofrecen la validación de las credenciales para los usuarios.

Active Directory le permite beneficiarse plenamente de las siguientes funciones:

- **Grupos de agentes personalizados**: utilice Active Directory o direcciones IP para agrupar agentes de forma manual y asignarlos a dominios en el árbol de agentes de OfficeScan.

  Para conocer más detalles, consulte *Agrupación de agentes automática en la página 2-63*.

- **Endpoints no administrados**: Asegúrese de que los endpoints de la red que no están administrados por el servidor de OfficeScan cumplen con las directrices de seguridad de la empresa.

  Para conocer más detalles, consulte *Conformidad con las normas de seguridad para Endpoints no administrados en la página 15-76*.

Sincronice la estructura de Active Directory de forma manual o periódica con el servidor de OfficeScan para garantizar la consistencia de los datos.

Para conocer más detalles, consulte *Sincronizar datos con dominios de Active Directory en la página 2-44*.

Integración de Active Directory con OfficeScan

Procedimiento

1. Vaya a **Administración** > **Active Directory** > **Integración con Active Directory**.
2. En **Dominios de Active Directory**, especifique el nombre del dominio de Active Directory.
3. Especifique las credenciales que utilizará el servidor de OfficeScan al sincronizar datos con el dominio de Active Directory especificado. Si el servidor no forma parte del dominio, se requerirán credenciales del dominio. En caso contrario, las credenciales son opcionales. Asegúrese de que estas credenciales no caduquen o el servidor no podrá sincronizar los datos.
   a. Haga clic en **Especificar las credenciales del dominio**.
   b. En la ventana emergente que se abre, escriba el nombre de usuario y la contraseña. El nombre de usuario se puede especificar mediante alguno de los formatos siguientes:
      - `dominio\nombre de usuario`
      - `nombredeusuario@dominio`
   c. Haga clic en **Guardar**.
4. Haga clic en el botón (+) para agregar más dominios. En caso necesario, especifique credenciales de dominio para cualquiera de los dominios agregados.
5. Haga clic en el botón (-) para eliminar dominios.
6. Especifique la configuración de cifrado si ha especificado credenciales de dominio. Como medida de seguridad, OfficeScan cifra las credenciales del dominio especificadas antes de guardarlas en la base de datos. Cuando OfficeScan sincroniza datos con cualquiera de los dominios especificados, utilizará una clave de cifrado para descifrar las credenciales de dominio.
   a. Vaya a la sección **Configuración de cifrado para credenciales del dominio**.

b. Escriba una clave de cifrado que no supere los 128 bytes.

c. Especifique un archivo en el que guardar la clave de cifrado. Puede elegir un formato de archivo popular como, por ejemplo, `.txt`. Escriba el nombre y la ruta de acceso completa del archivo, por ejemplo, `C:\AD_Encryption\EncryptionKey.txt`.

¡ADVERTENCIA!

Si el archivo se ha eliminado o si su ruta se ha modificado, OfficeScan no podrá sincronizar datos con ninguno de los dominios especificados.

7. Haga clic en una de las siguientes opciones:

   - **Guardar**: solo guarda la configuración. Dado que la sincronización de datos puede forzar los recursos del sistema, puede elegir guardar solo la configuración y sincronizar más tarde, por ejemplo durante horas que no sean críticas para la empresa.
   - **Guardar y sincronizar**: guarda la configuración y sincroniza los datos con los dominios de Active Directory.

8. Programar sincronizaciones periódicas. Para conocer más detalles, consulte *Sincronizar datos con dominios de Active Directory en la página 2-44*.

Sincronizar datos con dominios de Active Directory

Sincronice datos con dominios de Active Directory regularmente para mantener actualizada la estructura de árbol de agentes de OfficeScan y para consultar agentes sin gestionar.

Sincronizar manualmente datos con dominios de Active Directory

Procedimiento

1. Vaya a **Administración** > **Active Directory** > **Integración con Active Directory**.

2. Compruebe que las credenciales de dominio y la configuración de cifrado no haya cambiado.
3. Haga clic en **Guardar y sincronizar**.

Sincronizar automáticamente datos con dominios de Active Directory

Procedimiento

1. Vaya a **Administración** > **Active Directory** > **Sincronización programada**.
2. Seleccione **Activar la sincronización programada de Active Directory**.
3. Especifique el programa de sincronización.

   Nota

   Para las sincronizaciones diarias, semanales y mensuales, el periodo de tiempo es el número de horas en las que OfficeScan sincronizará Active Directory con el servidor de OfficeScan.

4. Haga clic en **Guardar**.

Árbol de agentes de OfficeScan

El árbol de agentes de OfficeScan muestra todos los agentes agrupados en dominios que el servidor gestiona actualmente. Los agentes están agrupados por dominios, por lo que

podrá configurar, gestionar y aplicar la misma configuración a todos los miembros del dominio al mismo tiempo.

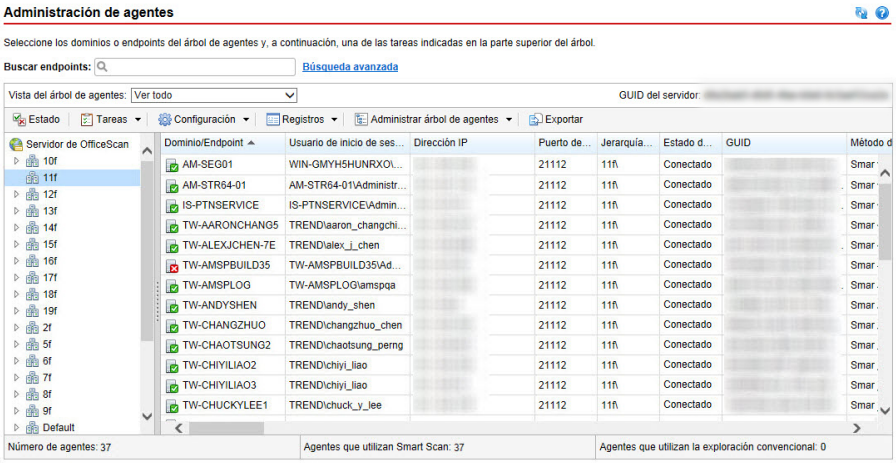


FIGURA 2-5. Árbol de agentes de OfficeScan

Estado de conexión del agente

El estado de la conexión del Agente de OfficeScan depende del modo en el que el servidor de OfficeScan se comunica con el Agente de OfficeScan. En la siguiente tabla se describen los diferentes estados de conexión disponibles para el Agente de OfficeScan.

TABLA 2-8. Estado de conexión del agente de OfficeScan

ESTADO	DESCRIPCIÓN
Conectado	El Agente de OfficeScan se puede conectar al servidor de OfficeScan para ofrecer comunicación bidireccional de estos elementos: • Configuración de políticas • Actualizaciones • Comandos de exploración • Sincronización de listas de objetos sospechosos • Envío de muestras • Envío de registros
Desconectado	El Agente de OfficeScan no tiene ninguna conexión funcional con el servidor de OfficeScan ni con Edge Relay Server.
Independiente	El Agente de OfficeScan se puede conectar al servidor de OfficeScan, pero la comunicación es limitada. Mientras está en el modo independiente: • El Agente de OfficeScan no acepta configuración de políticas del servidor. • El Agente de OfficeScan no inicia comandos de exploración desde el servidor. • El Agente de OfficeScan no envía registros al servidor. Puede configurar agentes independientes con derechos para permitir o bloquear actualizaciones de componentes si hay una conexión funcional con el servidor de OfficeScan disponible. Los usuarios finales pueden iniciar exploraciones y actualizaciones de forma manual en los agentes en modo independiente.

Estado	Descripción
Fuera de las instalaciones	El Agente de OfficeScan se encuentra fuera de la red de la empresa y no se puede conectar al servidor de OfficeScan directamente. No obstante, el Agente de OfficeScan puede conectarse a Edge Relay Server para estos elementos: • Sincronización de listas de objetos sospechosos • Envío de muestras • Envío de registros

Iconos del árbol de agentes

Los iconos de árbol de agentes de OfficeScan brindan sugerencias visuales que indican el tipo de endpoint y el estado de los Agentes de OfficeScan que OfficeScan administra.

Tabla 2-9. OfficeScan Iconos del árbol de agentes

Icono	Descripción
	Dominio
	Raíz
	Agente de actualización
	Agente de exploración convencional
	Agente de OfficeScan disponible para Smart Scan
	Agente de OfficeScan no disponible para Smart Scan
	Agente de actualización disponible para Smart Scan

Icono	Descripción
	Agente de actualización no disponible para Smart Scan

Tareas generales del árbol de agentes

A continuación se detallan las tareas generales que puede realizar cuando se visualice el árbol de agentes:

Procedimiento

- Haga clic en el icono de dominio raíz ( ) para seleccionar todos los dominios y agentes. Cuando selecciona el icono de dominio raíz y, a continuación, elige una de las tareas que se encuentran en la parte superior del árbol de agentes, aparece una pantalla para definir los valores de configuración. En la pantalla, elija alguna de las siguientes opciones generales:
  - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
  - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.
- Para seleccionar varios agentes o dominios seguidos:
  - En el panel derecho, seleccione el primer dominio, mantenga pulsada la tecla Mayús y haga clic en el último dominio o agente del intervalo.
- Para seleccionar un intervalo de dominios o agentes no consecutivos, en el panel derecho, haga clic en los dominios o agentes que desea seleccionar mientras mantiene pulsada la tecla Ctrl.
- Para buscar un agente que deba gestionarse, especifique el nombre del agente en el cuadro de texto **Buscar Endpoints**.

Una lista de resultados aparecerá en el árbol de agentes. Si desea contar con más opciones de búsqueda, haga clic en **Búsqueda avanzada**.

Nota

No se pueden especificar direcciones IPv4 ni IPv6 cuando se buscan agentes específicos. Utilice la búsqueda avanzada para buscar mediante la dirección IPv4 o IPv6. Para conocer más detalles, consulte *Opciones de la búsqueda avanzada en la página 2-51*.

- Tras seleccionar un dominio, la tabla del árbol de agentes se ampliará para mostrar los agentes pertenecientes al dominio, así como todas las columnas que contienen información de interés para cada agente. Si desea ver únicamente un conjunto de columnas relacionadas, seleccione un elemento en la vista del árbol de agentes.
  - **Ver todo**: muestra todas las columnas.
  - **Vista de actualización**: muestra todos los componentes y programas
  - **Vista de antivirus**: muestra los componentes del antivirus.
  - **Vista de antispyware**: muestra los componentes antispyware.
  - **Vista de protección de datos**: muestra el estado del módulo de protección de datos de los agentes.
  - **Vista del cortafuegos**: muestra los componentes del cortafuegos.
  - **Vista de protección inteligente**: muestra el método de exploración utilizado por los agentes (exploración convencional o Smart Scan) y los componentes de Smart Protection.
  - **Vista del agente de actualización**: muestra información de todos los agentes de actualización que administra el servidor de OfficeScan.
  - **Vista del agente fuera de las instalaciones**: muestra la información de todos los agentes que informan a Edge Relay Server.
- Para ordenar los agentes según la información de la columna, haga clic en el nombre de la columna.
- Para actualizar el árbol de agentes, haga clic en el icono de actualización ( ).

- Consulte las estadísticas del agente debajo del árbol de agentes, como el número total de agentes, el número de agentes Smart Scan y el número de agentes de exploración convencional.

Opciones de la búsqueda avanzada

Busque agentes en función de los siguientes criterios:

Procedimiento

- **Criterios básicos**: incluyen información básica acerca de endpoints, como la dirección IP, el sistema operativo, el dominio, la dirección MAC, el método de exploración y el estado de la reputación Web.
    - Para realizar búsquedas por segmento IPv4 se necesita un fragmento de una dirección IP que empiece por el primer octeto. La búsqueda mostrará todos los endpoints cuyas direcciones IP contengan la entrada indicada. Por ejemplo, si escribe 10.5, la búsqueda devolverá todos los equipos cuya dirección IP esté comprendida en el rango desde 10.5.0.0 hasta 10.5.255.255.
    - La búsqueda por intervalo de direcciones IPv6 requiere un prefijo y una longitud.
    - La búsqueda por dirección MAC requiere un intervalo de direcciones MAC con notación hexadecimal, por ejemplo, 000A1B123C12.
- **Versión del componente**: seleccione la casilla de verificación junto al nombre del componente, limite el criterio seleccionado **Anterior a** o **Anterior a inclusive**, y escriba un número de versión. De forma predeterminada se muestra el número de versión actual.
- **Estado**: incluye la configuración de agente.
- Haga clic en **Buscar** después de especificar los criterios de búsqueda. En el árbol de agentes aparecerá una lista de los nombres de endpoints que cumplen los criterios de la búsqueda.

Tareas específicas del árbol de agentes

El árbol de agentes se muestra al acceder a determinadas pantallas de la consola Web. En la parte superior del árbol de agentes se encuentran las opciones de menú específicas de la pantalla a la que haya accedido. Estas opciones de menú le permiten realizar tareas específicas, como configurar los valores del agente o iniciar tareas del agente. Para llevar a cabo cualquier tarea, seleccione el destino de la tarea y, a continuación, seleccione una opción de menú.

Las siguientes pantallas muestran el árbol de agentes:

- *Pantalla Administración de agentes en la página 2-52*
- *Pantalla Prevención de epidemias en la página 2-56*
- *Pantalla Selección del agente en la página 2-57*
- *Pantalla Recuperar en la página 2-58*
- *Pantalla Registros de riesgos de seguridad en la página 2-59*

Pantalla Administración de agentes

Para ver esta pantalla, vaya a **Agentes** > **Administración de agentes**.

Administre la configuración general de agentes y consulte la información de estado sobre agentes específicos (por ejemplo: **usuario de inicio de sesión**, **dirección IP** y **estado de conexión**) en la pantalla **Administración de agentes**.

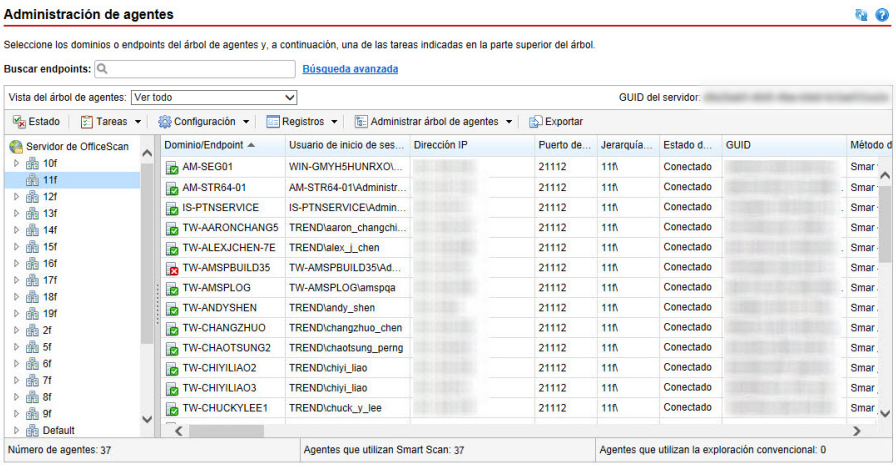


FIGURA 2-6. Pantalla Administración de agentes

En la siguiente tabla figuran las tareas que puede realizar:

TABLA 2-10. Tareas de Administración de agentes

BOTÓN MENÚ	TAREA
Estado	Ver información detallada sobre el agente. Para conocer más detalles, consulte *Visualización de información sobre agentes de OfficeScan en la página 15-60*.
Tareas	• Ejecute Explorar ahora en los endpoints del agente. Para conocer más detalles, consulte *Iniciar Explorar ahora en la página 7-26*. • Desinstalar el agente. Para conocer más detalles, consulte *Desinstalación del agente de OfficeScan desde la consola Web en la página 5-79*.

Botón Menú	Tarea
	• Restaurar detecciones de archivos sospechosos. Para conocer más detalles, consulte *Restauración de archivos en cuarentena en la página 7-46*. • Restaurar los componentes de spyware y grayware. Para conocer más detalles, consulte *Restaurar spyware/grayware en la página 7-56*.

Configuración	• Defina la configuración de exploración. Para ver los detalles, consulte los temas siguientes:
	  • *Tipos de métodos de exploración en la página 7-9*
	  • *Exploración manual en la página 7-19*
	  • *Exploración en tiempo real en la página 7-16*
	  • *Exploración programada en la página 7-21*
	  • *Explorar ahora en la página 7-24*
	• Configurar los ajustes de la reputación Web. Para conocer más detalles, consulte *Políticas de reputación Web en la página 12-5*.
	• Configuración del aprendizaje automático predictivo. Para conocer más detalles, consulte *Configuración de las opciones del aprendizaje automático predictivo en la página 8-3*.
	• Configuración de las conexiones sospechosas. Para conocer más detalles, consulte *Definir la configuración de conexión sospechosa en la página 8-7*.
	• Configure los parámetros de Supervisión del comportamiento. Para conocer más detalles, consulte *Supervisión del comportamiento en la página 9-2*.
	• Configure los valores de Control de dispositivos. Para conocer más detalles, consulte *Control de dispositivos en la página 10-2*.
	• Configurar las políticas de prevención de pérdida de datos Para conocer más detalles, consulte *Configuración de las políticas de prevención de pérdida de datos en la página 11-50*.

BOTÓN MENÚ	TAREA
	• Asignar agentes como agentes de actualización. Para conocer más detalles, consulte *Configuración del agente de actualización en la página 6-59*. • Configurar los derechos del agente y otros valores de configuración. Para conocer más detalles, consulte *Configuración de derechos y otras configuraciones de los agentes en la página 15-99*. • Active o desactive los servicios del Agente de OfficeScan. Para conocer más detalles, consulte *Servicios del agente de OfficeScan en la página 15-7*. • Configurar la lista de spyware/grayware permitidos. Para conocer más detalles, consulte *Lista de spyware/grayware permitido en la página 7-53*. • Configure la lista de programas de confianza. Para conocer más detalles, consulte *Configuración de la lista de programas de confianza en la página 7-57*. • Importar y exportar la configuración del agente. Para conocer más detalles, consulte *Importación y exportación de la configuración de los agentes en la página 15-61*.
Registros	Consulte los siguientes registros: • Registros de virus/malware (para obtener información detallada, consulte *Visualización de los registros de virus/malware en la página 7-98*) • Registros de spyware y grayware (para obtener información detallada, consulte *Visualización de los registros de spyware/grayware en la página 7-107*) • Registros del cortafuegos (para obtener información detallada, consulte *Registros del cortafuegos en la página 13-30*) • Registros de reputación Web (para obtener información detallada, consulte *Registros de amenazas Web en la página 12-22*) • Registros de conexiones sospechosas (para obtener información detallada, consulte *Ver los registros de conexión sospechosa en la página 8-15*)

Botón Menú	Tarea
	• Registros de archivos sospechosos (para obtener información detallada, consulte *Ver los registros de archivos sospechosos en la página 7-111*) • Registros de rellamadas de C&C (para obtener información detallada, consulte *Visualización de los registros de rellamadas de C&C en la página 12-24*). • Registros de supervisión del comportamiento (para obtener información detallada, consulte *Registros de supervisión del comportamiento en la página 9-18*) • Registros del aprendizaje automático predictivo (para obtener información, consulte *Visualización de los registros del aprendizaje automático predictivo en la página 8-11*) • Registros de control de dispositivos (para obtener información detallada, consulte *Registros de control de dispositivos en la página 10-19*) • Registros de DLP (para obtener información detallada, consulte *Registros de prevención de pérdida de datos en la página 11-60*) • Registros de operaciones de exploración (para obtener información detallada, consulte *Visualización de los registros de operaciones de exploración en la página 7-113*) Eliminar registros. Para conocer más detalles, consulte *Administración de registros en la página 14-43*.
Administrar el árbol de agentes	Administrar el árbol de agentes. Para conocer más detalles, consulte *Tareas de agrupación de agentes en la página 2-67*.
Exportar	Exportar una lista de agentes a un archivo de valores separados por comas (`.csv`).

Pantalla Prevención de epidemias

Para ver esta pantalla, vaya a **Agentes** > **Prevención de epidemias**.

Especifique y active la configuración de la prevención frente a epidemias en la pantalla **Prevención de epidemias**. Para conocer más detalles, consulte *Configuración de la prevención de epidemias de riesgos de seguridad en la página 7-118*.

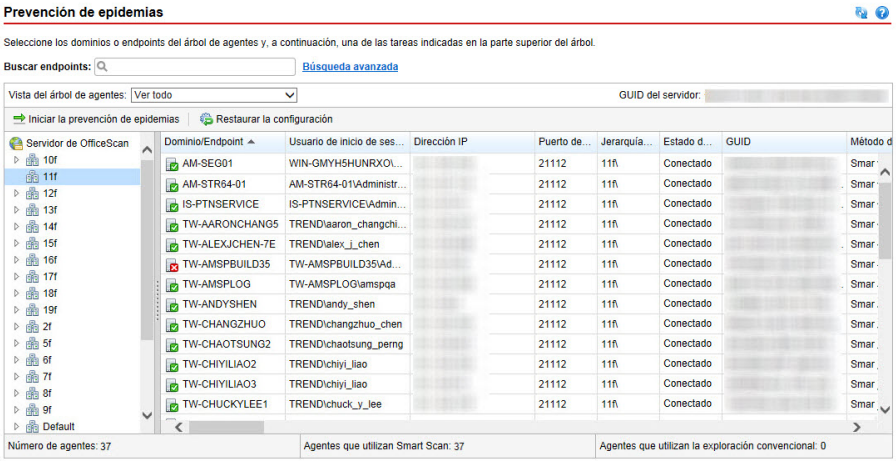


FIGURA 2-7. Pantalla Prevención de epidemias

Pantalla Selección del agente

Para ver esta pantalla, vaya a **Actualizaciones** > **Agentes** > **Actualización manual**. Elija **Seleccionar agentes manualmente** y haga clic en **Seleccionar**.

Inicie la actualización manual en la pantalla **Selección del agente**. Para conocer más detalles, consulte *Actualizaciones manuales del agente en la página 6-48*.

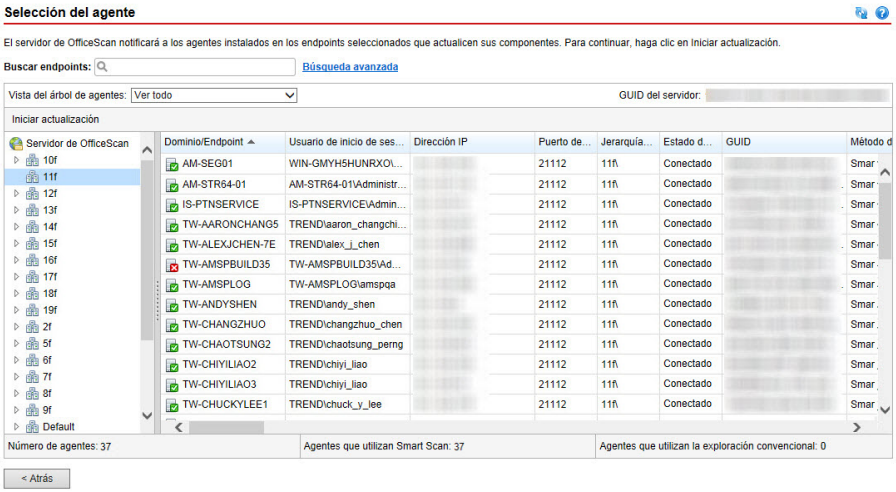


FIGURA 2-8. Pantalla Selección del agente

Pantalla Recuperar

Para ver esta pantalla, vaya a **Actualizaciones** > **Recuperar**. Haga clic en **Sincronizar con el servidor**.

Recupere los componentes de los agente en la pantalla **Recuperar**. Para conocer más detalles, consulte *Recuperar componentes de los agentes de OfficeScan en la página 6-56*.

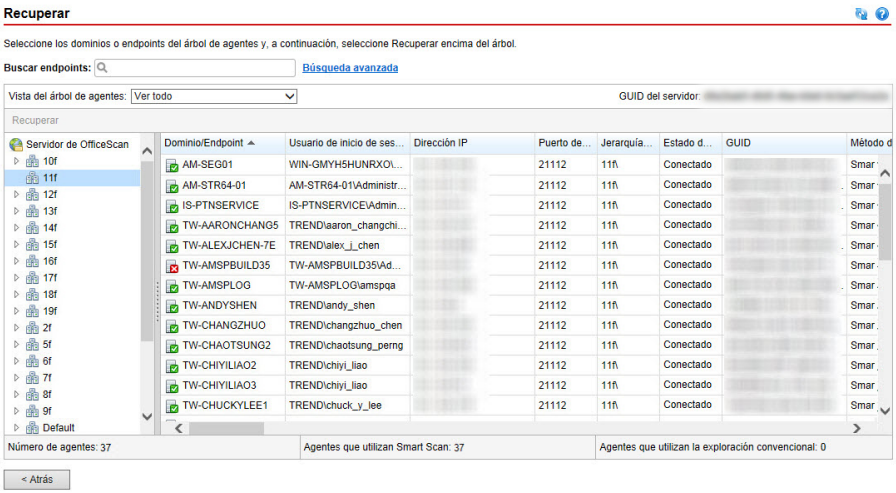


FIGURA 2-9. Pantalla Recuperar

Pantalla Registros de riesgos de seguridad

Para ver esta pantalla, vaya a **Registros** > **Agentes** > **Riesgos de seguridad**.

Consulte y gestione los registros en la pantalla **Registros de riesgos de seguridad**.

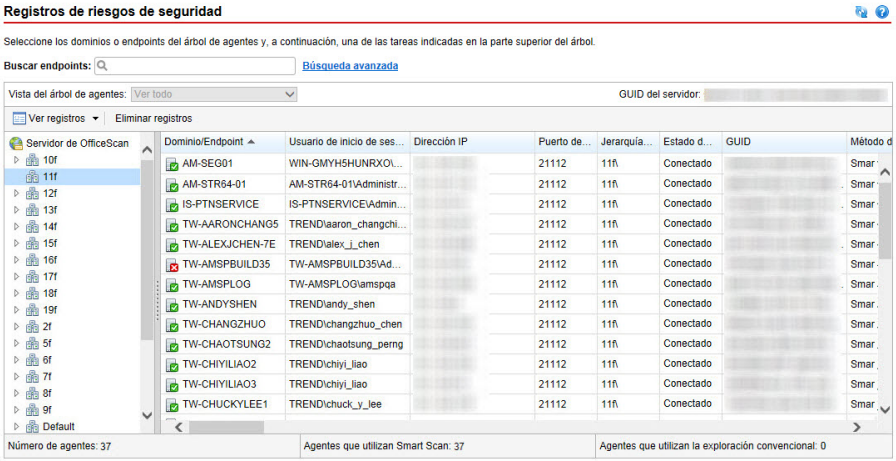


FIGURA 2-10. Pantalla Registros de riesgos de seguridad

Realice las siguientes tareas:

1. Vea los registros que los agentes envían al servidor. Para obtener información detallada, consulte:

   - *Visualización de los registros de virus/malware en la página 7-98*
   - *Visualización de los registros de spyware/grayware en la página 7-107*
   - *Ver registros del cortafuegos en la página 13-31*
   - *Ver registros de reputación Web en la página 12-23*
   - *Ver los registros de conexión sospechosa en la página 8-15*
   - *Ver los registros de archivos sospechosos en la página 7-111*
   - *Visualización de los registros de rellamadas de C&C en la página 12-24*
   - *Visualización de registros de supervisión del comportamiento en la página 9-18*

- *Visualización de los registros de Control de dispositivos en la página 10-20*
- *Visualización de los registros de prevención de pérdida de datos en la página 11-61*

2. Eliminar registros. Para conocer más detalles, consulte *Administración de registros en la página 14-43*.

Dominios de OfficeScan

Un dominio en OfficeScan es un grupo de agentes que comparten la misma configuración y ejecutan las mismas tareas. Si agrupa los agentes por dominios, podrá configurar, administrar y aplicar la misma configuración a todos los miembros del dominio. Para obtener más información sobre la agrupación de agentes, consulte *Agrupación de agentes en la página 2-61*.

Agrupación de agentes

Utilice la agrupación de agentes para crear dominios de forma manual o automática en el árbol de agentes de OfficeScan.

Hay dos formas de agrupar agentes en dominios.

TABLA 2-11. Métodos de agrupación de agentes

MÉTODO	AGRUPACIÓN DE AGENTES	DESCRIPCIONES
Manual	• Dominio NetBIOS • Dominio de Active Directory • Dominio DNS	La agrupación manual de agentes define el dominio al que debería pertenecer un agente instalado recientemente. Cuando el agente aparezca en el árbol de agentes, podrá moverlo a otro dominio o a otro servidor de OfficeScan. La agrupación manual de agentes también permite crear, administrar y eliminar dominios del árbol de agentes. Para conocer más detalles, consulte *Agrupación manual de agentes en la página 2-62*.

Método	Agrupación de agentes	Descripciones
Automático	Grupos de agentes personalizados	La agrupación automática de agentes utiliza reglas para ordenar los agentes en el árbol de agentes. Tras definir estas reglas, puede acceder al árbol de agentes para ordenar de forma manual los agentes o permitir que OfficeScan los ordene de forma automática cuando se produzcan sucesos concretos o a intervalos programados. Para conocer más detalles, consulte *Agrupación de agentes automática en la página 2-63*.

Agrupación manual de agentes

OfficeScan utiliza esta configuración solo durante instalaciones de agentes nuevas. El programa de instalación comprueba el dominio de la red a la que pertenece un endpoint de destino. En caso de que el nombre del dominio ya exista en el árbol de agentes, OfficeScan agrupará el agente en el endpoint de destino de ese dominio y aplicará los ajustes configurados para el dominio. Si no existe el nombre del dominio, OfficeScan añade el dominio al árbol de agentes, agrupa el agente en ese dominio y, a continuación, aplica la configuración raíz al dominio y al agente.

Configuración de agrupaciones manuales de agentes

Procedimiento

1. Vaya a **Agentes** > **Agrupación de agentes**.
2. Especifique el método de agrupación de agentes:
   - Dominio NetBIOS
   - Dominio de Active Directory
   - Dominio DNS
3. Haga clic en **Guardar**.

Qué hacer a continuación

Realice las siguientes tareas para administrar los dominios y los agentes agrupados en ellos:

- Añadir un dominio
- Eliminar un dominio o agente
- Cambiar el nombre de un dominio
- Mover un agente a otro dominio

Para conocer más detalles, consulte *Tareas de agrupación de agentes en la página 2-67*.

Agrupación de agentes automática

La agrupación de agentes automática utiliza reglas definidas mediante direcciones IP o dominios de Active Directory. Si una regla define una dirección IP o un intervalo de direcciones IP, el servidor de OfficeScan agrupará a los agentes con una dirección IP que coincida en un dominio específico del árbol de agentes. De forma similar, si una regla define uno o varios dominios de Active Directory, el servidor de OfficeScan agrupará los agentes que pertenezcan a un dominio concreto de Active Directory en un dominio específico del árbol de agentes.

Los agentes aplican las reglas de una en una. Priorice las reglas de modo que se aplique la de mayor prioridad si un agente cumple más de una.

Configurar la agrupación automática de agentes

Procedimiento

1. Vaya a **Agentes** > **Agrupación de agentes**
2. Vaya a la sección **Agrupación de agentes** y seleccione **Crear grupos de agentes personalizados para agentes de OfficeScan existentes**.
3. Vaya a la sección **Agrupación automática de agentes**.
4. Para comenzar a crear normas, haga clic en **Agregar** y, a continuación, seleccione **Active Directory** o **Dirección IP**.

- Si ha seleccionado **Active Directory**, consulte las instrucciones de configuración que se proporcionan en *Definición de reglas de agrupación de agentes mediante dominios de Active Directory en la página 2-65*.
- Si ha seleccionado **Dirección IP**, consulte las instrucciones de configuración que se proporcionan en *Definir reglas de agrupación de agentes por dirección IP en la página 2-66*.

5. Si ha creado más de una norma, priorice las normas mediante estos pasos:
   a. Seleccione una norma.
   b. Haga clic en una de las flechas de la columna **Prioridad de grupo** para hacer que la norma ascienda o descienda en la lista. El número de identificación de la norma cambia para reflejar su nueva posición.
6. Para utilizar las reglas durante la ordenación de agentes:
   a. Marque las casillas de verificación de las normas que desee utilizar.
   b. Para activar las reglas cambie el control de **Estado** a **Activado**.

Nota

Si no activa la casilla de verificación de una regla o si la desactiva, la regla no se utilizará al ordenar los agentes en el árbol de agentes. Por ejemplo, si la regla dicta que un agente se debe mover a un nuevo dominio, el agente no se moverá, sino que permanecerá en su dominio actual.

7. Especifique un programa de ordenación en la sección **Creación de dominios programada**.
   a. Seleccione **Activar la creación de dominios programada**.
   b. Especifique el programa en **Creación de dominios programada**.
8. Seleccione una de estas opciones:
   - **Guardar y crear dominio ahora**: Elija esta opción si ha especificado nuevos dominios en *Definir reglas de agrupación de agentes por dirección IP en la página 2-66*, paso 7 o en *Definición de reglas de agrupación de agentes mediante dominios de Active Directory en la página 2-65*, paso 7.

- **Guardar**: seleccione esta opción si no ha especificado nuevos dominios o si desea crearlos solo cuando se ejecute la ordenación de agentes.

Nota

La ordenación de agentes no comenzará tras completar este paso.

Definición de reglas de agrupación de agentes mediante dominios de Active Directory

Asegúrese de haber configurado la integración de Active Directory antes de llevar a cabo los pasos del proceso descrito a continuación. Para conocer más detalles, consulte *Integración con Active Directory en la página 2-42*.

Procedimiento

1. Vaya a **Agentes** > **Agrupación de agentes**.
2. Vaya a la sección **Agrupación de agentes** y seleccione **Crear grupos de agentes personalizados para agentes de OfficeScan existentes**.
3. Vaya a la sección **Agrupación automática de agentes**.
4. Haga clic en **Agregar** y, a continuación, seleccione **Active Directory**.

   Aparecerá una nueva pantalla.
5. Seleccione **Permitir agrupación**.
6. Especifique un nombre para la regla.
7. En **Fuente de Active Directory**, seleccione el dominio o dominios y los subdominios de Active Directory.
8. En **Árbol de agentes**, seleccione un dominio de OfficeScan existente al que asignar los dominios de Active Directory. Si el dominio de OfficeScan deseado no existe, lleve a cabo los siguientes pasos:

   a. Coloque el ratón sobre un dominio concreto de OfficeScan y haga clic en el icono de adición de dominio (➕).

b. Escriba el nombre del dominio en el cuadro de texto que se proporciona.

c. Haga clic en la marca de verificación junto al cuadro de texto. El dominio nuevo se agregará y se seleccionará automáticamente.

9. (Opcional) Active **Duplicar la estructura de Active Directory en el árbol de agentes de OfficeScan**. Esta opción duplica la jerarquía de los dominios de Active Directory seleccionados en el dominio de OfficeScan seleccionado.

10. Haga clic en **Guardar**.

Definir reglas de agrupación de agentes por dirección IP

Cree grupos de agente personalizados con direcciones IP de red para ordenar agentes en el árbol de OfficeScan agente. Esta función puede ayudar a los administradores a organizar la estructura del árbol de agentes de OfficeScan antes de que el agente se registre en el servidor de OfficeScan.

Procedimiento

1. Vaya a **Agentes** > **Agrupación de agentes**.
2. Vaya a la sección **Agrupación de agentes** y seleccione **Crear grupos de agentes personalizados para agentes de OfficeScan existentes**.
3. Vaya a la sección **Agrupación automática de agentes**.
4. Haga clic en **Agregar** y, a continuación, seleccione **Dirección IP**.

   Aparecerá una nueva pantalla.
5. Seleccione **Permitir agrupación**.
6. Especificar un nombre para la agrupación.
7. Especifique una de las siguientes opciones:
   - Una única dirección IPv4 o IPv6
   - Un intervalo de direcciones IPv4

- Un prefijo y una longitud IPv6

Nota

Si las direcciones IPv4 e IPv6 de un agente de doble pila pertenecen a dos grupos de agentes independientes, el agente se incluirá en el grupo IPv6. Si IPv6 está desactivada en el equipo host del agente, el agente se moverá al grupo IPv4.

8. Seleccione el dominio de OfficeScan al que se asignan la dirección IP o los rangos de dirección IP. Si el dominio no existe, realice lo siguiente::

   a. Pase el ratón por cualquier parte del árbol de agentes y haga clic en el icono de agregar un dominio.

FIGURA 2-11. Icono Agregar un dominio

   b. Escriba el dominio en el cuadro de texto que se proporciona.

   c. Haga clic en la marca de verificación junto al cuadro de texto. El dominio nuevo se agregará y se seleccionará automáticamente.

9. Haga clic en **Guardar**.

Tareas de agrupación de agentes

Puede realizar las tareas siguientes cuando se agrupan agentes en dominios:

- Añadir un dominio: Consulte *Añadir un dominio en la página 2-68* para obtener más información.
- Eliminar un dominio o un agente. Consulte *Eliminar un dominio o un agente en la página 2-68* para obtener más información.

- Cambiar el nombre de un dominio: Consulte *Cambiar el nombre de un dominio en la página 2-69* para obtener más información.
- Mover un agente a otro dominio o a otro servidor de OfficeScan. Consulte *Mover agentes de OfficeScan a otro dominio o servidor de OfficeScan en la página 2-70* para obtener más información.

Añadir un dominio

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. Haga clic en **Administrar árbol de agentes** > **Agregar un dominio**.
3. Escriba un nombre para el dominio que desea agregar.
4. Haga clic en **Agregar**.

   El nuevo dominio aparecerá en el árbol de agentes.
5. (Opcional) Cree subdominios.
   a. Seleccione el dominio primario.
   b. Haga clic en **Administrar árbol de agentes** > **Agregar un dominio**.
   c. Escriba el nombre de subdominio.

Eliminar un dominio o un agente

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, seleccione:
   - Uno o varios dominios
   - Uno, varios o todos los agentes de un dominio

3. Haga clic en **Administrar árbol de agentes** > **Eliminar dominio/agente**.

4. Para eliminar un dominio vacío, haga clic en **Eliminar dominio/agente**. Si el dominio contiene agentes y hace clic en **Eliminar dominio/agente**, el servidor de OfficeScan volverá a crear el dominio y agrupará a todos los agentes en ese dominio la siguiente vez que los agentes se conecten al servidor de OfficeScan. Puede realizar las siguientes tareas antes de eliminar el dominio:

   a. Mover los agentes a otros dominios. Para mover los agentes a otros dominios, arrástrelos y suelte los agentes en los dominios de destino.

   b. Eliminar todos los agentes.

5. Para eliminar un agente, haga clic en **Eliminar dominio/agente**.

Nota

Si borra el agente del árbol de agentes, no se quitará el Agente de OfficeScan del endpoint del agente. El Agente de OfficeScan todavía puede realizar las tareas independientes del servidor como, por ejemplo, la actualización de componentes. No obstante, el servidor no es consciente de la existencia del agente, por lo que no implementará configuraciones ni enviará notificaciones al agente.

Cambiar el nombre de un dominio

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. Seleccione un dominio en el árbol de agentes.
3. Haga clic en **Administrar árbol de agentes** > **Cambiar nombre del dominio**.
4. Escriba un nombre para el dominio.
5. Haga clic en **Cambiar nombre**.

   El nuevo nombre del dominio aparece en el árbol de agentes.

Mover agentes de OfficeScan a otro dominio o servidor de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, seleccione uno, varios o todos los agentes.
3. Haga clic en **Administrar árbol de agentes** > **Mover agente**.
4. Para mover agentes a otro dominio:
   - Seleccione **Mover los agentes seleccionados a otro dominio**.
   - Seleccione el dominio.
   - (Opcional) Aplique la configuración del nuevo dominio a los agentes.

   Consejo

   También puede arrastrar y soltar para mover agentes a otro dominio del árbol de agentes.
5. Para mover agentes a otro servidor de OfficeScan:
   - Seleccione **Mover los agentes seleccionados a otro servidor de OfficeScan**.
   - Escriba el nombre del servidor o la dirección IPv4/IPv6 y el número de puerto HTTP.
6. Haga clic en **Mover**.

Capítulo 3

Introducción a la protección de datos

En este capítulo se describe cómo instalar y activar el módulo de Protección de datos.

Los temas que se incluyen son:

- *Instalación de la protección de datos en la página 3-2*
- *Licencia de protección de datos en la página 3-4*
- *Implementación de la protección de datos en los agentes de OfficeScan en la página 3-6*
- *Carpeta forense y base de datos de DLP en la página 3-9*
- *Desinstalación de la protección de datos en la página 3-15*

Instalación de la protección de datos

El módulo de protección de datos incluye las siguientes funciones:

- **Prevención de pérdida de datos (DLP)**: evita la transmisión no autorizada de activos digitales.
- **Control de dispositivos**: Regula el acceso a los dispositivos externos

Nota

OfficeScan incorpora la función lista para usarse Control de dispositivos, la cual regula el acceso a dispositivos de uso frecuente, tales como dispositivos USB de almacenamiento. La función Control de dispositivos, que forma parte del módulo de protección de datos, amplía el rango de dispositivos supervisados. Para obtener una lista de los dispositivos supervisados, consulte *Control de dispositivos en la página 10-2*.

La prevención de pérdida de datos y el Control de dispositivos son funciones nativas de OfficeScan, pero tienen licencias individuales. Después de instalar el servidor de OfficeScan, estas funciones estarán disponibles, pero no se podrán utilizar ni implementar en agentes. La instalación de la protección de datos implica la descarga de un archivo desde el servidor de ActiveUpdate o desde una fuente de actualización personalizada, si se ha configurado alguna. Cuando dicho archivo se haya incorporado al servidor de OfficeScan, podrá activar la licencia de protección de datos con el fin de activar toda la funcionalidad de sus características. La instalación y la activación se realizan desde **Plug-in Manager**.

Importante

No es necesario que instale el módulo de Protección de datos si el software de prevención de pérdida de datos independiente de Trend Micro ya está instalado y ejecutándose en Endpoints.

Instalación de la protección de datos

Procedimiento

1. Abra la consola Web de OfficeScan y haga clic en **Complementos** en el menú principal.

2. En la pantalla de **Plug-in Manager**, vaya a la sección **Protección de datos de OfficeScan** y haga clic en **Descargar**.

   El tamaño del archivo que se va a descargar figura junto al botón **Descargar**.

   Plug-in Manager almacena el archivo descargado en <*Carpeta de instalación del servidor*>`\PCCSRV\Download\Product`.

   Nota

   Si Plug-in Manager no puede descargar el archivo, lo vuelve a intentar de forma automática una vez transcurridas 24 horas. Para activar manualmente OfficeScan Plug-in Manager con el fin de que descargue el archivo, reinicie el servicio Plug-in Manager desde Microsoft Management Console.

3. Supervise el progreso de descarga.

   Puede ignorar la pantalla durante la descarga.

   Si tiene problemas durante la descarga del archivo, compruebe los registros de actualización del servidor en la consola OfficeScan Web. En el menú principal, haga clic en **Registros** > **Actualización del servidor**.

   Después de que Plug-in Manager haya descargado el archivo, la protección de datos de OfficeScan se abrirá en una nueva pantalla.

   Nota

   Si no se visualiza la Protección de datos de OfficeScan, consulte los posibles motivos y sus soluciones en *Solución de problemas de Plug-in Manager en la página 17-13*.

4. Para instalar Protección de datos de OfficeScan al instante, haga clic en **Instalar ahora**, o para realizar la instalación más tarde, realice lo siguiente:

a. Haga clic en **Instalar más tarde**.

b. Abra la pantalla de **Plug-in Manager**.

c. Vaya a la sección **Protección de datos de OfficeScan** y haga clic en **Instalar**.

5. Lea el contrato de licencia y haga clic en **Aceptar** para aceptar las condiciones.

   Comienza la instalación.

6. Supervise el progreso de la instalación. Tras la instalación, se mostrará la versión de la protección de datos de OfficeScan.

Licencia de protección de datos

Visualice, active y renueve la licencia de protección de datos desde Plug-in Manager.

Solicite un código de activación a Trend Micro y, después, utilícelo para activar la licencia.

Activación de la licencia del Programa de complemento

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.

2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Administrar programa**.

   Aparecerá la pantalla **Nuevo código de activación de la licencia del producto**.

3. Escriba o copie y pegue el código de activación en los campos de texto.

4. Haga clic en **Guardar**.

Aparecerá la consola del complemento.

Ver y renovar la información sobre la licencia

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Administrar programa**.
3. Haga clic en **Ver información sobre la licencia** para ver información sobre la licencia actual en el sitio Web de Trend Micro.
4. Vea los siguientes detalles de la licencia en la pantalla que se abre.

Opción	Descripción
Estado	Muestra "Activada", "No activada" o "Caducada".
Versión	Muestra versión "Completa" o de "Evaluación". **Nota** La activación de las versiones completa y de evaluación se muestra solo como "Completa".
N.º de licencias	Muestra cuántos endpoints el programa de complemento puede administrar.
La licencia caduca el	Si el programa de complemento tiene varias licencias, se muestra la fecha de caducidad de mayor duración. Por ejemplo, si las fechas de caducidad son 31.12.11 y 30.06.11, aparecerá 31.12.11.
Código de activación	muestra el código de activación
Recordatorios	En función de la versión de licencia actual, el complemento muestra recordatorios acerca de la fecha de caducidad de la

OPCIÓN	DESCRIPCIÓN
	licencia durante el periodo de gracia (solo para las versiones completas) o en el momento en que expire.

Nota

La duración del periodo de gracia puede varía entre una zona y otra. Consulte a un representante de Trend Micro acerca del período de gracia de un programa de complemento.

5. Haga clic en **Actualizar información** para actualizar la pantalla con la información más reciente sobre la licencia.

6. Haga clic en **Nuevo código de activación** para abrir la pantalla **Nuevo código de activación de la licencia del producto**.

   Para conocer más detalles, consulte *Activación de la licencia del Programa de complemento en la página 3-4*.

Implementación de la protección de datos en los agentes de OfficeScan

Implemente el módulo de protección de datos en los Agentes de OfficeScan después de activar su licencia. Después de la implementación, los Agentes de OfficeScan comenzarán a utilizar la prevención de pérdida de datos y el control de dispositivos.

Importante

- Para evitar que afecte al rendimiento del sistema del equipo host, el módulo está desactivado de forma predeterminada en Windows Server 2003, Windows Server 2008 y Windows Server 2012. Si desea activar el módulo, supervise el rendimiento del sistema de forma constante y realice la acción necesaria cuando perciba una caída de dicho rendimiento.

  Puede activar o desactivar el módulo desde la consola Web. Para conocer más detalles, consulte *Servicios del agente de OfficeScan en la página 15-7*.

- Si el software de prevención de pérdida de datos de Trend Micro ya se encuentra en el endpoint, OfficeScan no lo sustituirá por el módulo de protección de datos.

- Los agentes en línea instalan el módulo de protección de datos inmediatamente. Los agentes independientes y desconectados instalarán el módulo cuando se vuelvan a conectar al servidor de OfficeScan.

- Los usuarios deben reiniciar los equipos para finalizar la instalación de los controladores de Prevención de pérdida de datos. Informe con antelación a los usuarios acerca del reinicio.

- Trend Micro recomienda activar el registro de depuración para que le ayude a solucionar problemas de implementación. Para conocer más detalles, consulte *Activar el registro de depuración del módulo de Protección de datos en la página 11-67*.

Implementación del módulo de protección de datos en los agentes de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, puede:

   - Hacer clic en el icono del dominio raíz ( ) para implementar el módulo en todos los agentes existentes y futuros.

   - Seleccione un dominio específico para implementar el módulo en todos los agentes existentes y futuros en el dominio.

- Seleccione un agente específico para implementar el módulo únicamente en ese agente.

3. Implemente el módulo de dos formas diferentes:

   - Haga clic en **Configuración** > **Configuración de DLP**.
   - Haga clic en **Configuración** > **Configuración de Control de dispositivos**.

   Nota

   Si realiza la implementación desde **Configuración** > **Configuración de DLP** y el módulo de protección de datos se ha implementado correctamente, se instalarán los controladores de la prevención de pérdida de datos. Si los controladores se instalan correctamente, se mostrará un mensaje para avisar a los usuarios de que deben reiniciar sus Endpoints para completar la instalación de los controladores.

   Si no aparece el mensaje, es posible que se hayan producido problemas durante la instalación de los controladores. Compruebe los registros de depuración, en el caso de que los haya activado, para obtener información detallada acerca de los problemas de instalación de los controladores.

4. Aparecerá un mensaje en que se le indicará el número de agentes que no han instalado el módulo. Haga clic en **Sí** para iniciar la implementación.

   Nota

   Si hace clic en **No** (o si el módulo no se ha implementado en uno o varios agentes por el motivo que sea), el mismo mensaje aparecerá cuando haga clic de nuevo en **Configuración** > **Configuración de DLP** o en **Configuración** > **Configuración del control de dispositivos**.

   Los Agentes de OfficeScan comenzarán a descargar el módulo desde el servidor.

5. Compruebe que el módulo se haya implementado en los agentes.

   a. Seleccione un dominio en el árbol de agentes.

   b. En la vista del árbol de agentes, seleccione **Vista de protección de datos** o **Ver todo**.

c. Compruebe la columna **Estado de la protección de datos**. El estado de la implementación puede ser cualquiera de los siguientes:

- **En funcionamiento**: El módulo se ha implementado correctamente y sus funciones se han activado.
- **Es necesario reiniciar**: Los controladores de la Prevención de pérdida de datos no se han instalado debido a que los usuarios no han reiniciado sus equipos. Si los controladores no están instalados, la prevención de pérdida de datos no funcionará.
- **Detenida**: el servicio del módulo no se ha iniciado o el endpoint de destino se ha apagado con normalidad. Para iniciar el servicio de protección de datos, vaya a **Agentes** > **Administración de agentes** > **Configuración** > **Configuración de servicios adicionales** y active los servicios de protección de datos.
- **No se puede instalar**: Se ha producido un problema al implementar el módulo en el agente. Es necesario volver a implementar el módulo desde el árbol de agentes.
- **No se puede instalar (ya existe la prevención de pérdida de datos)**: el software de prevención de pérdida de datos de Trend Micro ya se encuentra en el endpoint, OfficeScan no lo sustituirá por el módulo de protección de datos.
- **No instalado**: el módulo no se ha implementado en el agente. este estado aparece si elige no implementar el módulo en el agente o si el estado de este último durante la implementación es Desactivado o Independiente.

Carpeta forense y base de datos de DLP

Después de que se produzca un incidente de la prevención de pérdida de datos, OfficeScan registra los detalles del incidente en una base de datos forense especializada. OfficeScan también crea un archivo cifrado que contiene una copia de la información confidencial que desencadenó el incidente y genera un valor hash para poder verificarlo y garantizar la integridad de los datos confidenciales. OfficeScan crea los archivos

forenses cifrados en el equipo del agente y después los carga en una ubicación específica del servidor.

Importante

- Los archivos forenses cifrados contienen datos muy confidenciales y los administradores deberían tener cuidado al otorgar acceso a estos archivos.
- OfficeScan se integra con Control Manager para ofrecer a los usuarios de Control Manager con las funciones de Revisor de incidentes de DLP o de Director de cumplimiento de DLP la capacidad de acceder a los datos de los archivos cifrados. Para obtener información sobre las funciones de DLP y el acceso a datos de archivos forenses en Control Manager, consulte el *Manual del administrador de Control Manager 6.0 revisión 2* o posterior.

Modificar la configuración de la carpeta y la base de datos forense

Los administradores pueden cambiar la ubicación y el programa de eliminación de la carpeta forense y el tamaño máximo de los archivos que los agentes pueden cargar modificando los archivos INI de OfficeScan.

¡ADVERTENCIA!

Cambiar la ubicación de la carpeta forense tras registrar incidentes de prevención de pérdida de datos puede provocar la desconexión de los datos de la base de datos y de la ubicación de los archivos forenses existentes. Trend Micro recomienda trasladar manualmente los archivos forenses existentes a la nueva carpeta forense después de modificar la ubicación de esta.

La siguiente tabla describe la configuración del servidor disponible en el archivo de la <*Carpeta de instalación del servidor*>`\PCCSRV\Private\ofcserver.ini` ubicado en el servidor de OfficeScan.

TABLA 3-1. La configuración del servidor de la carpeta forense en `PCCSRV\Private\ofcserver.ini`

OBJETIVO	CONFIGURACIÓN DE INI	VALORES
Permitir la ubicación de la carpeta forense definida por el usuario	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: desactivar (predeterminado) 1: activar
Configurar la ubicación de la carpeta forense definida por el usuario	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **Nota** • Los administradores deben activar la configuración `EnableUserDefinedUploadFolder` antes de que la prevención de pérdida de datos aplique esta configuración. • La ubicación predeterminada de la carpeta forense es: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\DLPForensicData` • La ubicación de la carpeta forense definida por el usuario debe ser una unidad física (interna o externa) en el equipo servidor. OfficeScan no es compatible con la asignación de ubicaciones de unidades de red.	Valor predeterminado: <Sustituya este valor con la ruta de carpeta definida por el cliente. Por ejemplo: C:\VolumeData\OfficeScanDlpForensicData>. Valor definido por el usuario: debe ser la ubicación física de una unidad del equipo servidor.
Activar la purga de los archivos de datos forenses	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: desactivar 1: activar (predeterminado)

OBJETIVO	CONFIGURACIÓN DE INI	VALORES
Configurar la frecuencia de tiempo de la comprobación de la purga de archivos de datos forenses	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **Nota** • Los administradores deben activar la configuración `ForensicDataPurgeEnable` antes de que OfficeScan aplique esta configuración. • OfficeScan solo elimina los archivos de datos que han superado la fecha de caducidad especificada en la configuración `ForensicDataExpiredPeriodInDays`.	1: mensualmente, el primer día del mes a las 00:00 2: semanalmente (predeterminado), cada domingo a las 00:00 3: diariamente, cada día a las 00:00 4: cada hora a las HH:00
Configurar la cantidad de tiempo para almacenar archivos de datos forenses en el servidor	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	Valor predeterminado (en días): 180 Valor mínimo: 1 Valor máximo: 3.650
Configurar la frecuencia de tiempo de la comprobación de espacio en disco de los archivos forenses	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **Nota** Si el espacio en disco disponible en la carpeta de datos forenses es menor que el valor configurado para la configuración `InformUploadOnDiskFreeSpaceInGb`, OfficeScan registra un registro de evento en la consola Web.	Valor predeterminado (en segundos): 5

OBJETIVO	CONFIGURACIÓN DE INI	VALORES
Configurar la frecuencia de carga de la comprobación de espacio en disco de los archivos forenses	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **Nota** Si el espacio en disco disponible en la carpeta de datos forenses es menor que el valor configurado para la configuración `InformUploadOnDiskFreeSpaceInGb`, OfficeScan registra un registro de evento en la consola Web.	Valor predeterminado (en número de archivos): 200
Configurar el valor del espacio en disco mínimo que desencadena una notificación de espacio en disco limitado	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **Nota** Si el espacio en disco disponible en la carpeta de datos forenses es menor que el valor configurado, OfficeScan registra un registro de evento en la consola Web.	Valor predeterminado (en GB): 10
Configuración del espacio mínimo disponible para cargar archivos de datos forenses desde los agentes	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **Nota** Si el espacio en disco disponible en la carpeta de datos forenses es menor que el valor configurado, los agentes de OfficeScan no cargarán los archivos de datos forenses en el servidor y OfficeScan registrará un registro de suceso en la consola Web.	Valor predeterminado (en GB): 1

La siguiente tabla describe la configuración disponible del Agente de OfficeScan en el archivo <*Carpeta de instalación del servidor*>`\PCCSRV\ofcscan.ini` que se encuentra en el servidor de OfficeScan.

TABLA 3-2. Configuración del agente del archivo forense en `PCCSRV\ofcscan.ini`

OBJETIVO	CONFIGURACIÓN DE INI	VALORES
Activar la carga de los archivos de datos forenses en el servidor	`UploadForensicDataEnable`	0: desactivar 1: activar (predeterminado)
Configuración del tamaño máximo de los archivos que el Agente de OfficeScan carga en el servidor	`UploadForensicDataSizeLimitInMb` **Nota** El Agente de OfficeScan solo envía archivos que son menores que este tamaño al servidor.	Valor predeterminado (en MB): 10 Valor mínimo: 1 Valor máximo: 2048
Configuración de la cantidad de tiempo para almacenar archivos de datos forenses en el Agente de OfficeScan	`ForensicDataKeepDays` **Nota** El Agente de OfficeScan solo elimina los archivos de datos forenses que han pasado la fecha de caducidad especificada cada día a las 11:00 am.	Valor predeterminado (en días): 180 Valor mínimo: 1 Valor máximo: 3.650
Configuración de la frecuencia con la que el Agente de OfficeScan comprueba la conectividad con el servidor	`ForensicDataDelayUploadFrequenceInMinutes` **Nota** Los Agentes de OfficeScan que no pueden subir archivos forenses al servidor automáticamente intentan reenviar los archivos mediante el intervalo de tiempo especificado.	Valor predeterminado (en minutos): 5 Valor mínimo: 5 Valor máximo: 60

Crear una copia de seguridad de datos forenses

Dependiendo de la política de seguridad de la empresa, la cantidad de tiempo necesaria para almacenar la información de los datos forenses puede variar enormemente. Con el fin de liberar espacio en el disco del servidor, Trend Micro recomienda realizar una copia de seguridad manual de los datos de la carpeta forense y de la base de datos forense.

Procedimiento

1. Vaya a la ubicación de la carpeta de datos forenses en el servidor.
   - Ubicación predeterminada: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\DLPForensicData`
   - Para localizar la ubicación de la carpeta forense personalizada, consulte *Configurar la ubicación de la carpeta forense definida por el usuario en la página 3-11*.
2. Copie la carpeta a una nueva ubicación.
3. Para crear una copia de seguridad manual de la base de datos de datos forenses, desplácese a <*Carpeta de instalación del servidor*>`\PCCSRV\Private`.
4. Copie el archivo `DLPForensicDataTracker.db` a una nueva ubicación.

Desinstalación de la protección de datos

Si desinstala el módulo de protección de datos desde Plug-in Manager:

- Todas las configuraciones, opciones y registros de la prevención de pérdida de datos se eliminan del servidor de OfficeScan.
- Se eliminan del servidor todos los parámetros y configuraciones de Control de dispositivos que haya proporcionado el módulo de protección de datos.
- Se elimina el módulo de protección de datos de los agentes. Los endpoints del agente se deben reiniciar para quitar la protección de datos por completo.
- Las políticas de prevención de pérdida de datos ya no se aplicarán en los agentes.

- La función Control de dispositivos deja de supervisar el acceso a los siguientes dispositivos:
  - Adaptadores Bluetooth
  - Puertos COM y LPT
  - Interfaz IEEE 1394
  - Dispositivos de imagen
  - Dispositivos infrarrojo
  - Módems
  - Tarjeta PCMCIA
  - Llave de impresión de pantalla
  - NIC inalámbricas

Vuelva a instalar el módulo en Protección de datos en cualquier momento. Después de volver a instalarlo, active la licencia mediante un código de activación válido.

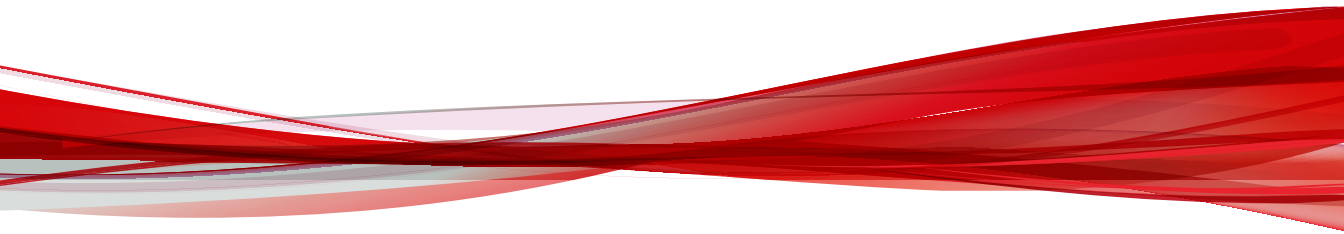
Desinstalar la protección de datos de Plug-in Manager

Procedimiento

1. Abra la consola Web de OfficeScan y haga clic en **Complementos** en el menú principal.
2. En la pantalla de **Plug-in Manager**, vaya a la sección **Protección de datos de OfficeScan** y haga clic en **Desinstalar**.
3. Supervise el progreso de desinstalación. Puede ignorar la pantalla durante la desinstalación.
4. Actualice la pantalla de **Plug-in Manager** después de la desinstalación. La protección de datos de OfficeScan estará disponible de nuevo para su instalación.

Parte II

Protección de los agentes de OfficeScan



Capítulo 4

Uso de la Smart Protection de Trend Micro

En este capítulo se tratan las soluciones de Smart Protection de Trend Micro y se describe cómo configurar el entorno necesario para utilizar estas soluciones.

Los temas que se incluyen son:

- *Acerca de la Smart Protection de Trend Micro en la página 4-2*
- *Servicios de Smart Protection en la página 4-3*
- *Fuentes de Smart Protection en la página 4-6*
- *Archivos de patrones de Smart Protection en la página 4-8*
- *Configuración de los Servicios de Smart Protection en la página 4-13*
- *Uso de los Servicios de Smart Protection en la página 4-33*

Acerca de la Smart Protection de Trend Micro

Trend Micro™ Smart Protection es una infraestructura de seguridad de contenidos de clientes por Internet de última generación diseñada para proteger a los clientes de los riesgos de seguridad y las amenazas Web. Cuenta con soluciones tanto locales como alojadas con el fin de proteger a los usuarios, independientemente de si se encuentran en la red, en casa o en movimiento, mediante agentes ligeros para acceder a la correlación única en la nube de correo electrónico y tecnologías de reputación Web y de File Reputation, así como a las bases de datos de amenazas. La protección de los clientes se actualiza automáticamente y se refuerza a medida que van accediendo a la red más productos, servicios y usuarios, creando un servicio de protección de supervisión de entorno en tiempo real.

Mediante la incorporación de las tecnologías de reputación, exploración y correlación en la red, las soluciones de Smart Protection de Trend Micro reducen la dependencia en descargas de archivos de patrones convencionales y suprimen los atrasos que comúnmente están asociados a las actualizaciones de los equipos de sobremesa.

Una nueva solución necesaria

En el enfoque de gestión de amenazas basada en archivos actual, la mayor parte de los patrones (o definiciones) que se necesitan para proteger los endpoints generalmente se envían según una programación. Estos patrones se envían por lotes desde Trend Micro a los agentes. Cuando se recibe una nueva actualización, el software de prevención de virus/malware del agente vuelve a cargar el lote de definiciones de patrones de los riesgos de virus/malware nuevos en la memoria. Si aparece un riesgo de virus/malware nuevo, el patrón se debe volver a actualizar de forma parcial o completa, y se vuelve a cargar en el agente para garantizar la protección.

A medida que ha ido pasando el tiempo, ha aumentado significativamente el volumen de amenazas emergentes exclusivas. Se espera que este volumen de amenazas siga creciendo casi exponencialmente en los próximos años. Esto es una tasa de crecimiento que supera con creces el volumen de los riesgos de seguridad conocidos actualmente. Aún más, el volumen de los riesgos de seguridad representa un nuevo tipo de riesgo de seguridad. El volumen de los riesgos de seguridad puede tener un impacto negativo en el rendimiento de los servidores y estaciones de trabajo, en el uso del ancho de banda de red y, en general, en el tiempo que se tarda en proporcionar una protección de calidad, o "tiempo para la protección".

Trend Micro ha sido pionero en un enfoque nuevo para gestionar el volumen de amenazas que se centra en hacer a los clientes de Trend Micro inmunes a esta amenaza que representa el volumen de virus o malware. La tecnología y la arquitectura que se utiliza en este esfuerzo pionero aprovecha la tecnología de redireccionamiento del almacenamiento de firmas y patrones de virus/malware a Internet. Mediante el redireccionamiento del almacenamiento de estas firmas de virus o malware a Internet, Trend Micro puede proporcionar mejor protección a sus clientes frente al futuro volumen de riesgos de seguridad emergentes.

Servicios de Smart Protection

La Smart Protection incluye servicios que ofrecen firmas antimalware, reputaciones Web y bases de datos de amenazas que hay almacenadas en la red.

Los Servicios de Smart Protection incluyen:

- **Servicios de File Reputation**: los servicios de File Reputation redireccionan un gran número de firmas antimalware almacenadas anteriormente en los equipos del agente a los orígenes de Smart Protection.

  Para conocer más detalles, consulte *Servicios de File Reputation en la página 4-3*.

- **Servicios de Reputación Web**: los Servicios de Reputación Web permiten que los orígenes de Smart Protection locales alojen datos de reputación de direcciones URL que solo Trend Microalojaba anteriormente. Ambas tecnologías garantizan un menor consumo de ancho de banda al actualizar patrones o verificar la validez de una URL.

  Para conocer más detalles, consulte *Servicios de reputación Web en la página 4-4*.

- **Smart Feedback**: Trend Micro continúa la recopilación de información que los productos de Trend Micro envían de forma anónima desde cualquier parte del mundo para determinar cada nueva amenaza de manera proactiva.

  Para conocer más detalles, consulte *Comentarios inteligentes en la página 4-5*.

Servicios de File Reputation

Los Servicios de File Reputation comprueban la reputación de cada archivo en una extensa base de datos en la nube. Como la información sobre malware se almacena en

red, los usuarios pueden acceder a ella de forma inmediata. Las redes con contenido de alto rendimiento y los servidores locales guardados en caché garantizan una latencia mínima durante el proceso de comprobación. La arquitectura nube-agente ofrece una protección más inmediata y elimina la carga de la implementación de patrones, además de reducir de forma significativa el tamaño global del agente.

Los agentes se deben encontrar en el modo Smart Scan para utilizar los servicios de File Reputation. Estos agentes se denominan agentes Smart Scan en este documento. Los agentes que no se encuentran en el modo Smart Scan no utilizan los servicios de File Reputation y se denominan agentes de exploración convencional. Los administradores de OfficeScan pueden configurar todos o varios de los agentes para que estén en modo Smart Scan.

Servicios de reputación Web

Con una de las bases de datos de dominios y reputaciones más grandes del mundo, la tecnología de reputación Web de Trend Micro realiza un seguimiento de la credibilidad de los dominios Web mediante la asignación de un resultado de reputación basado en factores como la antigüedad del sitio Web, los cambios en la ubicación histórica y las indicaciones de actividades sospechosas descubiertas mediante el análisis de comportamientos malintencionados. A continuación, la reputación Web continuará la exploración de los sitios y el bloqueo del acceso de los usuarios a los sitios infectados. Las funciones de reputación Web garantizan que las páginas a las que accede el usuario son seguras y no contienen amenazas Web, tales como malware, spyware y estafas de phishing que tienen como objetivo engañar al usuario para que proporcione información personal. Para aumentar la precisión y reducir los falsos positivos, la tecnología de reputación Web de Trend Micro asigna puntuaciones de reputación a páginas específicas dentro de los sitios en lugar de clasificar o bloquear sitios completos, ya que a veces son sólo partes de estos los que están afectados y las reputaciones pueden cambiar de forma dinámica con el tiempo.

Los Agentes de OfficeScan sujetos a las políticas de reputación Web utilizan los servicios de reputación Web. Los administradores de OfficeScan pueden aplicar a todos o a varios de los agentes las políticas de reputación Web.

Comentarios inteligentes

Trend Micro Smart Feedback proporciona una comunicación continua entre los productos Trend Micro y los centros de investigación de amenazas y sus tecnologías, que ofrecen asistencia 24 horas al día, los 7 días de la semana. Cada nueva amenaza identificada mediante cada una de las verificaciones rutinarias de la reputación del cliente actualiza automáticamente todas las bases de datos de amenazas de Trend Micro, lo que bloquea cualquier encuentro posterior del cliente con dicha amenaza.

Mediante el procesamiento continuo de la inteligencia de la amenaza, recopilada a través de su extensa red global de clientes y socios, Trend Micro ofrece protección automática en tiempo real frente a las amenazas más recientes y proporciona la seguridad "mejor juntos", esto es como un tipo de vigilancia vecinal automatizado que involucra a la comunidad en la protección de los demás. La privacidad de la información personal o empresarial de un cliente está siempre protegida ya que la información recopilada sobre las amenazas está basada en la reputación de la fuente de comunicación, no en el contenido de la comunicación específica.

Ejemplos de la información enviada a Trend Micro son:

- Sumas de comprobación de archivos
- Sitios Web a los que se ha accedido
- Información de archivos, incluido el tamaño y las rutas
- Nombres de archivos ejecutables

En cualquier momento puede poner fin a su participación en el programa desde la consola Web.

Consejo

No es necesario que participe con Smart Feedback para proteger sus endpoints. La participación es opcional y puede eliminar esta opción en cualquier momento. Trend Micro le recomienda que participe con Smart Feedback para ayudar a ofrecer una mayor protección total a todos los clientes de Trend Micro.

Para obtener más información sobre Smart Protection Network, visite el sitio:

http://www.trendmicro.es/tecnologia-innovacion/nuestra-tecnologia/smart-protection-network/

Fuentes de Smart Protection

Trend Micro proporciona Servicios de File Reputation y Servicios de Reputación Web a OfficeScan y a las fuentes de Smart Protection.

Los orígenes de Smart Protection alojan la mayoría de las definiciones de patrón de virus/malware para ofrecer los servicios de File Reputation, mientras que los Agentes de OfficeScan alojan el resto de definiciones. Un agente envía consultas de exploración a los orígenes de Smart Protection si sus definiciones de patrón no pueden determinar el riesgo del archivo. Las fuentes de Smart Protection determinan el riesgo valiéndose de la información de identificación.

Las fuentes de Smart Protection proporcionan Servicios de Reputación Web alojando los datos de reputación Web disponibles anteriormente solo a través de los servidores alojados por Trend Micro. Un agente envía consultas de reputación Web a los orígenes de Smart Protection para comprobar la reputación de los sitios Web a los que el usuario intenta acceder. El agente correlaciona la reputación de un sitio Web con la política de reputación Web específica que se aplica en el endpoint para determinar si se permite o se bloquea el acceso al sitio.

El origen de Smart Protection al que se conecta el agente depende de la ubicación del agente. Los Agentes se pueden conectar a Trend Micro Smart Protection Network o Smart Protection Server.

Red de Protección Inteligente de™ Trend Micro™

Trend Micro™ Smart Protection Network™ es una infraestructura de seguridad de contenidos de clientes por Internet de próxima generación diseñada para proteger a los clientes frente a riesgos de seguridad y las amenazas Web. Cuenta con soluciones tanto locales como alojadas por Trend Micro para proteger a los usuarios, independientemente de si se encuentran en la red, en casa o en movimiento. Smart Protection Network utiliza agentes para acceder a la correlación única de correo electrónico por Internet y a las tecnologías File Reputation y de reputación Web, así como a las bases de datos de amenazas. La protección de los clientes se actualiza automáticamente y se refuerza a

medida que van accediendo a la red más productos, servicios y usuarios, creando un servicio de protección de supervisión de entorno en tiempo real.

Para obtener más información sobre Smart Protection Network, visite el sitio:

http://www.trendmicro.es/tecnologia-innovacion/nuestra-tecnologia/smart-protection-network/

Smart Protection Server

Los Smart Protection Servers están disponibles para los usuarios que tengan acceso a la red de empresa local. Los servidores locales localizan servicios de Smart Protection para optimizar la eficacia de las operaciones de red de empresa.

Hay dos tipos de Smart Protection Servers:

- **Smart Protection Server integrado**: el programa OfficeScan Setup incluye un servidor de Smart Protection Server integrado que se instala en el mismo endpoint en el que se instala el servidor de OfficeScan. Tras la instalación, defina la configuración de este servidor desde la consola OfficeScan Web. El servidor integrado está diseñado para implementaciones de OfficeScan a pequeña escala. Para implementaciones de mayor tamaño, se requiere un servidor de Smart Protection Server independiente.
- **Servidor de Smart Protection Server independiente**: un servidor de Smart Protection Server independiente se instala en un servidor VMware o Hyper-V. El servidor independiente cuenta con una consola de administración independiente y no se controla desde la consola OfficeScan Web.

Comparación de las fuentes de Smart Protection

En la siguiente tabla figuran las diferencias entre la Smart Protection Network y el Smart Protection Server.

TABLA 4-1. Comparación de las fuentes de Smart Protection

REFERENCIAS DE LA COMPARACIÓN	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Disponibilidad	Se encuentra disponible para los agentes internos, que son agentes que reúnen los criterios de ubicación especificados en la consola Web de OfficeScan.	Se encuentra disponible principalmente para los agentes externos, que son agentes que no reúnen los criterios de ubicación especificados en la consola Web de OfficeScan.
Objetivo	Está diseñado con el fin de localizar los Servicios de Smart Protection en la red de la empresa y mejorar así el rendimiento.	Una infraestructura basada en Internet de alcance global que proporciona servicios de Smart Protection Services a los agentes que no tienen acceso inmediato a la red empresarial.
Administración	Los administradores de OfficeScan instalan y gestionan estas fuentes de Smart Protection	Trend Micro mantiene esta fuente
Fuente de actualización del patrón	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Protocolos de conexión de los agentes	HTTP y HTTPS	HTTPS

Archivos de patrones de Smart Protection

Los archivos de Smart Protection Pattern se utilizan para los servicios de File Reputation y de reputación Web. Trend Micro publica estos patrones a través de Trend Micro ActiveUpdate Server.

Smart Scan Agent Pattern

Smart Scan Agent Pattern se actualiza a diario y lo descarga el origen de actualización de los agentes de OfficeScan (el servidor de OfficeScan o un origen de actualización personalizado). A continuación, el origen de actualización implementa el patrón en los agentes Smart Scan.

Nota

Los agentes Smart Scan son Agentes de OfficeScan que los administradores han configurado para utilizar los servicios de File Reputation. Los agentes que no utilizan los servicios de File Reputation se denominan agentes de exploración convencional.

Los agentes Smart Scan utilizan Smart Scan Agent Pattern al realizar las exploraciones en busca de riesgos de seguridad. Si el patrón no puede determinar el riesgo del archivo, se utiliza otro patrón llamado Smart Scan Pattern.

Smart Scan Pattern

Smart Scan Pattern se actualiza cada hora y lo descargan las fuentes de Smart Protection. Los agentes Smart Scan no descargan el Smart Scan Pattern. Los agentes envían consultas de exploración a los orígenes de Smart Protection para comprobar las posibles amenazas contra Smart Scan Pattern.

Lista de bloqueo Web

Los orígenes de Smart Protection descargan la Lista de bloqueo Web. Los Agentes de OfficeScan sujetos a políticas de reputación Web no descargan la lista de bloqueo Web.

Nota

Los administradores pueden aplicar las políticas de reputación Web a todos o a varios agentes.

Los agentes sujetos a políticas de reputación Web envían consultas de reputación Web a un origen de Smart Protection para verificar la reputación de un sitio Web en la lista de

bloqueo Web. El agente correlaciona los datos de reputación recibidos del origen de Smart Protection con la política de reputación Web que se aplica en el endpoint. En función de la política, el agente permitirá o bloqueará el acceso al sitio.

Proceso de actualización de patrones de Smart Protection

Las actualizaciones de los patrones de Smart Protection parten de Trend Micro ActiveUpdate Server.

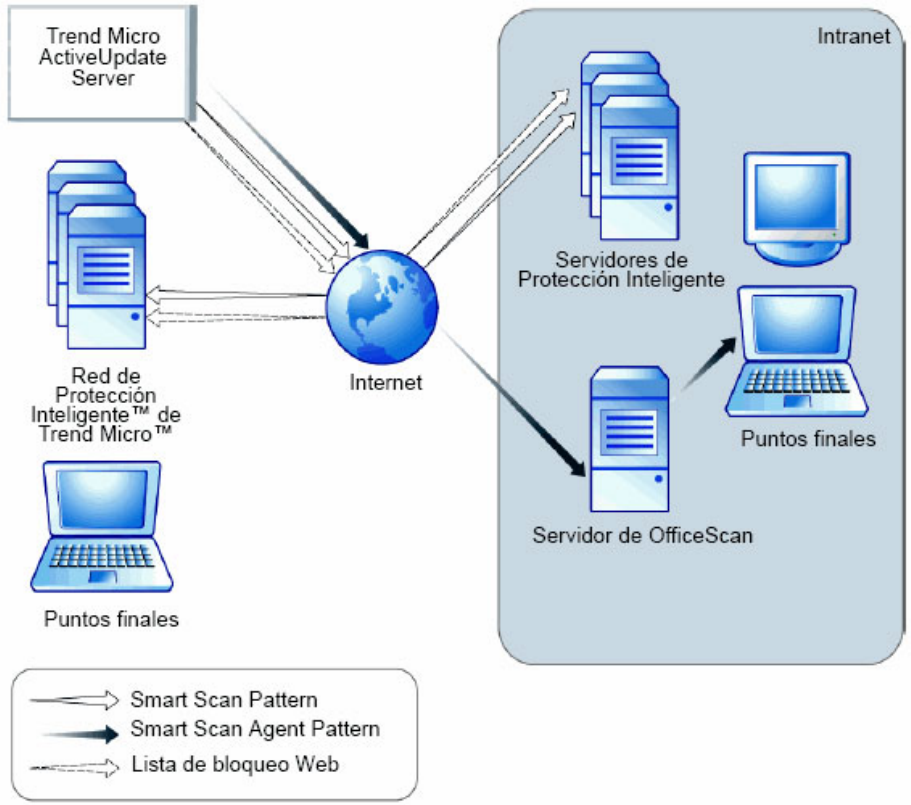


FIGURA 4-1. Proceso de actualización de patrones

Uso de patrones de Smart Protection

El Agente de OfficeScan utiliza Smart Scan Agent Pattern para explorar en busca de riesgos de seguridad y solo realiza consultas a Smart Scan Pattern si este no puede determinar el riesgo de un archivo. El agente consulta la lista de bloqueo Web cuando un usuario intenta acceder a un sitio Web. La tecnología de filtrado avanzada permite al agente "almacenar en caché" los resultados de la consulta. Esto elimina la necesidad de enviar la misma consulta más de una vez.

Los agentes que se encuentran actualmente en la intranet se pueden conectar al servidor de Smart Protection Server para realizar una consulta en Smart Scan Pattern o en la lista de bloqueo Web. Se requiere conexión de red para conectar con el Smart Protection Server. Si se ha configurado más de un Smart Protection Server, los administradores pueden determinar la prioridad de conexión.

Consejo

Instale varios Smart Protection Servers para garantizar una protección continuada en el caso de que no esté disponible la conexión a un Smart Protection Server.

Los agentes que no están actualmente en la intranet se pueden conectar a Trend Micro Smart Protection Network para realizar consultas. Se requiere conexión a Internet para establecer conexión con la Red de Smart Protection.

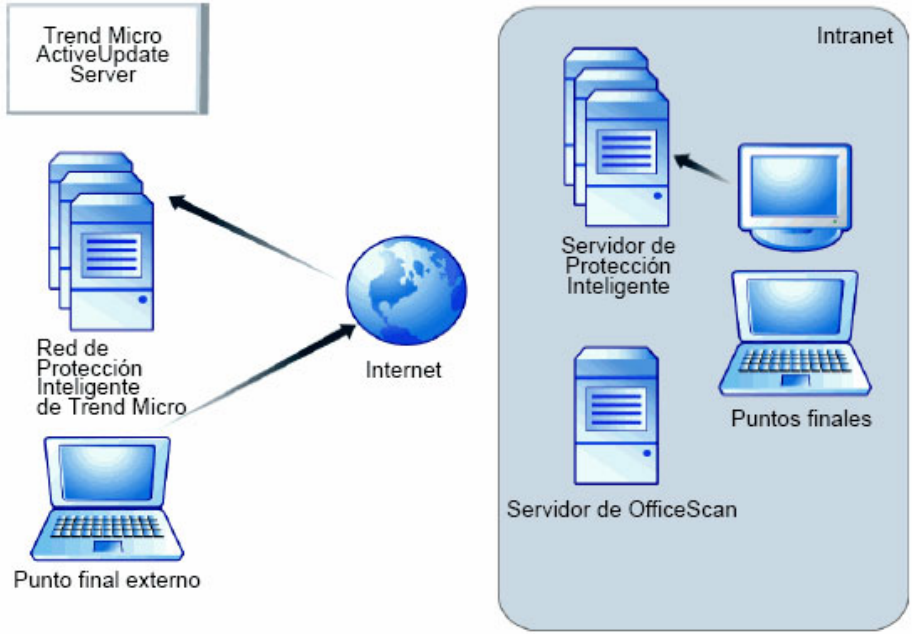


FIGURA 4-2. Proceso de consulta

Los agentes sin acceso a la red o a Internet también pueden beneficiarse de la protección proporcionada tanto por Smart Scan Agent Pattern como por la caché que contiene los resultados de las consultas anteriores. La protección solo se reduce cuando se necesita una nueva consulta y el agente, tras varios intentos, no puede alcanzar ningún origen de Smart Protection. En este caso, el agente marca el archivo para que sea comprobado y permite el acceso a este temporalmente. Cuando se restaure la conexión con una fuente de Smart Protection, todos los archivos marcados se volverán a explorar. Entonces, se realizará una acción de exploración en los archivos que se confirmen como amenazas.

En la siguiente tabla se resume el alcance de la protección en función de la ubicación del agente.

TABLA 4-2. Comportamientos de protección basados en la ubicación

LOCALIZACIÓN	ARCHIVO DE PATRONES Y COMPORTAMIENTO DE CONSULTA
Para acceder a la intranet	• **Archivo de patrones**: los agentes descargan el archivo de Smart Scan Agent Pattern del servidor de OfficeScan o de un origen de actualización personalizado. • **Consultas de File Reputation y de reputación Web**: los agentes se conectan al servidor de Smart Protection Server para realizar consultas.
Sin acceso a una intranet pero con conexión a la Red de Smart Protection	• **Archivo de patrones**: los agentes no descargan el archivo de Smart Scan Agent Pattern más reciente a menos que una conexión al servidor de OfficeScan o a un origen de actualización personalizado esté disponible. • **Consultas de File Reputation y de reputación Web**: los agentes se conectan a Smart Protection Network para realizar consultas.
Sin acceso a la intranet y sin conexión a la Red de Smart Protection	• **Archivo de patrones**: los agentes no descargan el archivo de Smart Scan Agent Pattern más reciente a menos que una conexión al servidor de OfficeScan o a un origen de actualización personalizado esté disponible. • **Consultas de File Reputation y de reputación Web**: los agentes no reciben los resultados de las consultas, por lo que deben confiar en Smart Scan Agent Pattern y en la caché que contiene los resultados de las consultas anteriores.

Configuración de los Servicios de Smart Protection

Antes de que los agentes puedan utilizar los servicios de File Reputation y de reputación Web, asegúrese de que el entorno de Smart Protection se ha configurado correctamente. Compruebe los siguientes aspectos:

- *Instalación del Smart Protection Server en la página 4-14*
- *Administración del Smart Protection Server Integrado en la página 4-19*
- *Lista de fuentes de Smart Protection en la página 4-23*
- *Configuración del proxy de conexión del agente en la página 4-32*
- *Instalaciones de Trend Micro Network VirusWall en la página 4-32*

Instalación del Smart Protection Server

Puede instalar el servidor de Smart Protection Server integrado o independiente si el número de agentes es igual o inferior a 1000. Instale un servidor de Smart Protection Server independiente si hay más de 1000 agentes.

Trend Micro recomienda instalar varios servidores de Smart Protection Server para las conmutaciones por error. Los que no pueden conectarse a un servidor determinado intentarán conectarse al resto de servidores que ha instalado.

El servidor integrado y el servidor de OfficeScan se ejecutan en el mismo endpoint, por lo que el rendimiento del endpoint puede reducirse significativamente en los dos servidores cuando haya mucho tráfico. Considere la opción de utilizar un servidor de Smart Protection Server independiente como el origen de Smart Protection principal para los agentes y el servidor integrado como una copia de seguridad.

Instalación del Smart Protection Server independiente

Para obtener instrucciones acerca de la instalación y la administración del Smart Protection Server independiente, consulte el *Manual de instalación y actualización del Smart Protection Server*.

Instalación de Smart Protection Server Integrado

Si instaló el servidor integrado durante la instalación del servidor de OfficeScan:

- Active el servidor integrado y configure los parámetros del servidor. Para conocer más detalles, consulte *Administración del Smart Protection Server Integrado en la página 4-19*.

- Si el mismo equipo contiene el servidor integrado y el Agente de OfficeScan, considere la opción de desactivar el cortafuegos de OfficeScan. El cortafuegos de OfficeScan está diseñado para utilizarse en endpoints de agentes y, por tanto, puede afectar al rendimiento si se usa en servidores. Para obtener instrucciones sobre cómo desactivar el cortafuegos, consulte *Activar o desactivar OfficeScan Firewall en la página 13-6*.

Nota

Tenga en cuenta las consecuencias si se desactiva el cortafuegos y asegúrese de que esta acción se ajusta a sus previsiones en materia de seguridad.

Consejo

Instale el Smart Protection Server integrado una vez que haya finalizado la instalación de OfficeScan mediante la *Herramienta Smart Protection Server Integrado en la página 4-15*.

Herramienta Smart Protection Server Integrado

La herramienta integrada Smart Protection de Trend Micro ayuda a los administradores a instalar o desinstalar el servidor de Smart Protection Server integrado una vez que la instalación del servidor de OfficeScan ha finalizado. La versión actual de OfficeScan no permite a los administradores instalar/eliminar un Smart Protection Server integrado una vez que la instalación del servidor de OfficeScan ha finalizado. Esta herramienta mejora la flexibilidad de las funciones de instalación de las versiones anteriores de OfficeScan.

Procedimiento

1. Abra una ventana de línea de comandos y vaya al directorio <*carpeta de instalación del servidor*>\PCCSRV\Admin\Utility\ISPSInstaller donde se encuentra `ISPSInstaller.exe`.

2. Ejecute `ISPSInstaller.exe` mediante uno de los siguientes comandos:

TABLA 4-3. Opciones del programa instalador

COMANDO	DESCRIPCIÓN
`ISPSInstaller.exe /i`	Instala el Smart Protection Server integrado mediante la configuración predeterminada de los puertos. Para obtener información detallada acerca de la configuración predeterminada de los puertos, consulte la siguiente tabla.
`ISPSInstaller.exe /i /f:[Número de puerto] /s:[Número de puerto] /w:[Número de puerto]`	Instala el servidor Smart Protection Server integrado mediante los puertos especificados. **Nota** Solo se pueden configurar los puertos cuando se utiliza un servidor Web Apache. Donde: • `/f:[Número de puerto]` representa el puerto HTTP de File Reputation • `/s:[Número de puerto]` representa el puerto HTTPS de File Reputation • `/w:[Número de puerto]` representa el puerto de reputación Web **Nota** A los puertos no especificados se les asigna de forma automática el valor predeterminado.
`ISPSInstaller.exe /u`	Desinstala el Smart Protection Server integrado

TABLA 4-4. Puertos para los servicios de reputación del servidor de Smart Protection Server integrado

SERVIDOR WEB Y CONFIGURACIÓN	PUERTOS PARA LOS SERVICIOS DE FILE REPUTATION		PUERTO HTTP PARA SERVICIOS DE REPUTACIÓN WEB
	HTTP	HTTPS (SSL)	
Sitio Web de IIS predeterminado con SSL activado	80	443 (no configurable)	80 (no configurable)
Sitio Web de IIS predeterminado con SSL desactivado	80	443 (no configurable)	80 (no configurable)
Sitio Web de IIS virtual con SSL activado	8080	4343 (configurable)	8080 (configurable)
Sitio Web de IIS virtual con SSL desactivado	8080	4343 (configurable)	8080 (configurable)

3. Una vez finalizada la instalación, abra la consola Web de OfficeScan y compruebe lo siguiente:

   - Abra la **Consola de administración de Microsoft** (introduciendo `services.msc` en el menú **Iniciar**) y compruebe que el Trend Micro Local Web Classification Server y Trend Micro Smart Scan Server aparezcan con el estado "Iniciado".
   - Abra el **Administrador de tareas de Windows**. En la pestaña **Procesos**, compruebe que `iCRCService.exe` y `LWCSService.exe` se estén ejecutando.
   - Compruebe que la opción de menú **Administración** > **Smart Protection** > **Servidor integrado** aparece en la consola Web de OfficeScan.

Prácticas recomendadas del Smart Protection Server

Optimice el rendimiento de los Smart Protection Servers mediante las siguientes acciones:

- Evite realizar exploraciones manuales y programadas simultáneamente. Escalone las exploraciones por grupos.
- Evite configurar todos los agentes de modo que realicen la opción Explorar ahora de manera simultánea.
- Personalice el Smart Protection Server para conexiones de red más lentas (alrededor de 512 Kbps) introduciendo cambios en el archivo `ptngrowth.ini`.

Personalización de ptngrowth.ini para el Servidor Independiente

Procedimiento

1. Abra el archivo `ptngrowth.ini` en `/var/tmcss/conf/`.
2. Modifique el archivo `ptngrowth.ini` con los valores recomendados indicados a continuación:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Guarde el archivo `ptngrowth.ini`.
4. Reinicie el servicio `lighttpd` escribiendo el siguiente comando de la interfaz de línea de comandos (CLI):
   - `service lighttpd restart`

Personalización de ptngrowth.ini para el Servidor Integrado

Procedimiento

1. Abra el archivo `ptngrowth.ini` de la *carpeta de instalación del servidor*`>\PCCSRV\WSS\`.

2. Modifique el archivo `ptngrowth.ini` con los valores recomendados indicados a continuación:
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Guarde el archivo `ptngrowth.ini`.
4. Reinicie el servicio del `Smart Protection Server de Trend Micro`.

Administración del Smart Protection Server Integrado

Administre el Smart Protection Server Integrado mediante las siguientes tareas:

- Activación de los Servicios de File Reputation y los Servicios de Reputación Web del servidor integrado
- Registro de las direcciones del servidor integrado
- Actualización de los componentes del servidor integrado
- Configuración de la Lista de URL permitidas/bloqueadas del servidor integrado

Para conocer más detalles, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

Activación de los Servicios de File Reputation y los Servicios de Reputación Web del servidor integrado

Para que los agentes envíen consultas de exploración y de reputación Web al servidor integrado, los servicios de File Reputation y de reputación Web deben estar activados. Al activar estos servicios también se permite que el servidor integrado actualice los componentes desde un servidor ActiveUpdate.

Estos servicios se activan automáticamente si elige instalar el servidor integrado durante la instalación del servidor de OfficeScan.

Si desactiva los servicios, asegúrese de que ha instalado servidores Smart Protection Server independientes a los que los agentes puedan enviar consultas.

Para conocer más detalles, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

Registro de las direcciones del servidor integrado

Necesitará las direcciones del servidor integrado cuando configure la lista de orígenes de Smart Protection para agentes internos. Para obtener información detallada sobre la lista, consulte la *Lista de fuentes de Smart Protection en la página 4-23*.

Cuando los agentes envían consultas de exploración al servidor integrado, identifican el servidor mediante una de las dos direcciones de los servicios de File Reputation: HTTP o HTTPS. La conexión mediante la dirección HTTPS permite una conexión más segura, mientras que la conexión HTTP utiliza menos ancho de banda.

Cuando los agentes envían consultas de reputación Web, estos identifican el servidor integrado por su dirección de servicios de reputación Web.

Consejo

Los agentes que se gestionan mediante otro servidor de OfficeScan también se conectan a este servidor integrado. En la consola Web del otro servidor de OfficeScan, agregue la dirección del servidor integrado a la lista de fuentes de Smart Protection.

Para conocer más detalles, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

Actualización de los componentes del servidor integrado

El servidor integrado actualiza los siguientes componentes:

- **Smart Scan Pattern**: los Agentes de OfficeScan verifican las posibles amenazas de Smart Scan Pattern enviando consultas de exploración al servidor integrado.
- **Lista de Bloqueo Web**: los Agentes de OfficeScan sujetos a políticas de reputación Web verifican la reputación de un sitio Web en la lista de bloqueo Web enviando consultas de reputación Web al servidor integrado.

Puede actualizar manualmente estos componentes o configurar un programa de actualización. El servidor integrado descarga los componentes del servidor ActiveUpdate.

Nota

Un servidor integrado que solo utilice IPv6 no puede actualizar directamente desde Trend Micro ActiveUpdate Server. Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir al servidor integrado que se conecte al servidor ActiveUpdate.

Para conocer más detalles, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

Configuración de la lista de URL permitidas/bloqueadas del servidor integrado

Los agentes conservan su propia lista de URL permitidas/bloqueadas. Configure la lista para los agentes cuando establezca las políticas de reputación Web (consulte *Políticas de reputación Web en la página 12-5* para obtener más información). Las URL contenidas en la lista del agente se permitirán o bloquearán automáticamente.

El servidor integrado tiene su propia lista de URL permitidas/bloqueadas Si una URL no se encuentra en la lista del agente, este envía una consulta de reputación Web al servidor integrado (si se ha asignado un origen de Smart Protection a dicho servidor). Si la URL se encuentra en la lista de URL permitidas/bloqueadas del servidor integrado, este notifica al agente para permitir o bloquear la URL.

Nota

La lista de URL bloqueadas tiene prioridad sobre la Lista de bloqueo Web.

Para agregar URL a la lista de URL permitidas/bloqueadas del servidor integrado, importe una lista de un Smart Protection Server independiente. No se puede agregar una URL de forma manual.

Para conocer más detalles, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

Configuración de los ajustes de Smart Protection Server integrado

Procedimiento

1. Vaya a **Administración** > **Smart Protection** > **Servidor integrado**.
2. Seleccione **Activar los Servicios de Reputación de Ficheros**.
3. Seleccione el protocolo (HTTP o HTTPS) que utilizarán los agentes cuando envíen consultas de exploración al servidor integrado.
4. Seleccione **Activar los Servicios de Reputación Web**.
5. Registre las direcciones del servidor integrado que se encuentran en la columna **Dirección del servidor**.
6. Para actualizar los componentes del servidor integrado:
   - Vea las versiones actuales de Smart Scan Pattern y de la Lista de bloqueo Web. Si hay alguna actualización disponible, haga clic en **Actualizar ahora**. El resultado de la actualización se muestra en la parte superior de la pantalla.
   - Para actualizar el patrón de forma automática:
     a. Seleccione **Activar las actualizaciones programadas**.
     b. Seleccione si las actualizaciones se realizan cada hora o cada 15 minutos.
     c. Seleccione una fuente de actualización en **Servicios de File Reputation**. Smart Scan Pattern se actualizará desde esta fuente.
     d. Seleccione una fuente de actualización en **Servicios de Reputación Web**. La Lista de bloqueo Web se actualizará desde esta fuente.

Nota

- Si selecciona el servidor ActiveUpdate como fuente de actualización, asegúrese de que el servidor tiene conexión a Internet y, en el caso de utilizar un servidor proxy, compruebe si la conexión a Internet se puede establecer utilizando la configuración del proxy. Consulte *Proxy para las actualizaciones del servidor de OfficeScan en la página 6-20* para obtener más información.
- Si selecciona una fuente de actualización personalizada, configure el entorno correspondiente y actualice los recursos de esta fuente de actualización. Además, asegúrese de que existe conexión entre el equipo servidor y la fuente de actualización. Si necesita ayuda a la hora de configurar una fuente de actualización, póngase en contacto con el proveedor de asistencia.

7. Para configurar la Lista de URL permitidas/bloqueadas del servidor integrado:
   a. Haga clic en **Importar** para llenar la lista con las URL a partir de un archivo `.csv` con formato aplicado previamente. Puede conseguir el archivo `.csv` de un Smart Protection Server independiente.
   b. Si dispone de una lista, haga clic en **Exportar** para guardar la lista en un archivo `.csv`.
8. Haga clic en **Guardar**.

Lista de fuentes de Smart Protection

Los agentes envían consultas a los orígenes de Smart Protection cuando realizan exploraciones en busca de riesgos de seguridad y determinan la reputación de un sitio Web.

Compatibilidad de las fuentes de Smart Protection con IPv6

Un agente que solo utiliza IPv6 no puede enviar consultas directamente a orígenes que utilizan únicamente IPv4, como:

- Smart Protection Server 2.0 (integrado o independiente)

Nota

La versión 2.5 del Smart Protection Server es la primera compatible con IPv6.

- Red de Smart Protection de Trend Micro

Del mismo modo, un agente que solo utiliza IPv4 no puede enviar consultas a servidores Smart Protection Server que utilizan únicamente IPv6.

Se necesita un servidor proxy de doble pila, como DeleGate, que convierta direcciones IP para permitir a los agentes que se conecten a los orígenes.

Orígenes de Smart Protection y ubicación del endpoint

El origen de Smart Protection al que se conecta el agente depende de la ubicación del endpoint del agente.

Para obtener información detallada sobre cómo configurar la ubicación, consulte *Ubicación del Endpoint en la página 15-2*.

TABLA 4-5. Fuentes de Smart Protection por ubicación

LOCALIZACIÓN	FUENTES DE SMART PROTECTION
externo	Los agentes externos envían consultas de exploración y de reputación Web a Trend Micro Smart Protection Network.

LOCALIZACIÓN	FUENTES DE SMART PROTECTION
interno	Los agentes internos envían consultas de exploración y de reputación Web a los servidores Smart Protection Server o a Trend Micro Smart Protection Network. Si ha instalado Smart Protection Servers, configure la lista de fuentes de Smart Protection en la consola OfficeScan Web. Un agente interno elige un servidor de la lista si necesita realizar una consulta. Si el agente no puede conectarse al primer servidor, elige otro servidor de la lista. **Consejo** Asigne un Smart Protection Server Independiente como la fuente de exploración principal y el Servidor Integrado como una copia de seguridad. De esta forma, se reduce el tráfico dirigido al endpoint que aloja el servidor de OfficeScan y el servidor integrado. El Servidor Independiente también puede procesar más consultas de exploración. Puede configurar la lista de fuentes de Smart Protection estándar o la personalizada. La lista estándar la utilizan todos los agentes internos. Las listas personalizadas definen un intervalo de direcciones IP. En caso de que una dirección IP de un agente interno se encuentre dentro del intervalo, el agente utilizará la lista personalizada.

Configuración de la lista estándar de fuentes de Smart Protection

Procedimiento

1. Vaya a **Administración** > **Smart Protection** > **Fuentes de Protección Inteligente**.
2. Haga clic en la pestaña **Agentes internos**.
3. Seleccione **Usar la lista estándar (para todos los agentes internos)**.
4. Haga clic en el enlace **lista estándar**.

Se abrirá una nueva pantalla.

5. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.

6. Especifique el nombre de host o la dirección IPv4/IPv6 del servidor Smart Protection Server. Si especifica una dirección IPv6, escríbala entre paréntesis.

   Nota

   Especifique el nombre de host si se conectan agentes IPv4 e IPv6 a Smart Protection Server.

7. Seleccione **Servicios de File Reputation**. Los agentes envían consultas de exploración mediante el protocolo HTTP o HTTPS. HTTPS permite una conexión más segura mientras que HTTP utiliza menos ancho de banda.

   a. Si desea que los agentes utilicen HTTP, escriba el puerto de escucha del servidor para las consultas HTTP. Si desea que los agentes utilicen HTTPS, seleccione SSL y escriba el puerto de escucha del servidor para las consultas HTTPS.

   b. Haga clic en **Probar la conexión** para comprobar si se puede establecer conexión con el servidor.

   Consejo

   Los puertos de escucha forman parte de la dirección del servidor. Para obtener la dirección del servidor:

   En el caso del servidor integrado, abra la consola Web de OfficeScan y vaya a **Administración** > **Smart Protection** > **Servidor integrado**.

   Para el servidor independiente, abra la consola del servidor independiente y vaya a la pantalla **Resumen**.

8. Seleccione **Servicios de Reputación Web**. Los agentes envían consultas de reputación Web mediante el protocolo HTTP. HTTPS no es compatible.

   a. Escriba el puerto de escucha del servidor para las consultas HTTP.

b. Haga clic en **Probar la conexión** para comprobar si se puede establecer conexión con el servidor.

9. Haga clic en **Guardar**.

   La pantalla se cerrará.

10. Para agregar más servidores, repita los pasos anteriores.

11. En la parte superior de la pantalla, seleccione **Orden** o **Aleatorio**.

    - **Orden**: los agentes seleccionan los servidores en el orden en que aparecen en la lista. Si selecciona **Orden**, use las flechas que se encuentran en la columna **Orden** para mover los servidores hacia arriba y abajo en la lista.
    - **Aleatorio**: los agentes seleccionan los servidores de forma aleatoria.

Consejo

El servidor de Smart Protection Server integrado y el servidor de OfficeScan se ejecutan en el mismo endpoint, por lo que el rendimiento del endpoint puede reducirse significativamente en los dos servidores cuando haya mucho tráfico. A fin de reducir el tráfico dirigido al equipo del servidor de OfficeScan, asigne un Smart Protection Server Independiente como la fuente de Smart Protection principal y el servidor integrado como una fuente de copia de seguridad.

12. Lleve a cabo tareas varias en la pantalla.

    - Si ha exportado una lista desde otro servidor y desea importarla a esta pantalla, haga clic en **Importar** y busque el archivo `.dat`. La lista se cargará en la pantalla.
    - Para exportar la lista a un archivo `.dat`, haga clic en **Exportar** y, a continuación, en **Guardar**.
    - Para actualizar el estado de servicio de los servidores, haga clic en **Actualizar**.
    - Haga clic en el nombre del servidor para realizar una de las siguientes acciones:
      - Para ver o editar la información sobre el servidor.
      - Visualice la dirección completa del servidor para los Servicios de Reputación Web o los Servicios de Reputación de Ficheros.

- Para abrir la consola de un Smart Protection Server, haga clic en **Iniciar consola**.
  - Para el servidor Smart Protection Server integrado, se mostrará la pantalla de configuración del servidor.
  - Para los Smart Protection Servers Independientes y el Smart Protection Server Integrado de otro servidor de OfficeScan, aparecerá la pantalla de inicio de sesión de la consola.
- Para eliminar una entrada, seleccione la casilla de verificación del servidor y haga clic en **Eliminar**.

13. Haga clic en **Guardar**.

    La pantalla se cerrará.

14. Haga clic en **Notificar a todos los agentes**.

Configuración de listas personalizadas de fuentes de Smart Protection

Procedimiento

1. Vaya a **Administración** > **Smart Protection** > **Fuentes de Protección Inteligente**.
2. Haga clic en la pestaña **Agentes internos**.
3. Seleccione **Utilizar listas personalizadas según la dirección IP del agente**.
4. (Opcional) Seleccione **Utilizar la lista estándar si ninguno de los servidores de las listas personalizadas está disponible**.

Consejo

Trend Micro recomienda activar esta característica para garantizar que los agentes se puedan conectar a un origen de Smart Protection si no se puede acceder a los orígenes personalizados.

5. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.

6. En la sección **Intervalo IP**, especifique un intervalo de direcciones IPv4 o IPv6, o ambas.

   Nota

   Los agentes con una dirección IPv4 pueden conectarse a servidores Smart Protection Server que solo utilicen IPv4 o que sean de doble pila. Los agentes con una dirección IPv6 pueden conectarse a servidores Smart Protection Server que solo utilicen IPv6 o que sean de doble pila. Los agentes con direcciones IPv4 e IPv6 pueden conectarse a cualquier Smart Protection Server.

7. En la sección **Configuración del proxy**, especifique la configuración del proxy que utilizarán los agentes para conectarse a servidores Smart Protection Server.

   a. Seleccione **Utilizar un servidor proxy para la comunicación entre agente y servidor de Smart Protection Server**.

   b. Especifique el nombre del servidor proxy o la dirección IPv4/IPv6, además del número de puerto.

   c. Si el servidor proxy necesita autenticación, escriba el nombre de usuario y la contraseña.

8. En **Lista personalizada del Smart Protection Server**, agregue los Smart Protection Servers.

   a. Especifique el nombre de host o la dirección IPv4/IPv6 del servidor Smart Protection Server. Si especifica una dirección IPv6, escríbala entre paréntesis.

      Nota

      Especifique el nombre de host si se conectan agentes IPv4 e IPv6 a Smart Protection Server.

   b. Seleccione **Servicios de File Reputation**. Los agentes envían consultas de exploración mediante el protocolo HTTP o HTTPS. HTTPS permite una conexión más segura mientras que HTTP utiliza menos ancho de banda.

i. Si desea que los agentes utilicen HTTP, escriba el puerto de escucha del servidor para las consultas HTTP. Si desea que los agentes utilicen HTTPS, seleccione **SSL** y escriba el puerto de escucha del servidor para las consultas HTTPS.

ii. Haga clic en **Probar la conexión** para comprobar si se puede establecer conexión con el servidor.

Consejo

Los puertos de escucha forman parte de la dirección del servidor. Para obtener la dirección del servidor:

En el caso del servidor integrado, abra la consola Web de OfficeScan y vaya a **Administración** > **Smart Protection** > **Servidor integrado**.

Para el servidor independiente, abra la consola del servidor independiente y vaya a la pantalla Resumen.

c. Seleccione **Servicios de Reputación Web**. Los agentes envían consultas de reputación Web mediante el protocolo HTTP. HTTPS no es compatible.

i. Escriba el puerto de escucha del servidor para las consultas HTTP.

ii. Haga clic en **Probar la conexión** para comprobar si se puede establecer conexión con el servidor.

d. Haga clic en **Agregar a la lista**.

e. Para agregar más servidores, repita los pasos anteriores.

f. Seleccione **Orden** o **Aleatorio**.

- **Orden**: los agentes seleccionan los servidores en el orden en que aparecen en la lista. Si selecciona **Orden**, use las flechas que se encuentran en la columna **Orden** para mover los servidores hacia arriba y abajo en la lista.
- **Aleatorio**: los agentes seleccionan los servidores de forma aleatoria.

Consejo

El servidor Smart Protection Server integrado y el servidor de OfficeScan se ejecutan en el mismo equipo y, por tanto, el rendimiento del equipo puede reducirse significativamente para los dos servidores cuando haya mucho tráfico. A fin de reducir el tráfico dirigido al equipo del servidor de OfficeScan, asigne un Smart Protection Server Independiente como la fuente de Smart Protection principal y el servidor integrado como una fuente de copia de seguridad.

g. Lleve a cabo tareas varias en la pantalla.

- Para actualizar el estado de servicio de los servidores, haga clic en **Actualizar**.
- Para abrir la consola de un Smart Protection Server, haga clic en **Iniciar consola**.
  - Para el servidor Smart Protection Server integrado, se mostrará la pantalla de configuración del servidor.
  - Para los Smart Protection Servers Independientes y el Smart Protection Server Integrado de otro servidor de OfficeScan, aparecerá la pantalla de inicio de sesión de la consola.
- Para eliminar alguna entrada, haga clic en **Eliminar** (

).

9. Haga clic en **Guardar**.

La pantalla se cerrará. La lista que acaba de agregar aparece como un enlace de intervalo de direcciones IP en la tabla **Intervalo de IP**.

10. Repita los pasos 4 al 8 para añadir más listas personalizadas.

11. Lleve a cabo tareas varias en la pantalla.

- Para modificar una lista, haga clic en el enlace de intervalo de direcciones IP y modifique la configuración en la pantalla que se abre.
- Para exportar la lista a un archivo .dat, haga clic en **Exportar** y, a continuación, en **Guardar**.

- Si ha exportado una lista desde otro servidor y desea importarla a esta pantalla, haga clic en **Importar** y busque el archivo `.dat`. La lista se cargará en la pantalla.

12. Haga clic en **Notificar a todos los agentes**.

Configuración del proxy de conexión del agente

Si la conexión a la red de Smart Protection requiere la autenticación del proxy, especifique las credenciales de autenticación. Para conocer más detalles, consulte *Proxy externo para agentes de OfficeScan en la página 15-55*.

Defina los valores internos de configuración del proxy que los agentes utilizarán cuando se conecten a un servidor Smart Protection Server. Para conocer más detalles, consulte *Proxy interno para agentes de OfficeScan en la página 15-54*.

Configuración de la ubicación del endpoint

OfficeScan incluye una función de conocimiento de ubicación que identifica la ubicación del equipo del agente y determina si el agente se conecta a Smart Protection Network o al servidor Smart Protection Server. Así se garantiza siempre la protección de los agentes independientemente de su ubicación.

Para establecer la configuración de ubicación, consulte *Ubicación del Endpoint en la página 15-2*.

Instalaciones de Trend Micro Network VirusWall

Si tiene instalado Trend Micro™Network VirusWall™Enforcer:

- Instale un archivo hot fix (compilación 1047 para Network VirusWall Enforcer 2500 y compilación 1013 para Network VirusWall Enforcer 1200).
- Actualice el motor OPSWAT a la versión 2.5.1017 para activar el producto y detectar un método de exploración del agente.

Uso de los Servicios de Smart Protection

Una vez que el entorno de Smart Protection se haya configurado correctamente, los agentes podrán utilizar los servicios de File Reputation y de reputación Web. También puede comenzar a configurar el Smart Feedback.

Nota

Para obtener instrucciones sobre cómo configurar el entorno de Smart Protection, consulte *Configuración de los Servicios de Smart Protection en la página 4-13*.

Para beneficiarse de la protección ofrecida por los servicios de File Reputation, los agentes deben utilizar el método de exploración llamado Smart Scan. Para obtener más información sobre Smart Scan y el modo de activarla en los agentes, consulte *Tipos de métodos de exploración en la página 7-9*.

Para permitir a los Agentes de OfficeScan utilizar los servicios de reputación Web, configure las políticas de reputación Web. Para conocer más detalles, consulte *Políticas de reputación Web en la página 12-5*.

Nota

La configuración de los métodos de exploración y las políticas de reputación Web son granulares. En función de sus necesidades, puede configurar parámetros que se apliquen a todos los agentes o configurar parámetros diferentes para agentes independientes o grupos de agentes.

Para obtener instrucciones acerca de cómo configurar el Smart Feedback, consulte *Smart Feedback en la página 14-69*.

Capítulo 5

Instalación del agente de OfficeScan

En este capítulo se describen los requisitos del sistema de OfficeScan y los procedimientos de instalación del Agente de OfficeScan.

Para obtener más información sobre la actualización del Agente de OfficeScan, consulte el *Manual de instalación y actualización de OfficeScan*.

Los temas que se incluyen son:

- *Instalaciones nueva del agente de OfficeScan en la página 5-2*
- *Consideraciones sobre la instalación en la página 5-2*
- *Consideraciones sobre la implementación en la página 5-13*
- *Migración al agente de OfficeScan en la página 5-71*
- *Posterior a la instalación en la página 5-75*
- *Desinstalación del Agente de OfficeScan en la página 5-78*

Instalaciones nueva del agente de OfficeScan

El Agente de OfficeScan se puede instalar en equipos que ejecuten las siguientes plataformas Microsoft Windows. OfficeScan también es compatible con diversos productos de terceros.

Visite el siguiente sitio Web para obtener una lista completa de los requisitos del sistema y los productos de terceros compatibles:

http://docs.trendmicro.com/es-es/enterprise/officescan.aspx

Consideraciones sobre la instalación

Antes de instalar agentes, tenga en cuenta lo siguiente:

TABLA 5-1. Consideraciones sobre la instalación de agentes

CONSIDERACIÓN	DESCRIPCIÓN
Compatibilidad con características de Windows	Algunas características de los Agente de OfficeScan no están disponibles en determinadas plataformas de Windows.
Compatibilidad con IPv6	El Agente de OfficeScan se puede instalar en agentes de doble pila o que solo utilizan IPv6. Sin embargo: • Algunos sistemas operativos Windows en los que puede instalarse el Agente de OfficeScan no son compatibles con el direccionamiento IPv6. • En algunos métodos de instalación, existen requisitos especiales para instalar correctamente el Agente de OfficeScan.
Direcciones IP del agente de OfficeScan	En agentes con direcciones IPv4 e IPv6, puede elegir qué dirección IP se utilizará cuando el agente se registre en el servidor.

Consideración	Descripción
Listas de excepciones	asegúrese de que las listas de excepciones para las funciones siguientes se han configurado correctamente: • **Supervisión del comportamiento**: agregue aplicaciones de endpoint críticas a la lista de programas permitidos para evitar que el Agente de OfficeScan bloquee dichas aplicaciones. Para obtener más información, consulte *Lista de excepción de supervisión del comportamiento en la página 9-10*. • **Reputación Web**: agregue sitios Web que considere seguros a la lista de URL permitidas para evitar que el Agente de OfficeScan bloquee el acceso a los sitios Web. Para obtener más información, consulte *Políticas de reputación Web en la página 12-5*.

Características del agente de OfficeScan

Las características del Agente de OfficeScan disponibles en el endpoint dependen del sistema operativo.

Tabla 5-2. Características del agente de OfficeScan en plataformas de servidor

Característica	Sistema operativo Windows			
	Servidor 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Exploración manual, exploración en tiempo real y exploración programada	Sí	Sí	Sí	Sí

Característica	Sistema operativo Windows			
	Servidor 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Actualización de componentes (manual y programada)	Sí	Sí	Sí	Sí
Agente de actualización	Sí	Sí	Sí	Sí
Reputación Web	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor
Damage Cleanup Services	Sí	Sí	Sí	Sí
Cortafuegos de OfficeScan	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor	Sí, pero desactivada de forma predeterminada durante la instalación del servidor

Característica	Sistema operativo Windows			
	Servidor 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Supervisión del comportamiento	Sí (32 bits), pero desactivada de forma predeterminada	Sí (32 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada
	No (64 bits)	Sí (64 bits), pero desactivada de forma predeterminada		
Autoprotección del agente para: • Claves de registro • Procesos	Sí (32 bits), pero desactivada de forma predeterminada	Sí (32 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada
	No (64 bits)	Sí (64 bits), pero desactivada de forma predeterminada		
Autoprotección del agente para: • Servicios • Protección de archivos	Sí	Sí	Sí	Sí

Característica	Sistema operativo Windows			
	Servidor 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Control de dispositivos (Servicio de prevención de cambios no autorizados)	Sí (32 bits), pero desactivada de forma predeterminada	Sí (32 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada
	No (64 bits)	Sí (64 bits), pero desactivada de forma predeterminada		
Protección de datos (incluida la protección de datos para el control de dispositivos)	Sí (32 bits), pero desactivada de forma predeterminada	Sí (32 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada
	Sí (64 bits), pero desactivada de forma predeterminada	Sí (64 bits), pero desactivada de forma predeterminada		
Configuración de conexión sospechosa	Sí	Sí	Sí	Sí
Envío de muestras	Sí	Sí	Sí	Sí
POP3 mail scan	Sí	Sí	Sí	Sí

Característica	Sistema operativo Windows			
	Servidor 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
Servicio Plug-in Manager del agente	Sí	Sí	Sí	Sí
Modo independiente	Sí	Sí (servidor) No (Server Core)	Sí	Sí
Smart Feedback	Sí	Sí	Sí	Sí

Tabla 5-3. Características del agente de OfficeScan en plataformas de escritorio

Característica	Sistema operativo Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Exploración manual, exploración en tiempo real y exploración programada	Sí	Sí	Sí	Sí	Sí
Actualización de componentes (manual y programada)	Sí	Sí	Sí	Sí	Sí
Agente de actualización	Sí	Sí	Sí	Sí	Sí

Característica	Sistema operativo Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Reputación Web	Sí	Sí	Sí	Sí, pero solamente compatibilidad limitada para el modo de interfaz de usuario de Windows	Sí
Damage Cleanup Services	Sí	Sí	Sí	Sí	Sí
Cortafuegos de OfficeScan	Sí	Sí	Sí	Sí	Sí
Supervisión del comportamiento	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)
	No (64 bits)	Sí (64 bits) Para la compatibilidad con Vista de 64 bits se requiere SP1 o SP2	Sí (64 bits)	Sí (64 bits)	Sí (64 bits)
Autoprotección del agente para: • Claves de registro • Procesos	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)
	No (64 bits)	Sí (64 bits) Para la compatibilidad con Vista de 64 bits se requiere SP1 o SP2	Sí (64 bits)	Sí (64 bits)	Sí (64 bits)

Característica	Sistema operativo Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Autoprotección del agente para: • Servicios • Protección de archivos	Sí	Sí	Sí	Sí	Sí
Control de dispositivos (Servicio de prevención de cambios no autorizados)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)
	No (64 bits)	Sí (64 bits) Para la compatibilidad con Vista de 64 bits se requiere SP1 o SP2	Sí (64 bits)	Sí (64 bits)	Sí (64 bits)
Protección de datos (incluida la protección de datos para el control de dispositivos)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits)	Sí (32 bits) en modo de escritorio	Sí (32 bits)
	Sí (64 bits)	Sí (64 bits)	Sí (64 bits)	Sí (64 bits) en modo de escritorio	Sí (64 bits)
Configuración de conexión sospechosa	Sí	Sí	Sí	Sí	Sí
Envío de muestras	Sí	Sí	Sí	Sí	Sí
POP3 mail scan	Sí	Sí	Sí	Sí	Sí
Servicio Plug-in Manager del agente	Sí	Sí	Sí	Sí	Sí

Característica	Sistema operativo Windows				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
Modo independiente	Sí	Sí	Sí	Sí	Sí
Smart Feedback	Sí	Sí	Sí	Sí	Sí

Instalación del agente de OfficeScan y compatibilidad con IPv6

En este tema se ofrecen algunas consideraciones que se deben tener en cuenta al instalar el Agente de OfficeScan en agentes de doble pila o que solo utilizan IPv6.

Sistema operativo

El Agente de OfficeScan solo se puede instalar en los siguientes sistemas operativos que son compatibles con el direccionamiento IPv6:

- Windows Vista™ (todas las ediciones)
- Windows Server 2008 (todas las ediciones)
- Windows 7 (todas las ediciones)
- Windows Server 2012 (todas las ediciones)
- Windows 8/8.1 (todas las ediciones)
- Windows 10 (ediciones Home, Pro, Education y Enterprise)
- Windows Server 2016 (todas las ediciones)

Visite el siguiente sitio Web para obtener una lista completa de los requisitos del sistema:

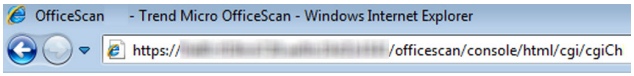
http://docs.trendmicro.com/es-es/enterprise/officescan.aspx

Métodos de instalación

Se pueden utilizar todos los métodos de instalación del Agente de OfficeScan para instalarlo en agentes de doble pila o que solo utilizan IPv6. En algunos métodos de instalación, existen requisitos especiales para instalar correctamente el Agente de OfficeScan.

No se puede migrar ServerProtect™ al Agente de OfficeScan mediante la herramienta ServerProtect Normal Server Migration, dado que esta herramienta no es compatible con el direccionamiento IPv6.

TABLA 5-4. Métodos de instalación y compatibilidad con IPv6

MÉTODO DE INSTALACIÓN	REQUISITOS/CONSIDERACIONES
Página Web de instalación e instalación basada en el explorador	La URL a la página de instalación incluye el nombre del host o la dirección IP del servidor de OfficeScan.  Si está realizando la instalación en un agente que solo utiliza IPv6, el servidor ha de ser de doble pila o debe utilizar únicamente IPv6; además, su nombre de host o dirección IPv6 deben formar parte de la URL. Para los agentes de doble pila, la dirección IPv6 que se muestra en la pantalla de estado de la instalación depende de la opción que se haya seleccionado en la sección **Dirección IP preferida** de **Agentes** > **Configuración global para los agentes** en la pestaña **Red**.
Agent Packager	Cuando esté ejecutando la herramienta de empaquetado, deberá seleccionar si desea asignar derechos de agente de actualización al agente. Recuerde que un agente de actualización que solo utiliza IPv6 puede distribuir las actualizaciones únicamente a agentes de doble pila o que solo utilizan IPv6.

Método de instalación	Requisitos/consideraciones
Conformidad con las normas de seguridad, Vulnerability Scanner e instalación remota	Un servidor que solo utiliza IPv6 no puede instalar el Agente de OfficeScan en endpoints que utilizan únicamente IPv4. De forma similar, un servidor que solo utiliza IPv4 no puede instalar el Agente de OfficeScan en endpoints que utilizan únicamente IPv6.

Direcciones IP del agente

Los servidores de OfficeScan instalados en un entorno que sea compatible con el direccionamiento IPv6 pueden administrar los siguientes Agentes de OfficeScan:

- Los servidores de OfficeScan instalados en equipos host que solo utilizan IPv6 pueden administrar agentes que solo utilizan IPv6.
- Los servidores de OfficeScan instalados en un equipo host de doble pila y que tienen asignadas direcciones IPv4 e IPv6 pueden administrar agentes de doble pila y que solo utilizan IPv6 o IPv4.

Después de instalar o actualizar los agentes, estos se registran en el servidor mediante una dirección IP.

- Los agentes que solo utilizan IPv6 se registran mediante una dirección IPv6.
- Los agentes que solo utilizan IPv4 se registran mediante una dirección IPv4.
- Los agentes de doble pila se registran mediante una dirección IPv4 o IPv6. Puede elegir la dirección IP que utilizarán estos agentes.

Configurar la dirección IP que los agentes de doble pila utilizan al registrarse en el servidor

Esta configuración solo está disponible para servidores de OfficeScan de doble pila y solo la aplican agentes de doble pila.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Red**.
3. Vaya a la sección **Dirección IP preferida**.
4. Seleccione una de estas opciones:
   - **Solo IPv4**: los Agentes utilizan su dirección IPv4.
   - **IPv4 en primer lugar y, después, IPv6**: los Agentes utilizan su dirección IPv4 primero. Si el agente no puede registrarse mediante su dirección IPv4, utilizará su dirección IPv6. Si el registro no se realiza correctamente con ninguna de las direcciones IP, el agente vuelve a intentarlo mediante la prioridad de dirección IP para esta selección.
   - **IPv6 en primer lugar y, después, IPv4**: los Agentes utilizan su dirección IPv6 primero. Si el agente no puede registrarse mediante su dirección IPv6, utilizará su dirección IPv4. Si el registro no se realiza correctamente con ninguna de las direcciones IP, el agente vuelve a intentarlo mediante la prioridad de dirección IP para esta selección.
5. Haga clic en **Guardar**.

Consideraciones sobre la implementación

En esta sección se ofrece un resumen de los diferentes métodos de instalación del Agente de OfficeScan para realizar una instalación nueva del Agente de OfficeScan. Todos los métodos de instalación requieren derechos de administrador local en los equipos de destino.

Si está instalando agentes y desea activar la compatibilidad con IPv6, lea las directrices de *Instalación del agente de OfficeScan y compatibilidad con IPv6 en la página 5-10*.

Tabla 5-5. Consideraciones sobre la implementación para la instalación

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Página Web de instalación Compatible con todos los sistemas operativos excepto Windows Server Core 2008 y Windows 8/8.1/ Server 2012/Server Core 2012 en modo de interfaz de usuario de Windows	No	No	Sí	No	No	Alto

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Instalaciones basadas en explorador Compatible con todos los sistemas operativos **Nota** No compatible con Windows 8, 8.1 ni Windows Server 2012 si operan en el modo de interfaz de usuario de Windows.	No	No	Sí	Sí	No	Alto (si las instalaciones se inician simultáneamente)
Instalaciones basadas en UNC Compatible con todos los sistemas operativos	No	No	Sí	Sí	No	Alto (si las instalaciones se inician simultáneamente)

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Instalaciones remotas Compatible con todos los sistemas operativos, salvo en: • Windows Vista Home Basic y Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (versiones básicas) • Windows 10 Home Edition	No	Sí	No	Sí	No	Alto
Configuración de inicio de sesión Compatible con todos los sistemas operativos	No	No	Sí	Sí	No	Alto (si las instalaciones se inician simultáneamente)

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Agent Packager Compatible con todos los sistemas operativos	No	No	Sí	Sí	No	Reducido, si se programa
Agent Packager (paquete de MSI implementado mediante Microsoft SMS) Compatible con todos los sistemas operativos	Sí	Sí	Sí/No	Sí	Sí	Reducido, si se programa
Agent Packager (paquete de MSI implementado mediante Active Directory) Compatible con todos los sistemas operativos	Sí	Sí	Sí/No	Sí	Sí	Alto (si las instalaciones se inician simultáneamente)
Imagen de disco de agente Compatible con todos los sistemas operativos	No	No	No	Sí	No	Bajo

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Trend Micro Vulnerability Scanner (TMVS) Compatible con todos los sistemas operativos, salvo en: • Windows Vista Home Basic y Home Premium Editions • Windows XP Home Edition • Windows 8/8.1 (versiones básicas) • Windows 10 Home Edition	No	Sí	No	Sí	No	Alto

Método de instalación y compatibilidad con sistemas operativos	Consideraciones sobre la implementación					
	Implementación de la WAN	Administración centralizada	Requiere la intervención del usuario	Precisa recursos de TI	Implementación en masa	Ancho de banda consumido
Instalaciones conformes con las normas de seguridad Compatible con todos los sistemas operativos, salvo en: • Windows Vista Home Basic y Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 (versiones básicas) • Windows 10 Home Edition	No	Sí	No	Sí	No	Alto

Instalaciones de la página Web de instalación

Los usuarios pueden instalar el programa del Agente de OfficeScan desde la página Web de instalación si ha instalado el servidor de OfficeScan en endpoints en los que se ejecuten las siguientes plataformas:

- Windows Server 2008 con Internet Information Server (IIS) 7.0
- Windows Server 2008 R2 con Internet Information Server (IIS) 7.5
- Windows Server 2012 con Internet Information Server (IIS) 8.0
- Windows Server 2012 R2 con Internet Information Server (IIS) 8.5
- Windows Server 2016 con Internet Information Server (IIS) 10.0

Para realizar la instalación desde la página Web, necesita los siguientes componentes:

- Internet Explorer con el nivel de seguridad establecido de forma que permita los controles ActiveX™. Las versiones requeridas son las siguientes:
  - 7.0 en Windows Vista y Windows Server 2008
  - 8.0 en Windows 7
  - 10.0 en Windows 8/8.1 y Windows Server 2012
  - 11.0 en Windows 10 y Windows Server 2016
- Derechos de administrador en el endpoint

Envíe las siguientes instrucciones a los usuarios para instalar el Agente de OfficeScan desde la página Web de instalación. Para enviar una notificación de instalación del agente a través de correo electrónico, consulte *Inicio de una instalación basada en explorador en la página 5-22*.

Instalar desde la página Web de instalación

Procedimiento

1. Inicie una sesión en el endpoint con una cuenta de administrador integrada.

Nota

Para plataformas de Windows 7, 8, 8.1 o 10, primero tiene que activar la cuenta de administrador integrada. Windows 7, 8, 8.1 y 10 desactivan la cuenta de administrador integrada de manera predeterminada. Para obtener más información, consulte el sitio de asistencia de Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

2. Si realiza la instalación en endpoints que ejecutan Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012, 2012 R2 o 2016, siga los pasos que se detallan a continuación:

   a. Inicie Internet Explorer y agregue la URL del servidor de OfficeScan (como, por ejemplo, `https://<Nombre del servidor de OfficeScan>:4343/officescan`) a la lista de sitios de confianza. En Windows 7, vaya a la pestaña **Herramientas** > **Opciones de Internet** > **Seguridad** para acceder a la lista; a continuación, seleccione el icono **Sitios de confianza** y haga clic en **Sitios**.

   b. Modifique la configuración de seguridad de Internet Explorer para activar **Pedir intervención del usuario automática para controles ActiveX**. En Windows 7, vaya a la pestaña **Herramientas** > **Opciones de Internet** > **Seguridad** y haga clic en **Nivel personalizado...**.

3. Abra una ventana de Internet Explorer y escriba:

   ```
   https://<nombre del servidor de OfficeScan>:<puerto>/officescan
   ```

4. Haga clic en el enlace del **instalador** de la página de inicio de sesión para ver las siguientes opciones de instalación:

   - **Instalación del agente basada en explorador** (solo Internet Explorer): siga las instrucciones en pantalla específicas para su sistema operativo.
   - **Instalación del agente de MSI**: descargue el paquete de 32 o 64 bits que corresponda según su sistema operativo y siga las instrucciones en pantalla.

   Nota

   Si el sistema lo solicita, permita la instalación de controles ActiveX.

5. Cuando se completa la instalación, aparece el icono del Agente de OfficeScan en la bandeja del sistema de Windows.

   Nota

   Para obtener una lista con los iconos que se visualizan en la bandeja del sistema, consulte *Iconos del agente de OfficeScan en la página 15-28*.

Instalación basada en explorador

Configure un mensaje de correo electrónico que indique a los usuarios de la red que instalen el Agente de OfficeScan. Para iniciar la instalación, los usuarios tienen que hacer clic en el enlace al instalador del Agente de OfficeScan que contiene el mensaje.

Antes de instalar Agentes de OfficeScan:

- Compruebe los requisitos de instalación del Agente de OfficeScan.
- Identifique los equipos de la red que actualmente no están protegidos frente a riesgos de seguridad. Realice las siguientes tareas:
  - Ejecute Trend Micro Vulnerability Scanner. Esta herramienta comprueba si los endpoints tienen instalado un software antivirus a partir del intervalo de direcciones IP especificado. Para conocer más detalles, consulte *Uso de Vulnerability Scanner en la página 5-43*.
  - Ejecute Conformidad con las normas de seguridad. Para conocer más detalles, consulte *Conformidad con las normas de seguridad para Endpoints no administrados en la página 15-76*.

Inicio de una instalación basada en explorador

Procedimiento

1. Vaya a **Agentes** > **Instalación de agentes** > **Basada en explorador**.
2. Modifique la línea del asunto del mensaje si es necesario.
3. Haga clic en **Crear correo electrónico.**

   Se abrirá el programa de correo predeterminado.
4. Envíe el mensaje de correo electrónico a los destinatarios que desee.

Realización de una instalación basada en UNC

`AutoPcc.exe` es un programa independiente que instala el Agente de OfficeScan en endpoints sin protección y actualiza los componentes y los archivos del programa. Los

endpoints deben formar parte del dominio para poder utilizar AutoPcc mediante una ruta de acceso con convención de nomenclatura universal (UNC).

Procedimiento

1. Vaya a **Agentes** > **Instalación de agentes** > **Basado en UNC**.

   - Para instalar el Agente de OfficeScan en un endpoint sin protección mediante `AutoPcc.exe`:

     a. Establezca conexión con el equipo del servidor. Vaya a la ruta de acceso UNC:

        `\\<nombre del equipo del servidor>\ofcscan`

     b. Haga clic con el botón derecho en `AutoPcc.exe` y seleccione **Ejecutar como administrador**.

   - Para realizar instalaciones remotas del escritorio con un `AutoPcc.exe`:

     a. Abra una Conexión a Escritorio remoto (Mstsc.exe) en el modo de consola. Esto obliga a que la instalación de `AutoPcc.exe` se ejecute en la sesión 0.

     b. Vaya al directorio `\\<nombre del equipo del servidor>\ofcscan` y ejecute `AutoPcc.exe`.

Instalar de forma remota desde la consola Web de OfficeScan

Instale el Agente de OfficeScan de forma remota en uno o varios endpoints conectados a la red. Asegúrese de que tiene derechos de administrador en los endpoints de destino para realizar la instalación remota. La instalación remota no instala el Agente de OfficeScan en los endpoints que ya ejecutan el servidor de OfficeScan.

Nota

Este método de instalación no puede utilizarse en endpoints que ejecutan Windows XP Home, Vista Home Basic y Home Premium, Windows 7 Home Basic y Home Premium (versiones de 32 y 64 bits), Windows 8 u 8.1 (versiones básicas de 32 y 64 bits), o Windows 10 Home. Un servidor que solo utiliza IPv6 no puede instalar el Agente de OfficeScan en agentes que utilizan únicamente IPv4. De forma similar, un servidor que solo utiliza IPv4 no puede instalar el Agente de OfficeScan en agentes que utilizan únicamente IPv6.

Procedimiento

1. Complete las siguientes tareas previas a la instalación para su versión de Windows.

   - Si ejecuta Windows XP:

     a. Active una cuenta de administrador de dominio integrada y defina la contraseña para la cuenta.

     b. En el endpoint, vaya a la pestaña **Mi PC** > **Herramientas** > **Opciones de carpeta** > **Ver** y desactive **Uso compartido simple de archivos**.

     c. Vaya a **Inicio** > **Programas** > **Firewall de Windows pestaña** > **Excepciones** y active la excepción **Compartir archivos e impresoras**.

     d. Abra la consola de administración de Microsoft (haga clic en **Inicio** > **Ejecutar** y escriba `services.msc`) e inicie los servicios **Registro remoto** y **Llamada de procedimiento remoto**. Cuando instale el Agente de OfficeScan, utilice la cuenta de administrador y la contraseña integradas.

   - Si ejecuta Windows Vista:

     a. Active una cuenta de administrador de dominio integrada y defina la contraseña para la cuenta.

     b. Haga clic en **Inicio** > **Panel de control** > **Seguridad** > **Firewall de Windows** > **Cambiar configuración**.

     c. Haga clic en la pestaña **Excepciones** y active la excepción **Compartir archivos e impresoras**.

     d. Abra la consola de administración de Microsoft (haga clic en **Inicio** > **Ejecutar** y escriba `services.msc`) e inicie los servicios **Registro**

remoto y **Llamada de procedimiento remoto**. Cuando instale el Agente de OfficeScan, utilice la cuenta de administrador y la contraseña integradas.

- Si ejecuta Windows 7, Windows 8 (Pro o Enterprise), Windows 8.1, Windows 10 (Pro, Education o Enterprise) o Windows Server 2012 o 2016:

  a. Active una cuenta de administrador de dominio integrada y defina la contraseña para la cuenta.

  b. Vaya a **Inicio** > **Programas** > **Herramientas administrativas** > **Firewall de Windows con seguridad avanzada**.

  c. Establezca las reglas de **Compartir archivos e impresoras** como «Dominio», «Privado» o «Público» en función de su entorno de red.

  d. Abra la consola de administración de Microsoft (haga clic en **Inicio** > **Ejecutar** y escriba `services.msc`) e inicie los servicios **Registro remoto** y **Llamada de procedimiento remoto**. Cuando instale el Agente de OfficeScan, utilice la cuenta de administrador y la contraseña integradas.

2. En la consola Web, vaya a **Agentes** > **Instalación de agentes** > **Remoto**.

3. Seleccione los endpoints de destino.

   - En la lista **Dominios y Endpoints** aparecerán todos los dominios de Windows de la red. Para ver los endpointes de un dominio, haga doble clic en el nombre del dominio. Seleccione un endpoint y haga clic en **Agregar**.

   - Si tiene un Nombre del Endpoint específico en mente, escriba el nombre del endpoint en el campo **Buscar Endpoints** en la parte superior de la página, y pulse Intro.

   OfficeScan le pedirá el nombre de usuario y la contraseña del endpoint de destino. Utilice el nombre de usuario y la contraseña de una cuenta de administrador para continuar.

4. Escriba el nombre de usuario y la contraseña y, a continuación, haga clic en **Iniciar sesión**.

   El endpoint de destino aparecerá en la tabla **Endpoints seleccionados**.

5. Repita los pasos 3 y 4 para agregar más endpoints.

6. Haga clic en **Instalar** cuando esté preparado para instalar el Agente de OfficeScan en los endpoints de destino.

   Aparecerá un cuadro de confirmación.

7. Haga clic en **Sí** para confirmar que desea instalar el Agente de OfficeScan en los endpoints de destino.

   Aparecerá una pantalla de progreso mientras se copian los archivos de programa en cada endpoint de destino.

Cuando OfficeScan finalice la instalación en un endpoint de destino, el nombre del endpoint desaparecerá de la lista **Endpoints seleccionados** y pasará a la lista **Dominios y endpoints** con una marca de verificación roja.

Cuando todos los endpoints de destino aparezcan con una marca de verificación roja en la lista **Dominios y endpoints**, habrá terminado la instalación remota.

Nota

Si realiza la instalación en varios endpoints, OfficeScan registrará cualquier instalación incorrecta en los registros (para obtener información detallada, consulte *Registros de instalación nueva en la página 18-16*), pero no retrasará las demás instalaciones. No es preciso que supervise la instalación tras hacer clic en **Instalar**. Compruebe los registros más adelante para ver los resultados de la instalación.

Instalar con Configuración de inicio de sesión

La configuración de inicio de sesión automatiza la instalación del Agente de OfficeScan en endpoints sin protección cuando éstos inician sesión en la red. Configuración de inicio de sesión añade el programa `AutoPcc.exe` a la secuencia de comandos de inicio de sesión del servidor.

`AutoPcc.exe` instala el Agente de OfficeScan en endpoints sin gestionar y actualiza los componentes y archivos del programa. Los endpoints deben formar parte del dominio para poder usar AutoPcc mediante el inicio de sesión.

Instalación de los programas de complemento

`AutoPcc.exe` instala automáticamente el Agente de OfficeScan en un endpoint sin protección con Windows Server 2003 cuando el endpoint inicia sesión en el servidor cuyas secuencias de comandos de inicio de sesión se han modificado. Sin embargo, `AutoPcc.exe` no instala el Agente de OfficeScan de manera automática en endpoints con Windows Vista, 7, 8, 8.1, 10, Server 2008, Server 2012 y Server 2016. Los usuarios deben conectarse al equipo del servidor, desplazarse hasta `\\<nombre del equipo del servidor>\ofcscan`, hacer clic con el botón derecho en `AutoPcc.exe` y, a continuación, seleccionar **Ejecutar como administrador**.

Para realizar una instalación remota del escritorio con un `AutoPcc.exe`:

- El endpoint debe ejecutarse en modo de consola `Mstsc.exe`. Esto obliga a que la instalación de `AutoPcc.exe` se ejecute en la sesión 0.
- Asigne una unidad a la carpeta "ofcscan" y ejecute `AutoPcc.exe` desde ese punto.

Actualizaciones de programas y componentes

`AutoPcc.exe` actualiza los archivos de programa así como el antivirus, antispyware y los componenetes de Damage Cleanup Services.

Scripts de Windows Server

Si ya tiene una secuencia de comandos de inicio de sesión, Configuración de inicio de sesión añade un comando que ejecuta `AutoPcc.exe`. De lo contrario, OfficeScan creará un archivo de lotes denominado `ofcscan.bat` que contiene el comando necesario para ejecutar `AutoPcc.exe`.

Configuración de inicio de sesión añade el texto siguiente al final de la secuencia de comandos:

```
\\<Nombre_de_servidor>\ofcscan\autopcc
```

Donde:

- `<Nombre_de_servidor>` es el nombre del endpoint o la dirección IP del equipo servidor de OfficeScan.

- "`ofcscan`" es el nombre de la carpeta compartida de OfficeScan en el servidor.
- "`autopcc`" es el enlace al archivo ejecutable autopcc que instala el Agente de OfficeScan.

Ubicación de la secuencia de comandos de inicio de sesión (a través de un directorio compartido de inicio de sesión en red):

- `Windows Server 2003: \\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008: \\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2012: \\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2016: \\Windows 2016 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

Adición de Autopcc.exe a la secuencia de comandos de inicio de sesión mediante Configuración de inicio de sesión

Procedimiento

1. En el endpoint que ha utilizado para ejecutar la instalación del servidor, haga clic en **Programas** > **Trend Micro OfficeScan Server <Nombre del servidor>** > **Configuración de inicio de sesión** en el menú Inicio de Windows.

   Se cargará la utilidad **Configuración de inicio de sesión**. La consola muestra un árbol en el que aparecen todos los dominios de la red.

2. Busque el servidor cuya secuencia de comandos de inicio de sesión desee modificar, márquelo y haga clic en **Seleccionar**. Asegúrese de que el servidor es un controlador de dominio principal y que dispone de derechos de administrador para acceder al servidor.

   Configuración de inicio de sesión le solicitará un nombre de usuario y una contraseña.

3. Escriba el nombre de usuario y la contraseña. Haga clic en **Aceptar** para continuar.

   Aparecerá la ventana **Selección de usuario**. La lista **Usuarios** muestra los perfiles de los usuarios que inician la sesión en el servidor. La lista **Usuarios seleccionados** muestra los perfiles de usuario cuya secuencia de comandos de inicio de sesión desea modificar.

4. Para modificar la secuencia de comandos de inicio de sesión de un perfil de usuario, seleccione dicho perfil en la lista de **usuarios** y, a continuación, haga clic en **Agregar**.

5. Para modificar la secuencia de comandos de inicio de sesión de todos los usuarios, haga clic en **Agregar todos**.

6. Para excluir un perfil de usuario seleccionado con anterioridad, seleccione el nombre correspondiente en la lista **Usuarios seleccionados** y haga clic en **Eliminar**.

7. Para restablecer las selecciones, haga clic en **Eliminar todos**.

8. Haga clic en **Aplicar** cuando todos los perfiles de usuario de destino se encuentren en la lista **Usuarios seleccionados**.

   Aparecerá un mensaje en el que se indica que ha modificado correctamente las secuencias de comando de inicio de sesión del servidor.

9. Haga clic en **Aceptar**.

   Configuración de inicio de sesión vuelve a la pantalla inicial.

10. Para modificar las secuencias de comandos de inicio de sesión de otros servidores, repita los pasos 2 a 4.

11. Para cerrar la utilidad Configuración de inicio de sesión, haga clic en **Salir**.

Instalar con Agent Packager

Agent Packager crea un paquete de instalación que se puede enviar a los usuarios a través de soportes convencionales, como puede ser un CD-ROM. Los usuarios ejecutan el paquete en el endpoint del agente para instalar o actualizar el Agente de OfficeScan y actualizar los componentes.

Agent Packager resulta especialmente útil al implementar el Agente de OfficeScan o componentes en agentes de oficinas remotas con un ancho de banda reducido. Agentes de OfficeScan que se instalan mediante Agent Packager envían un informe al servidor en el que se creó el paquete.

Agent Packager requiere lo siguiente:

- 350 MB de espacio libre en disco
- Windows Installer 2.0 (para ejecutar un paquete MSI)

Directrices para la implementación del paquete

1. Envíe el paquete a los usuarios y pídales que hagan doble clic en el archivo `EXE` o `MSI` para ejecutar el paquete del Agente de OfficeScan en sus endpoints.

   Nota

   Envíe el paquete solo a los usuarios cuyo Agente de OfficeScan informará al servidor dónde se ha creado el paquete.

2. Si tiene usuarios que desean instalar el paquete `EXE` en endpoints en los que se ejecuta Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 o Server 2016, indíqueles que deben hacer clic con el botón derecho en el archivo `EXE` y, a continuación, seleccionar **Ejecutar como administrador**.

3. Si ha creado un archivo `MSI`, realice las tareas que se detallan a continuación para implementar el paquete:

   - utilizar Active Directory o Microsoft SMS.

     Para obtener más información, consulte *Implementar un paquete MSI mediante Active Directory en la página 5-35* o *Implementar un paquete MSI mediante Microsoft SMS en la página 5-37*.

4. Inicie el paquete MSI desde una ventana del símbolo del sistema para instalar el Agente de OfficeScan de manera silenciosa en un endpoint remoto que ejecute Windows XP, Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 o Server 2016.

Directrices sobre métodos de exploración de los paquetes de agentes

Seleccione el método de exploración para el paquete. Consulte *Tipos de métodos de exploración en la página 7-9* para obtener más información.

Los componentes incluidos en el paquete dependen del método de exploración seleccionado. Para obtener información detallada acerca de los componentes disponibles para cada método de exploración, consulte *Actualizaciones del agente de OfficeScan en la página 6-30*.

Antes de seleccionar el método de exploración, tenga en cuenta las siguientes directrices para ayudarle a implementar el paquete de forma eficaz:

- En caso de que desee utilizar el paquete para actualizar el agente a esta versión de OfficeScan, seleccione el método de exploración a nivel de dominio en la consola Web. En la consola, vaya a **Agentes** > **Administración de agentes**, seleccione el dominio de árbol de agentes al que pertenece el agente y, a continuación, haga clic en **Configuración** > **Configuración de la exploración** > **Métodos de exploración**. El método de exploración de nivel de dominio debe ser coherente con el método de exploración seleccionado para el paquete.

- En caso de que vaya a utilizar el paquete para realizar una instalación nueva del Agente de OfficeScan, compruebe la configuración de la agrupación de agentes. En la consola Web, vaya a **Agentes** > **Agrupación de agentes**.

- Si la agrupación de agentes se ha creado mediante un domino NetBIOS, Active Directory o DNS, determine el dominio al que pertenece el endpoint de destino. En caso de que exista, compruebe el método de exploración configurado para el dominio. Si, por el contrario, el dominio no existe, determine el método de exploración a nivel de raíz. Para ello, seleccione el icono del dominio raíz ( ) en el árbol de agentes y, a continuación, haga clic en **Configuración** > **Configuración de la exploración** > **Métodos de exploración**. El método de exploración de nivel de dominio o de nivel raíz debe ser coherente con el método de exploración seleccionado para el paquete.

- Si la agrupación de agentes se realiza mediante grupos de agentes personalizados, compruebe la **prioridad de agrupación** y el **origen**.

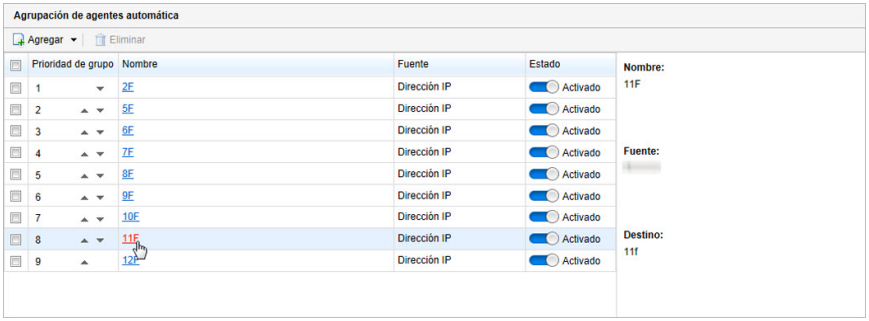


FIGURA 5-1. Panel de vista previa Agrupación automática de agentes

Si el endpoint de destino pertenece a un origen concreto, determine el **destino** correspondiente. El destino es el nombre del dominio que aparece en el árbol de agentes. El agente aplicará el método de exploración a ese dominio después de la instalación.

- Si va a utilizar el paquete para actualizar componentes en un agente mediante esta versión de OfficeScan, compruebe el método de exploración que se ha configurado para el dominio del árbol de agentes al que pertenece el agente. El método de exploración de nivel de dominio debe ser coherente con el método de exploración seleccionado para el paquete.

Creación de un paquete de instalación con Agent Packager

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a la *carpeta de instalación del servidor*> `\PCCSRV\Admin\Utility\ClientPackager`.

2. Haga doble clic en `ClnPack.exe` para ejecutar la herramienta.

   Se abrirá la consola de **Agent Packager**.

3. Seleccione el tipo de paquete que desee crear.

TABLA 5-6. Tipos de paquete del agente

TIPO DE PAQUETE	DESCRIPCIÓN
configuración	Seleccione **Instalar** para crear el paquete como un archivo ejecutable. El paquete instala el programa del Agente de OfficeScan con los componentes que se encuentran disponibles en el servidor en ese momento. Si el endpoint de destino tiene instalada una versión del agente anterior, el agente se actualizará al ejecutar el archivo ejecutable.
Actualizar	Seleccione **Actualizar** para crear un paquete que contenga los componentes disponibles en el servidor en ese momento. El paquete se creará como un archivo ejecutable. Utilice este paquete en caso de que haya problemas para actualizar los componentes en cualquier endpoint del agente.
MSI	Seleccione **MSI** para crear un paquete que se ajuste al formato del paquete de Microsoft Installer. El paquete también instala el programa del Agente de OfficeScan con los componentes que se encuentran disponibles en el servidor en ese momento. Si el endpoint de destino tiene instalada una versión del agente anterior, el agente se actualizará al ejecutar el archivo MSI.

4. Seleccione el sistema operativo para el que desea crear el paquete. Implemente el paquete únicamente en los endpoints en los que se ejecute este tipo de sistema operativo. Cree otro paquete para implementarlo en un sistema operativo de otro tipo.

5. Seleccione el método de exploración que implementará el paquete del agente.

   Para obtener más información sobre cómo seleccionar un método de exploración, consulte *Directrices sobre métodos de exploración de los paquetes de agentes en la página 5-31*.

6. En **Dominio**, seleccione una de las siguientes opciones:

   - **Permitir que el agente informe a su dominio automáticamente**: tras instalar el Agente de OfficeScan, el agente consulta la base de datos del servidor de OfficeScan e informa sobre su configuración de dominio al servidor.

- Cualquier dominio de la lista: Agent Packager se sincroniza con el servidor de OfficeScan y enumera los dominios que se usan actualmente en el árbol de agentes.

7. En **Opciones**, seleccione una de las siguientes opciones:

Opción	Descripción
Modo silencioso	Esta opción crea un paquete que se instala en el endpoint del agente en segundo plano, de forma que es inapreciable para el agente y, además, no muestra ninguna ventana sobre el estado de la instalación. Active esta opción si desea implementar el paquete de forma remota en el endpoint de destino.
Sobrescribir con la versión más reciente	Esta opción sobrescribe las versiones de los componentes del agente con las versiones más actualizadas disponibles en el servidor. Active esta opción para garantizar que los componentes del servidor y el agente estén sincronizados.
Desactivar exploración previa (solo para instalación nueva)	En caso de que el endpoint de destino no tenga instalado Agente de OfficeScan, el paquete explora el endpoint para comprobar si existen riesgos de seguridad antes de instalar el Agente de OfficeScan. Si está seguro de que en el endpoint de destino no existe ningún riesgo de seguridad, desactive la exploración previa. En caso de que esta opción esté activada, el programa de instalación buscará virusy malware en las zonas más vulnerables del endpoint, entre las que se incluyen las siguientes: • El área y el directorio de arranque (para virus de arranque) • La carpeta Windows • La carpeta Archivos de programa

8. En **Funciones del agente de actualización**, seleccione qué funciones puede implementar el agente de actualización.

9. En **Componentes**, seleccione los componentes y características que se incluirán en el paquete.

   - Para obtener información detallada acerca de los componentes, consulte *Componentes y programas de OfficeScan en la página 6-2*.

- El módulo de protección de datos solo está disponible si instala y activa la protección de datos. Para obtener información detallada acerca de la Protección de datos, consulte *Introducción a la protección de datos en la página 3-1*.

10. Junto a **Archivo de origen**, compruebe que la ubicación del archivo `ofcscan.ini` es correcta. Para modificar la ruta, haga clic en (...) y busque el archivo `ofcscan.ini`.

    De manera predeterminada, este archivo está en la carpeta `<carpeta de instalación del servidor>\PCCSRV` del servidor de OfficeScan.

11. En **Archivo de salida**, haga clic en (...), especifique la ubicación donde desee crear el paquete del Agente de OfficeScan y escriba el nombre de archivo del paquete (por ejemplo, `AgentSetup.exe`).

12. Haga clic en **Crear**.

    Cuando Agent Packager cree el paquete, aparecerá el mensaje «Paquete creado correctamente». Localice el paquete en el directorio que haya especificado en el paso anterior.

13. Implemente el paquete.

Implementar un paquete MSI mediante Active Directory

Aproveche las funciones que ofrece Active Directory para implementar el paquete MSI en múltiples endpoints del agente de forma simultánea.

Para consultar las instrucciones sobre la creación de un archivo MSI, consulte *Instalar con Agent Packager en la página 5-29*.

Procedimiento

1. Siga los pasos siguientes:

    - Para Windows Server 2003 y versiones anteriores:

        a. Abra la consola de Active Directory.

b. Haga clic con el botón derecho en la unidad organizativa (OU) donde desea implementar el paquete MSI y haga clic en **Propiedades**.

c. En la pestaña **Política de grupo**, haga clic en **Nueva**.

- Para Windows Server 2008 y Windows Server 2008 R2:

  a. Abra la **consola de administración de Política de grupo**. Haga clic en **Inicio** > **Panel de control** > **Herramientas administrativas** > **Administración de política de grupo**.

  b. En el árbol de la consola, amplíe **Objetos de política de grupo** en el bosque y el dominio que incluyen los objetos de política de grupo que desea editar.

  c. Haga doble clic en los Objetos de política de grupo que desee editar y luego haga clic en **Editar**. Esta acción abre el **editor de objetos de política de grupo**.

- Para Windows Server 2012 y Windows Server 2016:

  a. Abra la **consola de administración de Política de grupo**. Haga clic en **Administración de servidores** > **Herramientas** > **Administración de política de grupo**.

  b. En el árbol de la consola, amplíe **Objetos de política de grupo** en el bosque y el dominio que incluyen los objetos de política de grupo que desea editar.

  c. Haga doble clic en los Objetos de política de grupo que desee editar y luego haga clic en **Editar**. Esta acción abre el **editor de objetos de política de grupo**.

2. Elija entre la **Configuración de equipo** y **Configuración de usuario**, y abra **Parámetros del software** más abajo.

Consejo

Trend Micro recomienda utilizar **Configuración de equipo** en lugar de **Configuración de usuario** para garantizar una correcta instalación del paquete MSI independientemente del usuario que inicie sesión en el endpoint.

3. Debajo de **Parámetros del software**, haga clic con el botón derecho en **Instalación de software** y, a continuación, seleccione **Nuevo** y **Paquete**.

4. Ubique y seleccione el paquete MSI.

5. Seleccione un método de implementación y haga clic en **Aceptar**.

    - **Asignado**: el paquete MSI se implementa automáticamente la próxima vez que los usuarios inician sesión en el endpoint (si ha seleccionado Configuración de usuario) o cuando el endpoint se reinicia (si ha seleccionado Configuración de equipo). Este método no requiere la intervención del usuario.

    - **Publicado**: para ejecutar el paquete MSI, indique a los usuarios que se dirijan al Panel de control, abran la pantalla Agregar o quitar programas, y seleccionen la opción para agregar/instalar programas en la red. Cuando se visualiza el paquete MSI del Agente de OfficeScan, los usuarios pueden proceder a instalar el Agente de OfficeScan.

Implementar un paquete MSI mediante Microsoft SMS

Implemente el paquete MSI con Microsoft System Management Server (SMS) en caso de que Microsoft BackOffice SMS esté instalado en el servidor.

Para consultar las instrucciones sobre la creación de un archivo MSI, consulte *Instalar con Agent Packager en la página 5-29*.

El servidor SMS necesita obtener el archivo MSI del servidor de OfficeScan antes de poder implementar el paquete en los endpoints de destino.

- Local: el servidor SMS y el servidor de OfficeScan se encuentran en el mismo endpoint.

- Remoto: el servidor SMS y el servidor de OfficeScan se encuentran en endpoints diferentes.

Problemas conocidos al instalar con Microsoft SMS:

- En la columna **Tiempo de ejecución** de la consola de SMS aparece «Desconocido».

- Si la instalación no se ha realizado correctamente, el estado de la instalación puede continuar mostrando que está completa en el monitor del programa SMS.

  Para obtener instrucciones sobre cómo comprobar que la instalación ha sido correcta, consulte *Posterior a la instalación en la página 5-75*.

Las siguientes instrucciones son pertinentes si se utiliza Microsoft SMS 2.0 y 2003.

Obtención del paquete localmente

Procedimiento

1. Abra la consola **Administrador de SMS**.
2. En la pestaña **Árbol**, haga clic en **Paquetes**.
3. En el menú **Acción**, haga clic en **Nuevo** > **Paquete desde definición**.

   Aparecerá la pantalla **Bienvenido** del **Asistente para la creación de un paquete desde la definición**.
4. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Definición del paquete**.
5. Haga clic en **Examinar**.

   Aparecerá la pantalla **Abrir**.
6. Busque y seleccione el archivo del paquete MSI creado por Agent Packager y, a continuación, haga clic en **Abrir**.

   El nombre del paquete MSI aparece en la pantalla **Definición del paquete**. El paquete muestra "Agente de OfficeScan" y la versión del programa.
7. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Archivos de origen**.
8. Haga clic en **Obtener siempre los archivos desde un directorio de origen** y haga clic a continuación en **Siguiente**.

Aparecerá la pantalla **Directorio de origen**, con el nombre del paquete que desea crear y el directorio de origen.

9. Haga clic en **Unidad local en el servidor del sitio**.

10. Haga clic en **Examinar** y seleccione el directorio de origen que contiene el archivo MSI.

11. Haga clic en **Siguiente**.

    El asistente llevará a cabo el proceso de creación del paquete. Cuando haya finalizado el proceso, en la consola **Administrador de SMS** aparecerá el nombre del paquete.

Obtención del paquete remotamente

Procedimiento

1. En el servidor de OfficeScan, utilice Agent Packager para crear un paquete de instalación con una extensión `EXE` (no puede crear un paquete `MSI`). Consulte *Instalar con Agent Packager en la página 5-29* para obtener más información.

2. Cree una carpeta compartida en el endpoint en el que desea almacenar el origen.

3. Abra la consola Administrador de SMS.

4. En la pestaña **Árbol**, haga clic en **Paquetes**.

5. En el menú **Acción**, haga clic en **Nuevo** > **Paquete desde definición**.

   Aparecerá la pantalla **Bienvenido** del **Asistente para la creación de un paquete desde la definición**.

6. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Definición del paquete**.

7. Haga clic en **Examinar**.

   Aparecerá la pantalla **Abrir**.

8. Busque el archivo del paquete MSI. El archivo se encuentra en la carpeta compartida que ha creado.

9. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Archivos de origen**.

10. Haga clic en **Obtener siempre los archivos desde un directorio de origen** y haga clic a continuación en **Siguiente**.

    Aparecerá la pantalla **Directorio de origen**.

11. Haga clic en **Ruta de red (nombre UNC)**.

12. Haga clic en **Examinar** y seleccione el directorio de origen que contiene el archivo MSI (la carpeta compartida que ha creado).

13. Haga clic en **Siguiente**.

    El asistente llevará a cabo el proceso de creación del paquete. Cuando haya finalizado el proceso, en la consola **Administrador de SMS** aparecerá el nombre del paquete.

Distribuir del paquete a los Endpoints de destino

Procedimiento

1. En la pestaña **Árbol**, haga clic en **Anuncios**.

2. En el menú **Acción**, haga clic en **Todas las tareas** > **Distribuir software**.

   Aparecerá la pantalla **Bienvenido** del **asistente para la distribución de software**.

3. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Paquete**.

4. Haga clic en **Distribuir un paquete existente** y haga clic en el nombre del paquete de instalación que haya creado.

5. Haga clic en **Siguiente**.

   Aparecerá la pantalla **Puntos de distribución**.

6. Seleccione el punto de distribución en el que desea copiar el paquete y, a continuación, haga clic en **Siguiente**.

   Aparecerá la pantalla **Anunciar un programa**.

7. Haga clic en **Sí** para anunciar el paquete de instalación del Agente de OfficeScan y, a continuación, haga clic en **Siguiente**.

   Aparecerá la pantalla **Destino del anuncio**.

8. Haga clic en **Examinar** para seleccionar los endpoints de destino.

   Aparecerá la pantalla **Examinar colección**.

9. Haga clic en **Todos los sistemas Windows NT**.

10. Haga clic en **Aceptar**.

    Volverá a aparecer la pantalla **Destino del anuncio**.

11. Haga clic en **Siguiente**.

    Aparecerá la pantalla **Nombre del anuncio**.

12. En los cuadros de texto, escriba el nombre y los comentarios del anuncio y, a continuación, haga clic en **Siguiente**.

    Aparecerá la pantalla **Anuncio para subcolecciones**.

13. Decida si desea anunciar el paquete en las subcolecciones. Seleccione la opción habilitada para anunciar el programa únicamente a los miembros de la colección especificada o a los miembros de las subcolecciones.

14. Haga clic en **Siguiente**.

    Aparecerá la pantalla **Programa de anuncios**.

15. Especifique cuándo se anunciará el paquete de instalación del Agente de OfficeScan escribiendo o seleccionando la fecha y la hora.

Nota

Si desea que Microsoft SMS detenga el anuncio del paquete en una fecha determinada, haga clic en **Sí. Este anuncio debería caducar** y especifique a continuación la fecha y la hora en los cuadros de lista **Fecha y hora de caducidad**.

16. Haga clic en **Siguiente**.

    Aparecerá la pantalla **Asignar programa**.

17. Haga clic en **Sí. Asignar el programa** y haga clic a continuación en **Siguiente**.

    Microsoft SMS crea el anuncio y lo muestra en la consola de administración de SMS.

18. Cuando Microsoft SMS distribuya el programa anunciado (es decir, el programa del Agente de OfficeScan) a los endpoints de destino, se visualizará una pantalla en cada endpoint de destino. Indique a los usuarios que hagan clic en **Sí** y que sigan las instrucciones del asistente para instalar el Agente de OfficeScan en los endpoints.

Instalaciones mediante la imagen de disco de agente

La tecnología de copia de disco le permite crear una imagen del Agente de OfficeScan mediante el software de copia de disco y crear clones del mismo en otros equipos de la red.

La instalación de cada Agente de OfficeScan necesita un GUID (identificador exclusivo global) para que el servidor pueda identificar a los agentes de forma individual. Utilice el programa de OfficeScan `ImgSetup.exe` para crear un GUID distinto para cada clon.

Crear una imagen de disco del agente de OfficeScan

Procedimiento

1. Instale el Agente de OfficeScan en el endpoint.
2. Copie `ImgSetup.exe` desde <*Carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\ImgSetup` en este endpoint.
3. Ejecute `ImgSetup.exe` en este endpoint.

   Esto creará una clave de registro `RUN` en `HKEY_LOCAL_MACHINE`.
4. Cree una imagen del disco del Agente de OfficeScan mediante el software correspondiente.

5. Reinicie el clon.

   `ImgSetup.exe` se iniciará automáticamente y creará un nuevo valor GUID. El Agente de OfficeScan informará al servidor de este nuevo GUID y el servidor creará un registro nuevo para el nuevo Agente de OfficeScan.

¡ADVERTENCIA!

Para no tener dos equipos con el mismo nombre en la base de datos de OfficeScan, modifique manualmente el nombre del endpoint o del dominio del Agente de OfficeScan que haya clonado.

Uso de Vulnerability Scanner

Use Vulnerability Scanner para detectar las soluciones antivirus instaladas, buscar los equipos sin protección en la red e instalar los Agentes de OfficeScan en ellos.

Consideraciones para utilizar Vulnerability Scanner

Para ayudarle a decidir si utilizar Vulnerability Scanner, tenga en cuenta lo siguiente:

- *Administración de red en la página 5-44*
- *Arquitectura y topología de red en la página 5-44*
- *Especificaciones de software y hardware en la página 5-45*
- *Estructura de dominios en la página 5-45*
- *Tráfico de red en la página 5-46*
- *Tamaño de la red en la página 5-46*

Administración de red

Tabla 5-7. Administración de red

Configuración	Eficacia de Vulnerability Scanner
Administración con la política de seguridad estricta	Muy efectivo. Vulnerability Scanner indica si todos los equipos tienen algún software antivirus instalado.
Responsabilidad administrativa distribuida a través de sitios diferentes	Eficacia moderada
Administración centralizada	Eficacia moderada
Servicio de tercerización	Eficacia moderada
Los usuarios administran sus propios equipos	No efectivo. Porque Vulnerability Scanner explora la red para comprobar si hay algún programa antivirus instalado y no es flexible para dejar que los usuarios exploren sus propios equipos.

Arquitectura y topología de red

Tabla 5-8. Arquitectura y topología de red

Configuración	Eficacia de Vulnerability Scanner
Ubicación única	Muy efectivo. Vulnerability Scanner le permite explorar un segmento IP completo e instalar el Agente de OfficeScan en la LAN con facilidad.
Varias ubicaciones con conexión de alta velocidad	Eficacia moderada
Varias ubicaciones con conexión de baja velocidad	No efectivo. Es necesario que ejecute Vulnerability Scanner en cada ubicación y, además, la instalación del Agente de OfficeScan debe dirigirse a un servidor local de OfficeScan.
Equipos remotos y aislados	Eficacia moderada

Especificaciones de software y hardware

TABLA 5-9. Especificaciones de software y hardware

CONFIGURACIÓN	EFICACIA DE VULNERABILITY SCANNER
Sistemas operativos basados en Windows NT	Muy efectivo. Vulnerability Scanner puede instalar con facilidad el Agente de OfficeScan de forma remota en equipos en los que se ejecuten sistemas operativos basados en NT.
Sistemas operativos mixtos	Eficacia moderada. Vulnerability Scanner sólo puede realizar la instalación en equipos en los que se ejecuten sistemas operativos basados en Windows NT.
Software para la gestión de escritorio	No efectivo. Vulnerability Scanner no se puede utilizar con el software de gestión de escritorio. No obstante, puede ayudar a realizar un seguimiento del progreso de la instalación del Agente de OfficeScan.

Estructura de dominios

TABLA 5-10. Estructura de dominios

CONFIGURACIÓN	EFICACIA DE VULNERABILITY SCANNER
Microsoft Active Directory	Muy efectivo. Especifique la cuenta del administrador de dominios en Vulnerability Scanner para permitir la instalación remota del Agente de OfficeScan.
Grupo de trabajo	No efectivo. Vulnerability Scanner puede encontrar dificultades a la hora de realizar la instalación en equipos que usen contraseñas y cuentas administrativas diferentes.
Novell™ Directory Service	No efectivo. Vulnerability Scanner necesita una cuenta de dominios de Windows para instalar el Agente de OfficeScan.
Programas Peer To Peer (P2P)	No efectivo. Vulnerability Scanner puede encontrar dificultades a la hora de realizar la instalación en equipos que usen contraseñas y cuentas administrativas diferentes.

Tráfico de red

TABLA 5-11. Tráfico de red

CONFIGURACIÓN	EFICACIA DE VULNERABILITY SCANNER
Conexión LAN	Muy efectivo
512 Kbps	Eficacia moderada
Conexión T1 y superior	Eficacia moderada
Marcación telefónica	No efectivo. La instalación del Agente de OfficeScan tardará mucho tiempo en realizarse.

Tamaño de la red

TABLA 5-12. Tamaño de la red

CONFIGURACIÓN	EFICACIA DE VULNERABILITY SCANNER
Empresa muy grande	Muy efectivo. Cuanto más grande sea la red, más necesario será Vulnerability Scanner para comprobar las instalaciones del Agente de OfficeScan.
Pequeña y mediana empresa	Eficacia moderada. En el caso de redes pequeñas, Vulnerability Scanner puede utilizarse como una opción para instalar el Agente de OfficeScan. Es posible que sea mucho más sencillo aplicar otros métodos de instalación del Agente de OfficeScan.

Directrices para la instalación del agente de OfficeScan con Vulnerability Scanner

Vulnerability Scanner no instalará el Agente de OfficeScan si:

- El servidor de OfficeScan u otro software de seguridad está instalado en el equipo host de destino.
- El endpoint remoto ejecuta Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7 Home Basic, Windows 7 Home

Premium, Windows 8 (versiones básicas), Windows 8.1 (versiones básicas) o Windows 10 Home.

Nota

Puede instalar el Agente de OfficeScan en el equipo host de destino mediante los otros métodos de instalación, los cuales se describen en *Consideraciones sobre la implementación en la página 5-13*.

Antes de utilizar Vulnerability Scanner para instalar el Agente de OfficeScan, siga los pasos que se detallan a continuación:

- Para Windows Vista (Business, Enterprise o Ultimate Edition) o Windows 7 (Professional, Enterprise o Ultimate Edition), Windows 8 (Pro o Enterprise), Windows 8.1 (Pro o Enterprise), Windows 10 (Pro, Education o Enterprise), Windows Server 2012 (todas las ediciones) o Windows Server 2016 (todas las ediciones):

  1. Active una cuenta de administrador integrado y defina la contraseña para la cuenta.

  2. Haga clic en **Inicio** > **Programas** > **Herramientas administrativas** > **Firewall de Windows con seguridad avanzada**.

  3. En Perfil de dominio, Perfil privado y Perfil público, establezca el estado del cortafuegos en "Desactivado".

  4. Abra la Consola de administración de Microsoft (haga clic en **Iniciar** > **Ejecutar** y escriba `services.msc`) e inicie el servicio **Registro remoto**. Cuando instale el Agente de OfficeScan, utilice la cuenta de administrador y la contraseña integradas.

- Para Windows XP Professional (versión de 32 bits o 64 bits):

  1. Abra Windows Explorer y haga clic en **Herramientas** > **Opciones de carpeta**.

  2. Haga clic en la pestaña **Ver** y desactive la opción **Utilizar uso compartido simple de archivos (recomendado)**.

Métodos de exploración de vulnerabilidades

La exploración de vulnerabilidades comprueba la presencia de software de seguridad en equipos host y puede instalar el Agente de OfficeScan en aquellos equipos host que no estén protegidos.

Hay varios modos de ejecutar una exploración de vulnerabilidades.

TABLA 5-13. Métodos de exploración de vulnerabilidades

MÉTODO	DETALLES
Exploración de vulnerabilidades manual	Los administradores pueden ejecutar exploraciones de vulnerabilidades bajo petición.
Exploración DHCP	Los administradores pueden ejecutar exploraciones de vulnerabilidades en equipos host que soliciten direcciones IP desde un servidor DHCP. Vulnerability Scanner utiliza el puerto de escucha 67, que es el puerto de escucha del servidor DHCP para solicitudes DHCP. Si detecta una solicitud DHCP desde un equipo host, se ejecutará una exploración de vulnerabilidades en dicho equipo. **Nota** Vulnerability Scanner no puede detectar solicitudes DHCP si se ha iniciado en Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 o Windows Server 2012.
Exploración de vulnerabilidades programada	Las exploraciones de vulnerabilidades se ejecutan de forma automática en función del programa configurado por los administradores.

Una vez que se ejecute Vulnerability Scanner, esta aplicación mostrará el estado del Agente de OfficeScan en los equipos host de destino. El estado puede ser cualquiera de los siguientes:

- **Normal**: el Agente de OfficeScan se está ejecutando correctamente.
- **Anómalo**: los servicios del Agente de OfficeScan no se están ejecutando o el agente no tiene protección en tiempo real.

- **No instalado**: falta el servicio TMListen o el Agente de OfficeScan no se ha instalado.
- **No accesible**: Vulnerability Scanner no ha podido establecer conexión con el equipo host para determinar el estado del Agente de OfficeScan.

Ejecución de una exploración de vulnerabilidades manual

Procedimiento

1. Para ejecutar una exploración de vulnerabilidades en el equipo del servidor de OfficeScan, vaya a la <carpeta de instalación del servidor>`\PCCSRV\Admin\Utility\TMVS` y haga doble clic en `TMVS.exe`. Aparecerá la consola de **Trend Micro Vulnerability Scanner**. Para ejecutar una exploración de vulnerabilidades en otro endpoint que esté ejecutando Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 o Server 2012/2016:

   a. En el equipo del servidor de OfficeScan, vaya a `<carpeta de instalación del servidor>\PCCSRV\Admin\Utility`.

   b. Copie la carpeta `TMVS` en el otro endpoint.

   c. En el otro endpoint, abra la carpeta `TMVS` y haga doble clic en `TMVS.exe`.

      Aparecerá la consola de **Trend Micro Vulnerability Scanner**.

   Nota

   No puede utilizar Terminal Server para iniciar la herramienta.

2. Vaya a la sección **Exploración manual**.
3. Escriba el intervalo de direcciones IP de los endpoints que desee comprobar.

   a. Escriba un intervalo de direcciones IPv4.

Nota

Vulnerability Scanner solo puede realizar consultas en un intervalo de direcciones IPv4 si se ejecuta en un equipo host de doble pila o que solo utilice IPv4. Vulnerability Scanner solo admite un intervalo de direcciones IP de clase B; por ejemplo, de `168.212.1.1` a `168.212.254.254`.

b. Para un intervalo de direcciones IPv6, escriba el prefijo y la longitud de IPv6.

Nota

Vulnerability Scanner solo puede realizar consultas en un intervalo de direcciones IPv6 si se ejecuta en un equipo host de doble pila o que solo utilice IPv6.

4. Haga clic en **Settings**.

   Aparecerá la pantalla **Settings**.

5. Defina los siguientes valores de configuración:

OPCIÓN	DESCRIPCIÓN
Configuración del comando ping	la exploración de vulnerabilidades puede enviar comandos "ping" a las direcciones IP que se hayan especificado en el paso anterior para comprobar que estén en uso. Si un equipo host de destino está utilizando una dirección IP, Vulnerability Scanner puede determinar el sistema operativo del equipo host. Para conocer más detalles, consulte *Configuración del comando ping en la página 5-65*.
Método de recuperación de las descripciones de los equipos	para equipos host que respondan al comando "ping", Vulnerability Scanner puede recuperar información adicional acerca de los equipos host. Para conocer más detalles, consulte *Método de recuperación de las descripciones de los endpoints en la página 5-62*.
Consulta del producto	Vulnerability Scanner puede comprobar la presencia de software de seguridad en los equipos host de destino.

Opción	Descripción
	Para conocer más detalles, consulte *Consulta del producto en la página 5-59*.
Configuración del servidor de OfficeScan	Defina esta configuración si desea que Vulnerability Scanner instale el Agente de OfficeScan de forma automática en equipos host sin protección. Esta configuración identifica el servidor principal y las credenciales administrativas que el Agente de OfficeScan utiliza para iniciar sesión en los equipos host. Para conocer más detalles, consulte *Configuración del servidor de OfficeScan en la página 5-67*. **Nota** Algunas circunstancias pueden impedir la instalación del Agente de OfficeScan en los equipos host de destino. Para conocer más detalles, consulte *Directrices para la instalación del agente de OfficeScan con Vulnerability Scanner en la página 5-46*.
Notificaciones	Vulnerability Scanner puede enviar los resultados de la exploración de vulnerabilidades a los administradores de OfficeScan. También puede mostrar notificaciones en los equipos host que no estén protegidos. Para conocer más detalles, consulte *Notificaciones en la página 5-63*.
Guardar resultados	además de enviar los resultados de la exploración de vulnerabilidades a los administradores, la exploración de vulnerabilidades también puede guardar los resultados en un archivo `.csv`. Para conocer más detalles, consulte *Resultados de la exploración de vulnerabilidades en la página 5-65*.

6. Haga clic en **Aceptar**.

7. Haga clic en **Iniciar**.

   Los resultados de la exploración de vulnerabilidades aparecen en la tabla **Resultados** de la pestaña **Exploración manual**.

Nota

La información de la dirección MAC no aparece en la tabla **Resultados** si el endpoint ejecuta Windows Server 2008 o Windows Server 2012.

8. Para guardar los resultados en un archivo de valores separados por comas (CSV), haga clic en **Exportar**, localice la carpeta en la que desea guardarlo, escriba el nombre del archivo y, a continuación, haga clic en **Guardar**.

Ejecución de una exploración DHCP

Procedimiento

1. Defina los valores de configuración de DHCP en el archivo `TMVS.ini` que se encuentra en la siguiente carpeta: <carpeta de instalación del servidor>`\PCCSRV\Admin\Utility\TMVS`.

TABLA 5-14. Configuración de DHCP en el archivo `TMVS.ini`

PARÁMETRO	DESCRIPCIÓN
DhcpThreadNum=x	Especifique el número de amenaza para el modo DHCP. El mínimo es 3 y el máximo 100. El valor predeterminado es 8.
DhcpDelayScan=x	Se trata del tiempo de demora en segundos antes de comprobar si en el endpoint solicitante se encuentra instalado algún software antivirus. El mínimo es 0 (sin tiempo de espera) y el máximo 600. El valor predeterminado es 30.
LogReport=x	0 desactiva el inicio de sesión y 1 lo activa. Vulnerability Scanner envía los resultados de la exploración al servidor de OfficeScan. Los registros se muestran en la pantalla **Registros de sucesos del sistema** de la consola Web.
OsceServer=x	Se trata del nombre DNS o de la dirección IP del servidor de OfficeScan.

PARÁMETRO	DESCRIPCIÓN
OsceServerPort=x	Se trata del puerto del servidor Web del servidor de OfficeScan.

2. Para ejecutar una exploración de vulnerabilidades en el equipo del servidor de OfficeScan, vaya a la <carpeta de instalación del servidor>`\PCCSRV\Admin\Utility\TMVS` y haga doble clic en `TMVS.exe`. Aparecerá la consola de **Trend Micro Vulnerability Scanner**. Para ejecutar una exploración de vulnerabilidades en otro endpoint que esté ejecutando Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 o Server 2012/2016:

   a. En el equipo del servidor de OfficeScan, vaya a `<carpeta de instalación del servidor>\PCCSRV\Admin\Utility`.

   b. Copie la carpeta `TMVS` en el otro endpoint.

   c. En el otro endpoint, abra la carpeta `TMVS` y haga doble clic en `TMVS.exe`.

      Aparecerá la consola de **Trend Micro Vulnerability Scanner**.

Nota

No puede utilizar Terminal Server para iniciar la herramienta.

3. En la sección **Exploración manual**, haga clic en **Configuración**.

   Aparecerá la pantalla **Settings**.

4. Defina los siguientes valores de configuración:

OPCIÓN	DESCRIPCIÓN
Consulta del producto	Vulnerability Scanner puede comprobar la presencia de software de seguridad en los equipos host de destino. Para conocer más detalles, consulte *Consulta del producto en la página 5-59*.
Configuración del servidor de OfficeScan	Defina esta configuración si desea que Vulnerability Scanner instale el Agente de OfficeScan de forma automática en equipos host sin protección. Esta configuración identifica el servidor principal y las credenciales administrativas que el

OPCIÓN	DESCRIPCIÓN
	Agente de OfficeScan utiliza para iniciar sesión en los equipos host. Para conocer más detalles, consulte *Configuración del servidor de OfficeScan en la página 5-67*. **Nota** Algunas circunstancias pueden impedir la instalación del Agente de OfficeScan en los equipos host de destino. Para conocer más detalles, consulte *Directrices para la instalación del agente de OfficeScan con Vulnerability Scanner en la página 5-46*.
Notificaciones	Vulnerability Scanner puede enviar los resultados de la exploración de vulnerabilidades a los administradores de OfficeScan. También puede mostrar notificaciones en los equipos host que no estén protegidos. Para conocer más detalles, consulte *Notificaciones en la página 5-63*.
Guardar resultados	además de enviar los resultados de la exploración de vulnerabilidades a los administradores, la exploración de vulnerabilidades también puede guardar los resultados en un archivo `.csv`. Para conocer más detalles, consulte *Resultados de la exploración de vulnerabilidades en la página 5-65*.

5. Haga clic en **Aceptar**.

6. En la tabla de **resultados**, haga clic en la pestaña **DHCP Scan** (Exploración de DHCP).

Nota

La pestaña **Exploración DHCP** no está disponible en equipos en los que se ejecute Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 y Windows Server 2012.

7. Haga clic en **Iniciar**.

Vulnerability Scanner comienza a escuchar las solicitudes DHCP y realiza la exploración de vulnerabilidades en los equipos a medida que inician sesión en la red.

8. Para guardar los resultados en un archivo de valores separados por comas (CSV), haga clic en **Exportar**, localice la carpeta en la que desea guardarlo, escriba el nombre del archivo y, a continuación, haga clic en **Guardar**.

Configuración de una exploración de vulnerabilidades programada

Procedimiento

1. Para ejecutar una exploración de vulnerabilidades en el equipo del servidor de OfficeScan, vaya a la <carpeta de instalación del servidor>`\PCCSRV\Admin\Utility\TMVS` y haga doble clic en `TMVS.exe`. Aparecerá la consola de **Trend Micro Vulnerability Scanner**. Para ejecutar una exploración de vulnerabilidades en otro endpoint que esté ejecutando Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 o Server 2012/2016:

   a. En el equipo del servidor de OfficeScan, vaya a `<carpeta de instalación del servidor>\PCCSRV\Admin\Utility`.

   b. Copie la carpeta `TMVS` en el otro endpoint.

   c. En el otro endpoint, abra la carpeta `TMVS` y haga doble clic en `TMVS.exe`.

      Aparecerá la consola de **Trend Micro Vulnerability Scanner**.

   Nota

   No puede utilizar Terminal Server para iniciar la herramienta.

2. Vaya a la sección **Exploración programada**.

3. Haga clic en **Agregar/editar**.

   Aparecerá la pantalla **Exploración programada**.

4. escriba un nombre para la exploración de vulnerabilidades programada.

5. Escriba el intervalo de direcciones IP de los endpoints que desee comprobar.

   a. Escriba un intervalo de direcciones IPv4.

   Nota

   Vulnerability Scanner solo puede realizar consultas en un intervalo de direcciones IPv4 si se ejecuta en un equipo host de doble pila o que solo utilice IPv4. Vulnerability Scanner solo admite un intervalo de direcciones IP de clase B; por ejemplo, de `168.212.1.1` a `168.212.254.254`.

   b. Para un intervalo de direcciones IPv6, escriba el prefijo y la longitud de IPv6.

   Nota

   Vulnerability Scanner solo puede realizar consultas en un intervalo de direcciones IPv6 si se ejecuta en un equipo host de doble pila o que solo utilice IPv6.

6. Especifique la hora de inicio del **Programa** con un formato de 24 horas y, luego, seleccione con qué frecuencia que se ejecutará la exploración. Las opciones entre las que puede elegir son diariamente, semanalmente o mensualmente.

7. seleccione la configuración que vaya a usar para una exploración de vulnerabilidades.

   a. Seleccione **Usar la configuración actual** si ha definido y quiere usar la configuración de exploración de vulnerabilidades manual.

   Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades manual, consulte *Ejecución de una exploración de vulnerabilidades manual en la página 5-49*.

   b. Si no ha especificado una configuración de la exploración de vulnerabilidades manual o si quiere utilizar otra configuración, seleccione **Modificar la configuración** y, después, haga clic en **Configuración**.

   Aparecerá la pantalla **Settings**.

c. Defina los siguientes valores de configuración:

Configuración del comando ping	la exploración de vulnerabilidades puede enviar comandos "ping" a las direcciones IP que se hayan especificado en el paso anterior para comprobar que estén en uso. Si un equipo host de destino está utilizando una dirección IP, Vulnerability Scanner puede determinar el sistema operativo del equipo host. Para conocer más detalles, consulte *Configuración del comando ping en la página 5-65*.
Método de recuperación de las descripciones de los equipos	para equipos host que respondan al comando "ping", Vulnerability Scanner puede recuperar información adicional acerca de los equipos host. Para conocer más detalles, consulte *Método de recuperación de las descripciones de los endpoints en la página 5-62*.
Consulta del producto	Vulnerability Scanner puede comprobar la presencia de software de seguridad en los equipos host de destino. Para conocer más detalles, consulte *Consulta del producto en la página 5-59*.
Configuración del servidor de OfficeScan	Defina esta configuración si desea que Vulnerability Scanner instale el Agente de OfficeScan de forma automática en equipos host sin protección. Esta configuración identifica el servidor principal y las credenciales administrativas que el Agente de OfficeScan utiliza para iniciar sesión en los equipos host. Para conocer más detalles, consulte *Configuración del servidor de OfficeScan en la página 5-67*. **Nota** Algunas circunstancias pueden impedir la instalación del Agente de OfficeScan en los equipos host de destino. Para conocer más detalles, consulte *Directrices para la instalación del agente de OfficeScan con Vulnerability Scanner en la página 5-46*.

Notificaciones	Vulnerability Scanner puede enviar los resultados de la exploración de vulnerabilidades a los administradores de OfficeScan. También puede mostrar notificaciones en los equipos host que no estén protegidos. Para conocer más detalles, consulte *Notificaciones en la página 5-63*.
Guardar resultados	además de enviar los resultados de la exploración de vulnerabilidades a los administradores, la exploración de vulnerabilidades también puede guardar los resultados en un archivo `.csv`. Para conocer más detalles, consulte *Resultados de la exploración de vulnerabilidades en la página 5-65*.

8. Haga clic en **Aceptar**.

   La pantalla **Exploración programada** se cierra. La exploración programada de vulnerabilidades que se ha creado aparecerá en la sección **Exploración programada**. Si ha activado las notificaciones, Vulnerability Scanner le enviará los resultados de la exploración de vulnerabilidades programada.

9. Si desea ejecutar la exploración de vulnerabilidades programada inmediatamente, haga clic en **Ejecutar ahora**.

   Los resultados de la exploración de vulnerabilidades aparecen en la tabla **Resultados** de la pestaña **Exploración programada**.

   Nota

   La información de la dirección MAC no aparece en la tabla **Resultados** si el endpoint ejecuta Windows Server 2008 o Windows Server 2012.

10. Para guardar los resultados en un archivo de valores separados por comas (CSV), haga clic en **Exportar**, localice la carpeta en la que desea guardarlo, escriba el nombre del archivo y, a continuación, haga clic en **Guardar**.

Configuración de la exploración de vulnerabilidades

La configuración de la exploración de vulnerabilidades se define desde Trend Micro Vulnerability Scanner `TMVS.exe`) o desde el archivo `TMVS.ini`.

Nota

Consulte *Registros de depuración del servidor con LogServer.exe en la página 18-3* para obtener información sobre cómo recopilar registros de depuración para Vulnerability Scanner.

Consulta del producto

Vulnerability Scanner puede comprobar la presencia de software de seguridad en los agentes. En la siguiente tabla se indica cómo Vulnerability Scanner comprueba los productos de seguridad:

TABLA 5-15. Productos de seguridad comprobados por Vulnerability Scanner

PRODUCTO	DESCRIPCIÓN
ServerProtect para Windows	Vulnerability Scanner utiliza el endpoint RPC para comprobar si `SPNTSVC.exe` se está ejecutando. Devuelve información que incluye las versiones del sistema operativo, del motor de escaneo de virus y también del patrón de virus. Vulnerability Scanner no puede detectar el servidor de información ni la consola de administración de ServerProtect.
ServerProtect para Linux	Si el endpoint de destino no ejecuta Windows, Vulnerability Scanner se intenta conectar al puerto 14942 para determinar si se ha instalado ServerProtect for Linux.
Agente de OfficeScan	Vulnerability Scanner utiliza el puerto del Agente de OfficeScan para comprobar si el Agente de OfficeScan está instalado. También comprueba si el proceso `TmListen.exe` se está ejecutando. Recupera el número de puerto automáticamente si se ejecuta desde su ubicación predeterminada. Si ha iniciado Vulnerability Scanner en un endpoint que no sea el servidor de OfficeScan, compruebe los puertos de comunicación del otro endpoint y, a continuación, utilícelos.

Producto	Descripción
PortalProtect™	Vulnerability Scanner carga la página Web `http://localhost:port/PortalProtect/index.html` para comprobar la instalación del producto.
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner carga la página Web `http://direcciónIP:puerto/scanmail.html` para comprobar si está instalado ScanMail. ScanMail utiliza el puerto 16372 de forma predeterminada. En caso de que utilice un número de puerto distinto, especifíquelo. De lo contrario, Vulnerability Scanner no puede detectar ScanMail.
Familia InterScan™	Vulnerability Scanner carga cada una de las páginas Web de los diferentes productos para comprobar la instalación de los mismos. • InterScan Messaging Security Suite 5.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x: `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner utiliza el puerto 40116 para comprobar si está instalado Trend Micro Internet Security.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner envía un token especial al puerto TCP 8081, el cual es puerto predeterminado de ePolicy Orchestrator para establecer una conexión entre el servidor y el agente. El endpoint en el que esté instalado este antivirus responde con un tipo de token especial. Vulnerability Scanner no puede detectar el producto McAfee VirusScan independiente.
Norton Antivirus™ Corporate Edition	Vulnerability Scanner envía un símbolo especial al puerto UDP 2967, el puerto predeterminado de Norton Antivirus Corporate Edition RTVScan. El endpoint en el que esté instalado este antivirus responde con un tipo de token especial. Por tanto, el índice de precisión no se garantiza por el hecho de que Norton Antivirus Corporate Edition se comunica mediante UDP. Asimismo, el tráfico de red puede influir en el tiempo de espera de UDP.

Vulnerability Scanner detecta productos y equipos que utilizan los siguientes protocolos:

- **RPC**: detecta ServerProtect for NT
- **UDP**: detecta clientes de Norton AntiVirus Corporate Edition
- **TCP**: detecta McAfee VirusScan ePolicy Orchestrator
- **ICMP**: detecta equipos mediante el envío de paquetes ICMP
- **HTTP**: detecta Agentes de OfficeScan
- **DHCP**: si se detecta una solicitud DHCP, Vulnerability Scanner comprueba si ya se ha instalado el software antivirus en el endpoint solicitante.

Configuración de consultas del producto

La configuración de consultas del producto es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Para especificar la configuración de consultas del producto desde Vulnerability Scanner (`TMVS.exe`):

   a. Inicie `TMVS.exe`.

   b. Haga clic en **Settings**.

      Aparecerá la pantalla **Settings**.

   c. Vaya a la sección **Consulta del producto**.

   d. Seleccione los productos que se van a comprobar.

   e. Haga clic en **Configuración** junto al nombre del producto y, después, especifique el número de puerto que comprobará Vulnerability Scanner.

   f. Haga clic en **Aceptar**.

      La pantalla **Configuración** se cerrará.

2. Para definir el número de equipos que Vulnerability Scanner comprobará simultáneamente a fin de determinar si disponen de software de seguridad:

   a. Vaya a *carpeta de instalación del servidor*>\PCCSRV\Admin\Utility\TMVS y abra TMVS.ini con un editor de texto, como Bloc de notas.

   b. Para definir el número de equipos que se comprobarán durante las exploraciones de vulnerabilidades manuales, cambie el valor de ThreadNumManual. Especifique un valor comprendido entre 8 y 64.

      Por ejemplo, escriba `ThreadNumManual=60` si desea que Vulnerability Scanner compruebe 60 equipos de forma simultánea.

   c. Para definir el número de equipos que se comprobarán durante las exploraciones de vulnerabilidades programadas, cambie el valor de ThreadNumSchedule. Especifique un valor comprendido entre 8 y 64.

      Por ejemplo, escriba `ThreadNumSchedule=50` si desea que Vulnerability Scanner compruebe 50 equipos de forma simultánea.

   d. Guarde TMVS.ini.

Método de recuperación de las descripciones de los endpoints

Cuando Vulnerability Scanner pueda enviar comandos "ping" a equipos host, podrá recuperar información adicional acerca de dichos equipos. Hay dos métodos para recuperar información:

- **Recuperación rápida**: solo recupera el nombre del endpoint.
- **Recuperación normal**: recupera tanto información del dominio como del endpoint.

Configuración de la recuperación

La configuración de la recuperación es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Inicie `TMVS.exe`.
2. Haga clic en **Settings**.

   Aparecerá la pantalla **Settings**.
3. Vaya a la sección **Método de recuperación de las descripciones de los equipos**.
4. Seleccione **Normal** o **Rápida**.
5. Si ha seleccionado **Normal**, elija **Recuperar descripciones de los equipos cuando estén disponibles**.
6. Haga clic en **Aceptar**.

   La pantalla **Configuración** se cerrará.

Notificaciones

Vulnerability Scanner puede enviar los resultados de la exploración de vulnerabilidades a los administradores de OfficeScan. También puede mostrar notificaciones en los equipos host que no estén protegidos.

Configuración de la notificación

La configuración de las notificaciones es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Inicie `TMVS.exe`.
2. Haga clic en **Settings**.

   Aparecerá la pantalla **Settings**.
3. Vaya a la sección **Notificaciones**.

4. Para enviarse automáticamente los resultados de la exploración de vulnerabilidades a sí mismo o a otros administradores de la organización:

   a. Seleccione **Enviar por correo electrónico los resultados al administrador del sistema**.

   b. Haga clic en **Configurar** para especificar la configuración del correo electrónico.

   c. En **To**, escriba la dirección de correo electrónico del destinatario.

   d. En **De**, escriba la dirección de correo electrónico del remitente.

   e. En **Servidor SMTP**, escriba la dirección del servidor SMTP.

      Por ejemplo, puede escribir `smtp.empresa.com`. La información sobre el servidor SMTP es necesaria.

   f. En **Subject**, escriba un nuevo asunto de mensaje o acepte el que se muestra de manera predeterminada.

   g. Haga clic en **Aceptar**.

5. Para informar a los usuarios de que sus equipos no tienen instalado software de seguridad:

   a. Seleccione **Mostrar una notificación en los equipos sin protección**.

   b. Haga clic en **Personalizar** para configurar el mensaje de notificación.

   c. En la pantalla **Mensaje de notificación**, escriba un mensaje nuevo o acepte el predeterminado.

   d. Haga clic en **Aceptar**.

6. Haga clic en **Aceptar**.

   La pantalla **Configuración** se cerrará.

Resultados de la exploración de vulnerabilidades

Puede configurar Vulnerability Scanner para guardar los resultados de la exploración de vulnerabilidades en un archivo de valores separados por comas (CSV).

Configuración de los resultados de la exploración

La configuración de los resultados de la exploración de vulnerabilidades es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Inicie `TMVS.exe`.
2. Haga clic en **Settings**.

   Aparecerá la pantalla **Settings**.
3. Vaya a la sección **Guardar resultados**.
4. Seleccione **Guardar automáticamente los resultados en un archivo CSV**.
5. Para cambiar la carpeta predeterminada donde se guardan los archivos `CSV`:
   a. Haga clic en **Examinar**.
   b. Seleccione una carpeta de destino en el endpoint o en la red.
   c. Haga clic en **Aceptar**.
6. Haga clic en **Aceptar**.

   La pantalla **Configuración** se cerrará.

Configuración del comando ping

Utilice la configuración del comando "ping" para validar la existencia de un equipo de destino y determinar su sistema operativo. Si esta configuración está desactivada, Vulnerability Scanner explora todas las direcciones IP del intervalo de direcciones IP

especificado, incluso aquellas que no se utilicen en ningún equipo host, por lo que el intento de exploración durará más de lo que debiera.

Configuración del comando ping

La configuración del comando ping es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Para especificar la configuración del comando ping desde Vulnerability Scanner (`TMVS.exe`):
   a. Inicie `TMVS.exe`.
   b. Haga clic en **Settings**.

      Aparecerá la pantalla **Settings**.
   c. Vaya a la sección de configuración del **Comando ping**.
   d. Seleccione **Permitir que Vulnerability Scanner envíe comandos ping a los equipos de la red para comprobar su estado**.
   e. En los campos **Tamaño del paquete** y **Tiempo de espera**, acepte o modifique los valores predeterminados.
   f. Seleccione **Detectar el tipo de sistema operativo mediante la opción de huellas de sistema operativo ICMP**.

      Si selecciona esta opción, Vulnerability Scanner determina si un equipo host ejecuta Windows u otro sistema operativo. Vulnerability Scanner puede identificar la versión de Windows en aquellos equipos host que ejecuten dicho sistema operativo.
   g. Haga clic en **Aceptar**.

      La pantalla **Configuración** se cerrará.
2. Para definir el número de equipos a los que Vulnerability Scanner enviará comandos ping simultáneamente:

a. Vaya a *carpeta de instalación del servidor*>\PCCSRV\Admin\Utility\TMVS y abra TMVS.ini con un editor de texto, como Bloc de notas.

b. Cambie el valor de EchoNum. Especifique un valor comprendido entre 1 y 64.

   Por ejemplo, escriba `EchoNum=60` si desea que Vulnerability Scanner envíe comandos ping a 60 equipos de forma simultánea.

c. Guarde TMVS.ini.

Configuración del servidor de OfficeScan

La configuración del servidor de OfficeScan se utiliza cuando:

- Vulnerability Scanner instala el Agente de OfficeScan en equipos de destino que no estén protegidos. La configuración del servidor permite que Vulnerability Scanner identifique el servidor principal del Agente de OfficeScan y las credenciales administrativas que se utilizarán para iniciar sesión en los equipos de destino.

  Nota

  Algunas circunstancias pueden impedir la instalación del Agente de OfficeScan en los equipos host de destino.

  Para conocer más detalles, consulte *Directrices para la instalación del agente de OfficeScan con Vulnerability Scanner en la página 5-46*.

- Vulnerability Scanner envía los registros de la instalación del agente al servidor de OfficeScan.

Configuración del servidor de OfficeScan

La configuración del servidor de OfficeScan es un subconjunto de la configuración de la exploración de vulnerabilidades. Para obtener información detallada acerca de la configuración de la exploración de vulnerabilidades, consulte *Métodos de exploración de vulnerabilidades en la página 5-48*.

Procedimiento

1. Inicie `TMVS.exe`.
2. Haga clic en **Settings**.

   Aparecerá la pantalla **Settings**.
3. Vaya a la sección **Configuración del servidor de OfficeScan**.
4. Escriba el nombre y el número de puerto del servidor de OfficeScan.
5. Seleccione **Instalar automáticamente el agente de OfficeScan en equipos sin protección**.
6. Para configurar las credenciales administrativas:
   a. Haga clic en **Instalar en cuenta**.
   b. En la pantalla **Información de la cuenta**, escriba un nombre de usuario y una contraseña.
   c. Haga clic en **Aceptar**.
7. Seleccione **Enviar registros al servidor de OfficeScan**.
8. Haga clic en **Aceptar**.

   La pantalla **Configuración** se cerrará.

Instalar de conformidad con las normas de seguridad

Instale Agentes de OfficeScan en equipos dentro de los dominios de la red o instale el Agente de OfficeScan en un endpoint de destino mediante su dirección IP.

Antes de instalar el Agente de OfficeScan, tenga en cuenta los siguientes aspectos:

Procedimiento

1. Registre las credenciales de inicio de sesión de cada endpoint. OfficeScan le pedirá que especifique las credenciales de inicio de sesión durante la instalación.

2. El Agente de OfficeScan no se instalará en un endpoint si:

   - El servidor de OfficeScan está instalado en el endpoint.
   - El endpoint ejecuta Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8 (versiones básicas), Windows 8.1 (versiones básicas) y Windows 10 Home. Si cuenta con equipos en los que se ejecuten estas plataformas, seleccione otro método de instalación. Consulte *Consideraciones sobre la implementación en la página 5-13* para obtener más información.

3. Si el endpoint de destino ejecuta Windows Vista (Business, Enterprise o Ultimate Edition), Windows 7 (Professional, Enterprise o Ultimate Edition), Windows 8 (Pro, Enterprise), Windows 8.1 (Pro, Enterprise), Windows 10 (Pro, Education, Enterprise) o Windows Server 2012 (Standard), aplique los siguientes pasos en dicho endpoint:

   a. Active una cuenta de administrador integrado y defina la contraseña para la cuenta.

   b. Desactive el cortafuegos de Windows.

   c. Haga clic en **Iniciar** > **Programas** > **Herramientas administrativas** > **Cortafuegos de Windows con seguridad avanzada**.

   d. En Perfil de dominio, Perfil privado y Perfil público, establezca el estado del cortafuegos en "Desactivado".

   e. Abra la Consola de administración de Microsoft (haga clic en **Inicio** > **Ejecutar** y escriba `services.msc`) e inicie el servicio **Registro remoto**. Cuando instale el Agente de OfficeScan, utilice la cuenta de administrador y la contraseña integradas.

4. En caso de que en el endpoint esté instalado algún programa de seguridad de endpoint de Trend Micro o de otros fabricantes, compruebe si OfficeScan puede desinstalar dicho software automáticamente a fin de sustituirlo por el Agente de OfficeScan. Para acceder a una lista de programas de seguridad de agente que OfficeScan puede desinstalar automáticamente, abra los siguientes archivos en *Carpeta de instalación del servidor*>`\PCCSRV\Admin`. Puede abrir estos archivos mediante un editor de texto como el Bloc de notas

- `tmuninst.ptn`
- `tmuninst_as.ptn`

En caso de que el software que está instalado en el endpoint de destino no se encuentre en la lista, primero desinstálelo manualmente. Dependiendo del proceso de desinstalación del software, se tendrá que reiniciar o no el endpoint tras la desinstalación.

Instalación del agente de OfficeScan

Procedimiento

1. Vaya a **Valoración** > **Endpoints no administrados**.
2. En la parte superior del árbol de agentes, haga clic en **Instalar**.
   - Si hace clic en **Instalar** y en el endpoint ya hay instalada una versión anterior del Agente de OfficeScan, se omitirá la instalación y, por tanto, el agente no se actualizará a esta versión. Se debe desactivar una opción para actualizar el agente.
     a. Vaya a **Agentes** > **Administración de agentes**.
     b. Haga clic en la pestaña **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones**.
     c. Desactive la opción **Los agentes de OfficeScan pueden actualizar componentes pero no pueden actualizar el programa del agente ni implementar archivos HotFix**.
3. Especifique la cuenta de administrador con derecho a inicio de sesión para cada endpoint y, a continuación, haga clic en **Iniciar sesión**. OfficeScan empezará a instalar el agente en el endpoint de destino.
4. Consulte el estado de la instalación.

Migración al agente de OfficeScan

Reemplace el software de seguridad del agente instalado en un endpoint de destino con el Agente de OfficeScan.

Migrar desde otro software de seguridad de endpoint

Al instalar el Agente de OfficeScan, el programa de instalación comprueba si existe otro software de seguridad de endpoint de Trend Micro o de otro fabricante instalado en el endpoint de destino. El programa de instalación puede desinstalar dicho software automáticamente y sustituirlo por el Agente de OfficeScan.

Para acceder a una lista de programas de seguridad de endpoint que OfficeScan puede desinstalar automáticamente, abra los siguientes archivos en la *carpeta de instalación del servidor*>\PCCSRV\Admin. Abra estos archivos con un editor de texto como el Bloc de notas.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

En caso de que el software que está instalado en el endpoint de destino no se encuentre en la lista, primero desinstálelo manualmente. Dependiendo del proceso de desinstalación del software, se tendrá que reiniciar o no el endpoint tras la desinstalación.

Problemas de migración de los agentes de OfficeScan

- Si la migración de agentes automática se ha realizado correctamente, pero un usuario tiene problemas con un agente justo después de la instalación, reinicie el Agente de OfficeScan.
- En caso de que el programa de instalación de OfficeScan ha continuado la instalación del Agente de OfficeScan, pero no ha podido desinstalar el otro software de seguridad, ocurrirán conflictos entre ambos. Desinstálelos y, a continuación, instale el Agente de OfficeScan mediante cualquiera de los métodos de instalación que se mencionan en *Consideraciones sobre la implementación en la página 5-13*.

Migrar desde servidores ServerProtect normales

La herramienta ServerProtect™ Normal Server Migration es una herramienta que ayuda a realizar la migración de los equipos que ejecutan el servidor normal de Trend Micro ServerProtect al Agente de OfficeScan.

La herramienta ServerProtect Normal Server Migration Tool comparte la misma especificación de hardware y software que el servidor de OfficeScan. Ejecute la herramienta en equipos que ejecuten Windows Server 2003 o Windows Server 2008.

Cuando la desinstalación del servidor normal de ServerProtect es correcta, la herramienta instala el Agente de OfficeScan. También migra la configuración de la lista de exclusión de la exploración (para todos los tipos de exploración) al Agente de OfficeScan.

Mientras se instala el Agente de OfficeScan, el instalador de agentes de la herramienta de migración a veces puede exceder el tiempo de espera y notificarle que la instalación no se ha realizado con éxito. Sin embargo, el Agente de OfficeScan se puede haber instalado correctamente. Compruebe la instalación en el endpoint del agente desde la consola Web de OfficeScan.

La migración no se realiza correctamente en los casos siguientes:

- El agente remoto únicamente tiene una dirección IPv6. La herramienta de migración no es compatible con las direcciones IPv6.
- El agente remoto no puede utilizar el protocolo NetBIOS.
- Los puertos 455, 337 y 339 están bloqueados.
- El agente remoto no puede utilizar el protocolo RPC.
- El servicio Remote Registry Service se detiene.

Nota

La herramienta ServerProtect Normal Server Migration no desinstala el agente de Control Manager™ para ServerProtect. Para conocer más instrucciones sobre cómo desinstalar el agente, consulte la documentación correspondiente de ServerProtect y/o Control Manager.

Uso de la herramienta ServerProtect Normal Server Migration Tool

Procedimiento

1. En el equipo del servidor de OfficeScan, abra la <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\SPNSXfr` y copie los archivos `SPNSXfr.exe` y `SPNSX.ini` en `<carpeta de instalación del servidor>\PCCSRV\Admin`.

2. Haga doble clic en `SPNSXfr.exe` para abrir la herramienta.

   Aparecerá la consola de **ServerProtect Normal Server Migration Tool**.

3. Seleccione el servidor de OfficeScan. La ruta de acceso del servidor de OfficeScan aparece en OfficeScan server path. Si no es correcta, haga clic en **Browse** y seleccione la carpeta `PCCSRV` en el directorio en el que está instalado OfficeScan. Para que la herramienta vuelva a buscar automáticamente el servidor de OfficeScan la próxima vez que se ejecute la herramienta, active la casilla de verificación **Buscar automáticamente la ruta del servidor** (activada de forma predeterminada).

4. Para seleccionar los equipos que ejecutan ServerProtect Normal Server en los que se llevará a cabo la migración, haga clic en una de las siguientes opciones de **Endpoint de destino**:

   - **Árbol de red de Windows**: muestra un árbol con los dominios de la red. Para seleccionar los equipos mediante este método, haga clic en los dominios en los que desee buscar los equipos del agente.

   - **Nombre del servidor de información**: permite buscar por nombre del servidor de información. Para seleccionar equipos con este método, escriba en el cuadro de texto el nombre de un servidor de información de la red. Para buscar varios servidores de información, introduzca punto y coma ";" para separar los nombres de los servidores.

   - **Nombre de servidor normal**: permite buscar por nombre de servidor normal. Para seleccionar equipos con este método, escriba en el cuadro de texto el nombre de un servidor normal de la red. Para buscar varios servidores Normal Server, introduzca punto y coma ";" para separar los nombres de los servidores.

- **Búsqueda de intervalos IP**: permite buscar por intervalo de direcciones IP. Para seleccionar equipos mediante este método, escriba un rango de direcciones IP de clase B en el rango IP.

Nota

Si un servidor DNS de la red no responde durante la búsqueda de agentes, la búsqueda dejará de responder. Respete el tiempo de espera de la búsqueda.

5. Seleccione **Reiniciar después de la instalación** para reiniciar automáticamente los equipos de destino tras la migración.

   Se requiere reiniciar para que la migración se complete correctamente. Si no selecciona esta opción, reinicie manualmente los equipos tras la migración.

6. Haga clic en **Buscar**.

   Los resultados de la búsqueda aparecen en **ServerProtect Normal Servers**.

7. Haga clic en los equipos en que desea realizar la migración

   a. Para seleccionar todos los equipos, haga clic en **Seleccionar todo**.

   b. Para borrar todos los equipos, haga clic en **Deseleccionar todo**.

   c. Para exportar la lista a un archivo de datos de valores separados por comas (CSV), haga clic en **Exportar a CSV**.

8. Si se requiere un nombre de usuario y una contraseña para iniciar sesión en los equipos de destino, lleve a cabo lo siguiente:

   a. Active la casilla de verificación **Utilizar cuenta/contraseña de grupo**.

   b. Haga clic en **Establecer cuenta de inicio de sesión**.

      Aparecerá la ventana Enter Administration Information.

   c. Escriba el nombre de usuario y la contraseña.

Nota

Use la cuenta de administrador local o de dominio para iniciar sesión en el endpoint de destino. Si inicia sesión sin los derechos suficientes como "invitado" o "usuario normal", no podrá realizar la instalación.

d. Haga clic en **Aceptar**.

e. Haga clic en **Volver a preguntar si el inicio de sesión se realiza incorrectamente** para poder escribir el nombre de usuario y la contraseña otra vez durante el proceso de migración si no puede iniciar la sesión.

9. Haga clic en **Migrate**.

10. Si no seleccionó la opción **Reiniciar después de la instalación**, reinicie los equipos de destino para completar la migración.

Posterior a la instalación

Después del proceso de instalación, compruebe lo siguiente:

- *Acceso directo al agente de OfficeScan en la página 5-75*
- *Lista de programas en la página 5-76*
- *Servicios del agente de OfficeScan en la página 5-76*
- *Registros de instalación del agente de OfficeScan en la página 5-76*

Acceso directo al agente de OfficeScan

Los accesos directos al Agente de OfficeScan aparecen en el menú de Inicio del endpoint del agente.

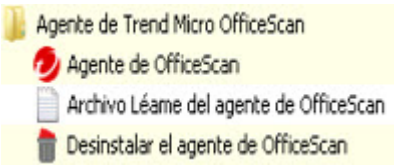


FIGURA 5-2. Acceso directo al Agente de OfficeScan

Nota

No está disponible en las plataformas de Windows 8, 8.1, 10 o Windows Server 2012, 2012 R2 y 2016.

Lista de programas

Agente de Trend Micro OfficeScan se encuentra en la lista **Agregar o quitar programas** en el panel de control del endpoint del agente.

Servicios del agente de OfficeScan

Los siguientes servicios del Agente de OfficeScan aparecen en **Microsoft Management Console**:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- Servicio proxy de OfficeScan NT (`TmProxy.exe`)

  Nota

  OfficeScan NT Proxy Service no existe en plataformas de Windows 7/8/8.1/10 o Windows Server 2008 R2/2012/2016.

- Cortafuegos de OfficeScan NT (`TmPfw.exe`); si se activó el cortafuegos durante la instalación
- Servicio de prevención de cambios no autorizados de Trend Micro (`TMBMSRV.exe`)
- Marco de soluciones del cliente habitual de Trend Micro (`TmCCSF.exe`)

Registros de instalación del agente de OfficeScan

El registro de instalación del Agente de OfficeScan (`OFCNT.LOG`) se puede encontrar en las siguientes ubicaciones:

- `%windir%` para todos los métodos de instalación excepto para la instalación del paquete MSI
- `%temp%` para el método de instalación del paquete MSI

Tareas posteriores a la instalación recomendadas

Trend Micro recomienda realizar las siguientes tareas posteriores a la instalación.

Actualizaciones de los componentes

Actualice los componentes del Agente de OfficeScan para asegurarse de que los agentes cuentan con la protección más actualizada frente a los riesgos de seguridad. Puede ejecutar las actualizaciones manuales del agente desde la consola Web o indicar a los usuarios que utilicen la función "Actualizar ahora" en sus equipos.

Exploración de prueba mediante la secuencia de comandos de prueba EICAR

El Instituto europeo de investigación antivirus (EICAR) ha desarrollado una secuencia de comandos de prueba para confirmar de forma segura la instalación y la configuración correctas del software antivirus. Visite el sitio Web de EICAR para obtener más información:

http://www.eicar.org

La secuencia de comandos de prueba EICAR es un archivo de texto inerte con una extensión `.com`. No es un virus y no contiene ningún fragmento de código de virus, pero la gran parte de los programas antivirus reaccionan ante él como si se tratara de un virus. Utilícelo para simular un incidente de virus y confirmar que las notificaciones por correo electrónico y los registros de virus funcionan correctamente.

¡ADVERTENCIA!

No utilice nunca virus reales para probar el producto antivirus.

Realización de una exploración de prueba

Procedimiento

1. Active la exploración en tiempo real en el agente.
2. Copie la siguiente cadena y péguela en el Bloc de notas, o en cualquier otro editor de texto sin formato: `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Guarde el archivo como `EICAR.com` en un directorio temporal. OfficeScan detecta el archivo de inmediato.
4. Para probar otros equipos de la red, adjunte el archivo EICAR.com a un mensaje de correo electrónico y envíelo a uno de los equipos.

Consejo

Trend Micro recomienda comprimir el archivo EICAR mediante un software habilitado para ello (como WinZip) y realizar a continuación otra prueba de exploración.

Desinstalación del Agente de OfficeScan

Hay dos formas de desinstalar el Agente de OfficeScan de los equipos:

- *Desinstalación del agente de OfficeScan desde la consola Web en la página 5-79*
- *Ejecución del programa de desinstalación del agente de OfficeScan en la página 5-81*

En caso de que no se pueda desinstalar el Agente de OfficeScan con los métodos mencionados anteriormente, desinstálelo manualmente. Para conocer más detalles, consulte *Desinstalación manual del agente de OfficeScan en la página 5-81*.

Desinstalación del agente de OfficeScan desde la consola Web

Desinstale el programa del Agente de OfficeScan desde la consola Web. Realice la desinstalación solo si experimenta problemas con el programa y vuelva a instalarlo inmediatamente para mantener el endpoint protegido frente a riesgos de seguridad.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Tareas** > **Desinstalación del agente**.
4. En la pantalla **Desinstalación del agente**, haga clic en **Iniciar la desinstalación**. El servidor envía una notificación a los agentes.
5. Compruebe el estado de la notificación y determine si hay agentes que no la recibieron.
   a. Haga clic en **Seleccionar los endpoints sin notificar** y, a continuación, haga clic en **Iniciar desinstalación** para volver a enviar la notificación de inmediato a los agentes que no la recibieron.
   b. Haga clic en **Detener desinstalación** para indicar a OfficeScan que deje de enviar la notificación a los agentes que ya la han recibido. Los agentes que ya han recibido la notificación y que ya están realizando la desinstalación ignorarán este comando.

Programa de desinstalación del agente de OfficeScan

Conceda a los usuarios el derecho de desinstalar el programa del Agente de OfficeScan y, después, indíqueles que ejecuten el programa de desinstalación del agente en sus equipos.

En función de cuál sea su configuración, puede que necesite una contraseña para la desinstalación. En caso de que necesite una contraseña, asegúrese de compartirla

únicamente con aquellos usuarios que vayan a ejecutar el programa de desinstalación y, después, modifíquela de inmediato si la ha divulgado a otros usuarios.

Conceder el derecho de desinstalación del agente de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Desinstalación**.
5. Para permitir la desinstalación sin contraseña, seleccione **Permitir a los usuarios desinstalar el agente de OfficeScan**. Si se precisa una contraseña, seleccione **Exigir una contraseña a los usuarios para desinstalar el agente de OfficeScan**, introdúzcala y, a continuación, confírmela.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Ejecución del programa de desinstalación del agente de OfficeScan

Procedimiento

1. En el menú **Iniciar** de Windows, haga clic en **Programas** > **Agente de Trend Micro OfficeScan** > **Desinstalar agente de OfficeScan**.

   También puede aplicar los siguientes pasos:

   a. Haga clic en **Panel de control** > **Agregar o quitar programas**.

   b. Localice **Agente de Trend Micro OfficeScan** y, a continuación, haga clic en **Cambiar**.

   c. Siga las instrucciones que aparecen en pantalla.

2. Escriba la contraseña de desinstalación en caso de que se le solicite. OfficeScan notifica al usuario sobre el progreso y la finalización de la desinstalación. No es necesario que el usuario reinicie el endpoint del agente para completar la desinstalación.

Desinstalación manual del agente de OfficeScan

Realice la desinstalación manual únicamente si tiene problemas para desinstalar el Agente de OfficeScan desde la consola Web o después de ejecutar el programa de desinstalación.

Procedimiento

1. Inicie sesión en el endpoint del agente con una cuenta que tenga derechos de administrador.

2. Haga clic con el botón derecho del ratón en el icono del Agente de OfficeScan de la bandeja del sistema y seleccione **Descargar OfficeScan**. Si se le solicita una contraseña, especifique la de descarga y, a continuación, haga clic en **Aceptar**.

Nota

- En Windows 8, 8.1, 10, Windows Server 2012 y Windows Server 2016, cambie al modo de escritorio para descargar el Agente de OfficeScan.
- Desactive la contraseña en los equipos en los que se vaya a descargar el Agente de OfficeScan. Para conocer más detalles, consulte *Configuración de derechos y otras configuraciones de los agentes en la página 15-99*.

3. En caso de que no se haya especificado la contraseña de descarga, detenga los siguientes servicios en la Consola de administración de Microsoft.
   - Servicio de escucha de OfficeScan NT
   - Cortafuegos de OfficeScan NT
   - Exploración en tiempo real de OfficeScan NT
   - Servicio proxy de OfficeScan NT

     Nota

     OfficeScan NT Proxy Service no existe en las plataformas de Windows 7, 8, 8.1, 10 o Windows Server 2008 R2, 2012 y 2016.

   - Servicio de prevención de cambios no autorizados de Trend Micro
   - Marco de soluciones del cliente habitual de Trend Micro
4. Elimine el acceso directo al Agente de OfficeScan del menú Inicio.
   - En Windows 8, 8.1, 10, Windows Server 2012 y Windows Server 2016:
     a. Cambie al modo de escritorio.
     b. Mueva el cursor del mouse a la esquina inferior derecha de la pantalla y haga clic en **Inicio** desde el menú que aparece.

        Aparecerá la pantalla **Inicio**.
     c. Haga clic con el botón derecho en **Trend Micro OfficeScan**.
     d. Haga clic en **Desanclar de Inicio**.

- En el resto de plataformas Windows:

  Haga clic en **Inicio** > **Programas**, haga clic con el botón derecho en **Agente de Trend Micro OfficeScan** y, a continuación, haga clic en **Eliminar**.

5. Abra el Editor del registro (`regedit.exe`).

¡ADVERTENCIA!

Para aplicar los siguientes pasos, es necesario que elimine las claves de registro. Realizar cambios incorrectos en el registro puede causar graves problemas en el sistema. Haga siempre una copia de seguridad antes de realizar cambios en el registro. Para obtener más información, consulte la ayuda del editor del registro.

6. Elimine las siguientes claves de registro:

   - En caso de que no haya ningún otro producto de Trend Micro instalado en el endpoint:

     - Para equipos de 32 bits:

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

     - Para equipos de 64 bits:

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`

   - En el caso de que sí haya otros productos de Trend Micro instalados en el endpoint, elimine solo las siguientes claves:

     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog`

       Para equipos de 64 bits:

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro \OfcWatchDog`

     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

Para equipos de 64 bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro
\PC-cillinNTCorp
```

7. Elimine las siguientes claves o valores de registro:

   - Para sistemas de 32 bits:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\OfficeScanNT`
     - Supervisor de OfficeScanNT (`REG_SZ`) en `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
   - Para sistemas de 64 bits:
     - `HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft \Windows\CurrentVersion\Uninstall\OfficeScanNT`
     - Supervisor de OfficeScanNT (`REG_SZ`) en `HKEY_LOCAL_MACHINE \SOFTWARE\ Wow6432Node\Microsoft\Windows \CurrentVersion\Run`

8. Elimine todas las instancias de las siguientes claves de registro en las ubicaciones que se indican a continuación:

   - Ubicaciones:
     - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
     - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`
   - Claves:
     - NTRtScan
     - tmccsf
     - tmcfw

- tmcomm
- TmFilter
- TmListen
- tmpfw
- TmPreFilter
- TmProxy

Nota

TmProxy no existe en las plataformas de Windows 7, 8, 8.1, 10 o Windows Server 2008 R2, 2012 y 2016.

- tmtdi

Nota

tmtdi no existe en las plataformas de Windows 7, 8, 8.1, 10 o Windows Server 2012 y 2016.

- VSApiNt
- tmlwf (para equipos con Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 y 2016)
- tmwfp (para equipos con Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 y 2016)
- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw (para equipos con Windows 7/8/8.1/10/Server 2008 R2/Server 2012)

- tmusa (para equipos con Windows 7, 8, 8.1, 10, Server 2008 R2, Server 2012 y 2016)
- tmnciesc
- tmeext (para Windows XP/2003)
- tmel (para equipos con Windows 8, 8.1, 10, Server 2012 y 2016)
- tmumh

9. Cierre el Editor del Registro.

10. Haga clic en **Iniciar** > **Configuración** > **Panel de control** y, a continuación, haga doble clic en **Sistema**.

Nota

Para sistemas con Windows 8, 8.1, 10, Windows Server 2012 y Windows Server 2016, omita este paso.

11. Haga clic en la pestaña **Hardware** y, a continuación, haga clic en **Administrador de dispositivos**.

Nota

Para sistemas con Windows 8, 8.1, 10, Windows Server 2012 y Windows Server 2016, omita este paso.

12. Haga clic en **Ver** > **Mostrar dispositivos ocultos**.

Nota

Para sistemas con Windows 8, 8.1, 10, Windows Server 2012 y Windows Server 2016, omita este paso.

13. Expanda **Controladores que no son Plug and Play** y, a continuación, desinstale los siguientes dispositivos (para Windows XP/Vista/7/Server 2003/Server 2008):

- tmactmon
- tmcomm

- TMEBC
- tmevtmgr
- TMUMH
- Filtro de Trend Micro
- Trend Micro PreFilter
- Controlador TDI de Trend Micro
- Trend Micro VSAPI NT
- Servicio de prevención de cambios no autorizados de Trend Micro
- Trend Micro WFP Callout Driver (para equipos con Windows Vista/Server 2008/7)

14. Elimine manualmente los controladores de Trend Micro a través de un editor de línea de comandos (Windows 8/8.1/10/Server 2012 solamente) con los siguientes comandos:

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`
- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`
- `sc delete tmumh`

- `sc delete tmccsf`
- `sc delete Tmnciesc`
- `sc delete tmlwf`

Nota

Ejecute el editor de línea de comandos mediante privilegios administrados (por ejemplo, haga clic con el botón derecho en `cmd.exe` y haga clic en **Ejecutar como administrador**) para asegurarse de que los comandos se ejecuten correctamente.

15. Desinstale el controlador del cortafuegos común.

a. Haga clic con el botón derecho del ratón en **Mis sitios de red** y, a continuación, haga clic en **Propiedades**.

b. Haga clic con el botón derecho del ratón en **Conexión de área local** y, a continuación, haga clic en **Propiedades**.

c. En la pestaña **General**, seleccione **driver del cortafuegos común de Trend Micro** y haga clic en **Desinstalar**.

Nota

Los siguientes pasos solo son aplicables a sistemas operativos Windows Vista, Server 2008, 7, 8, 8.1, 10 y Server 2012. Los agentes que utilicen cualquier otro sistema operativo deben ir directamente al paso 15.

d. Haga clic con el botón derecho del ratón en **Red** y haga clic en **Propiedades**.

e. Haga clic en **Administrar conexiones de red**.

f. Haga clic con el botón derecho del ratón en **Conexión de área local** y, a continuación, haga clic en **Propiedades**.

g. En la pestaña **Redes**, seleccione **Trend Micro NDIS 6.0 Filter Driver** y haga clic en **Desinstalar**.

16. Reinicie el endpoint del agente.

17. En caso de que no haya ningún otro producto de Trend Micro instalado en el endpoint, elimine la carpeta de instalación de `Trend Micro` (normalmente `C:`

`\Archivos de programa\Trend Micro`). En el caso de equipos de 64 bits, ésta puede encontrarse en `C:\Archivos de programa (x86)\\Trend Micro`.

18. En caso de que sí haya otros productos de Trend Micro instalados, elimine las siguientes carpetas:

- <*Carpeta de instalación del agente*>
- La carpeta `BM` de la carpeta de instalación de `Trend Micro` (normalmente se encuentra en `C:\Archivos de programa\Trend Micro\BM` para los sistemas de 32 bits y `C:\Archivos de programa (x86)\Trend Micro \BM` para los sistemas de 64 bits)

Capítulo 6

Mantener actualizada la protección

En este capítulo se describen los componentes y los procedimientos de actualización de OfficeScan.

Los temas que se incluyen son:

- *Componentes y programas de OfficeScan en la página 6-2*
- *Información general de actualizaciones en la página 6-13*
- *Actualizaciones del servidor de OfficeScan en la página 6-16*
- *Actualizaciones del Smart Protection Server Integrado en la página 6-29*
- *Actualizaciones del agente de OfficeScan en la página 6-30*
- *Agentes de actualización en la página 6-59*
- *Resumen de la actualización de componentes en la página 6-68*

Componentes y programas de OfficeScan

OfficeScan utiliza componentes y programas para proteger los equipos del agente de los últimos riesgos de seguridad. Utilice las actualizaciones manuales o programadas para mantener estos componentes y programas siempre actualizados.

Además de estos componentes, los agentes de OfficeScan también reciben los archivos del servidor de OfficeScan. Los agentes necesitan los archivos de configuración para aplicar la nueva configuración. Cada vez que se modifica la configuración de OfficeScan desde la consola Web también se modifican los archivos de configuración.

Los componentes se agrupan de la forma siguiente:

- *Componentes antivirus en la página 6-3*
- *Componentes antispyware en la página 6-7*
- *Componentes de Damage Cleanup Services en la página 6-7*
- *Componentes del cortafuegos en la página 6-8*
- *Componentes de supervisión de comportamiento en la página 6-8*
- *Componentes de las conexiones sospechosas en la página 6-10*
- *Solución de explotación del explorador en la página 6-10*
- *Programas en la página 6-10*
- *Componente de Reputación Web en la página 6-12*

Componentes antivirus

Componente	Descripción
Motor de exploración antivirus de 32 y 64 bits	El motor de exploración es el pilar en el que se fundamentan todos los productos de Trend Micro y se desarrolló como respuesta a los virus basados en archivos. El motor de exploración es en la actualidad muy sofisticado y es capaz de detectar varios tipos de virus y malware. El motor de exploración también detecta virus controlados que se crean y utilizan para investigar. Más que explorar cada uno de los bytes de cada archivo, lo que hacen el motor y el archivo de patrón es trabajar juntos para identificar lo siguiente: • Características delatoras del código de virus • La ubicación concreta en la que reside el virus dentro de un archivo
Patrón de virus	El patrón de virus contiene información que ayuda a los Agentes de OfficeScan a identificar los virus o el malware más recientes, así como los ataques de amenazas mixtas. Trend Micro crea y publica nuevas versiones del patrón de virus varias veces por semana y siempre que se detecta un virus o malware especialmente dañino.
controlador de exploración antivirus	Controlador de la exploración antivirus que supervisa las operaciones del usuario con los archivos. Las operaciones incluyen la apertura o el cierre de un archivo y la ejecución de una aplicación. Hay dos versiones de este controlador. Dichas versiones son `TmXPFlt.sys` y `TmPreFlt.sys`. `TmXPFlt.sys` se usa para la configuración en tiempo real del Motor de exploración antivirus, mientras que `TmPreFlt.sys` se usa para supervisar las operaciones de los usuarios. **Nota** Este componente no se muestra en la consola. Para comprobar la versión, vaya a <*Carpeta de instalación del servidor*>`\PCCSRV\Pccnt\Drv`. Haga clic con el botón derecho del ratón en el archivo `.sys`, seleccione **Propiedades** y vaya a la pestaña **Versión**.

COMPONENTE	DESCRIPCIÓN
Smart Scan Pattern Smart Scan Agent Pattern	En el modo Smart Scan, los Agentes de OfficeScan utilizan dos patrones ligeros que funcionan juntos para proporcionar la misma protección que ofrecen los patrones antimalware y antispyware convencionales. El **Smart Scan Pattern** contiene la mayoría de las definiciones de patrones. El **Smart Scan Agent Pattern** contiene todas las demás definiciones de patrones no halladas en el Smart Scan Pattern. El Agente de OfficeScan busca de amenazas de seguridad mediante **Smart Scan Agent Pattern**. Los Agentes de OfficeScan que no pueden determinar el riesgo del archivo durante la exploración comprueban el riesgo enviando una consulta de exploración al servidor de exploración, un servicio alojado en el Servidor de OfficeScan. El servidor de exploración verifica el riesgo usando el **Smart Scan Pattern**. El Agente de OfficeScan guarda en la caché el resultado de la consulta de exploración proporcionado por el servidor de exploración para mejorar el rendimiento de la exploración.
Patrón de IntelliTrap	El Patrón de IntelliTrap detecta los archivos de compresión en tiempo real empaquetados como archivos ejecutables. Para conocer más detalles, consulte *IntelliTrap en la página E-7*.
Patrón de excepciones de IntelliTrap	El Patrón de Excepciones de Intellitrap contiene una lista de archivos comprimidos "permitidos".

COMPONENTE	DESCRIPCIÓN
Patrón de inspección de la memoria	La exploración en tiempo real usa el patrón de inspección de memoria para evaluar los archivos comprimidos ejecutables que identifica la supervisión de comportamiento. La exploración en tiempo real lleva a cabo las siguientes acciones en los archivos comprimidos ejecutables: 1. Crea un archivo de asignación en la memoria después de verificar la ruta de la imagen del proceso. **Nota** La lista de exclusión de la exploración sobrescribe la exploración de archivos. 2. Envía el ID del proceso al servicio de protección avanzada que, a continuación: a. Usa el motor de exploración antivirus para explorar la memoria. b. Filtra el proceso a través de las listas de permitidos para archivos del sistema de Windows, archivos firmados digitalmente de fuentes fiables y archivos comprobados por Trend Micro. OfficeScan no realizará ninguna acción en los archivos una vez comprobada su seguridad. 3. Después de procesar la exploración de la memoria, el servicio de protección avanzada envía los resultados a la exploración en tiempo real. 4. La exploración en tiempo real pone en cuarentena las amenazas de malware que se hayan detectado y finaliza el proceso.
Motor de inteligencia contextual de 32/64 bits	El motor de inteligencia contextual supervisa los procesos que ejecutan los archivos de baja incidencia y extrae características de comportamiento que el controlador de consultas de inteligencia contextual envía al motor de aprendizaje automático predictivo para su análisis.
Patrón de inteligencia contextual	El patrón de inteligencia contextual contiene una lista de comportamientos permitidos que no son relevantes para ninguna amenaza conocida.

COMPONENTE	DESCRIPCIÓN
Controlador de consultas de inteligencia contextual de 32/64 bits	El controlador de consultas de inteligencia contextual procesa los comportamientos identificados por el motor de inteligencia contextual y envía el informe al motor de aprendizaje automático predictivo.
Motor de exploración de amenazas avanzadas de 32/64 bits	El motor de exploración de amenazas avanzadas extrae las característica de archivo de los archivos de baja incidencia y envía la información al motor de aprendizaje automático predictivo.
Patrón de correlación de amenazas avanzadas	El patrón de correlación de amenazas avanzadas contiene una lista de características de archivo que no son relevantes para ninguna amenaza conocida.

Actualizar el motor de exploración

Al almacenar la información más reciente sobre virus/malware en los patrones de virus, Trend Micro minimiza el número de actualizaciones del motor de exploración a la vez que mantiene la protección actualizada. No obstante, Trend Micro publica regularmente nuevas versiones del motor de exploración y las pone en circulación cuando:

- Se incorporan nuevas tecnologías de exploración y detección en el software.
- Se descubre un nuevo virus/malware potencialmente dañino que el motor de exploración no puede gestionar.
- Se mejora el rendimiento de la exploración.
- Se añaden formatos de archivo, lenguajes de secuencias de comandos, y formatos de codificación o compresión.

Componentes antispyware

Componente	Descripción
Patrón de spyware y grayware	El patrón de spyware/grayware identifica el spyware/grayware en archivos y programas, módulos de memoria, registro de Windows y accesos directos de URL.
Motor de exploración de spyware/grayware de 32/64 bits	El motor de exploración de spyware/grayware explora en busca de spyware/grayware y realiza la acción de exploración necesaria.
Patrón de supervisión activa de spyware	El patrón de supervisión activa de spyware se usa para explorar el spyware/grayware en tiempo real. Solo los agentes de exploración convencional utilizan este patrón. Los agentes Smart Scan utilizan Smart Scan Agent Pattern para la exploración de spyware/grayware en tiempo real. Los agentes envían consultas de exploración a un origen de Smart Protection si el riesgo del objetivo de la exploración no se puede determinar durante la exploración.

Componentes de Damage Cleanup Services

Componente	Descripción
Motor de Damage Cleanup de 32 y 64 bits	El motor de Damage Cleanup busca y elimina los troyanos y los procesos troyanos.
Plantilla de Damage Cleanup	El motor de Damage Cleanup utiliza la plantilla de Damage Cleanup para identificar los archivos y procesos troyanos, y poder eliminarlos.
Early Boot Cleanup Driver de 32/64 bits	El Early Boot Cleanup Driver de Trend Micro se carga antes de los controladores del sistema operativo, lo que permite detectar y bloquear los rootkits de arranque. Una vez se ha cargado el Agente de OfficeScan, el Early Boot Cleanup Driver de Trend Micro llama a Damage Cleanup Services para limpiar el rootkit.

Componentes del cortafuegos

Componente	Descripción
Controlador del cortafuegos habitual de 32/64 bits	El controlador del cortafuegos habitual se utiliza con el patrón del cortafuegos habitual para explorar los endpoints del agente en busca de virus de red. Este controlador es compatible con plataformas de 32 y 64 bits.
Patrón del cortafuegos habitual	Al igual que un patrón de virus, el patrón del cortafuegos habitual ayuda a los agentes a identificar firmas de virus, patrones exclusivos de bits y bytes que indican la presencia de un virus de red.

Componentes de supervisión de comportamiento

Componente	Descripción
Patrón de detección de la supervisión de comportamiento (32/64 bits)	Este patrón contiene las reglas de detección del comportamiento sospechoso de ser una amenaza.
Controlador básico de la supervisión del comportamiento de 32 y 64 bits	Este controlador en modo kernel supervisa los sucesos del sistema y los transmite al Servicio básico de la supervisión de comportamiento para la aplicación de las políticas.
Servicio básico de la supervisión de comportamiento de 32 y 64 bits	Este servicio en modo de usuario cuenta con las siguientes funciones: • Ofrece detección de rootkits • Regula el acceso a los dispositivos externos • Protege archivos, claves de Registro y servicios.
Patrón de configuración de la supervisión de comportamiento	El controlador de la supervisión de comportamiento utiliza este patrón para identificar los sucesos normales del sistema y los excluye de la aplicación de las políticas.

COMPONENTE	DESCRIPCIÓN
Patrón de firmas digitales	Este patrón contiene una lista de firmas digitales válidas que el Servicio básico de supervisión de comportamiento utiliza para determinar si el programa responsable del suceso de un sistema es o no seguro.
Patrón de aplicación de políticas	El servicio básico de la supervisión de comportamiento contrasta los sucesos del sistema con las políticas de este patrón.
Patrón del activador de exploración de memoria (32/64 bits)	La supervisión de comportamiento usa el patrón de activación de exploración de memoria para identificar posibles amenazas después de detectar las siguientes operaciones: • Acción de escritura de archivos • Acciones de escritura del registro • Creación de nuevos procesos Una vez identificada cualquiera de estas operaciones, la supervisión de comportamiento llama al patrón de inspección de memoria de la exploración en tiempo real para comprobar si existen riesgos de seguridad. Si desea más información sobre las operaciones de exploración en tiempo real, consulte *Patrón de inspección de memoria en la página 6-5*.
Patrón de Damage Recovery	El patrón de Damage Recovery contiene políticas que se utilizan para supervisar el comportamiento de amenazas sospechosas.
Patrón de supervisión de inspección del programa	El patrón de supervisión de inspección del programa supervisa y almacena los puntos de inspección que se utilizan para la supervisión de comportamiento.

Componentes de las conexiones sospechosas

Componente	Descripción
Lista de IP de C&C general	La lista de IP de C&C general funciona con el motor de examen de contenido de red (NCIE) para detectar las conexiones de red con los servidores de &C conocidos. El NCIE detecta el contacto con el servidor de C&C a través de cualquier canal de red. OfficeScan registra toda la información de conexión en los servidores de la lista IP de C&C global para su evaluación.
Patrón de regla de relevancia	El servicio Conexiones sospechosas usa el patrón de regla de relevancia para detectar firmas de familias de malware únicas localizadas en los encabezados de los paquetes de red.

Solución de explotación del explorador

Componente	Descripción
Patrón de prevención de explotación del explorador	Este patrón identifica las explotaciones más recientes del explorador Web e impide que se utilicen de forma que el explorador resulte comprometido.
Patrón unificado del analizador de secuencias de comando	Este patrón analiza las secuencias de comandos de las páginas Web e identifica las que son maliciosas.

Programas

Componente	Descripción
Agente de OfficeScan	El programa del Agente de OfficeScan ofrece protección frente a los riesgos de seguridad.

COMPONENTE	DESCRIPCIÓN
Archivos hotfix, parches y service packs	Tras la publicación oficial de un producto, Trend Micro suele desarrollar los siguientes elementos para solucionar algunos problemas, mejorar el rendimiento del producto o incluir nuevas características: • *Revisión en la página E-5* • *Parche en la página E-10* • *Revisión de seguridad en la página E-11* • *Service Pack en la página E-12* El distribuidor o proveedor de asistencia puede ponerse en contacto con el usuario cuando estos elementos están disponibles. Visite el sitio Web de Trend Micro para obtener más información sobre las nuevas publicaciones de archivos Hotfix, revisiones y service packs: http://downloadcenter.trendmicro.com/index.php?regs=ES Todas las publicaciones incluyen un archivo Léame que contiene información sobre la instalación, implementación y configuración. Lea detenidamente el archivo Léame antes de efectuar la instalación.

Historial de archivos hotfix y parches

Cuando el servidor de OfficeScan implementa archivos HotFix y revisiones en los Agentes de OfficeScan, el programa del Agente de OfficeScan registra la información relacionada con el archivo HotFix o la revisión en el editor del registro. Puede consultar dicha información de varios agentes utilizando software logístico del tipo de Microsoft SMS, LANDesk™ o BigFix™.

Nota

Esta función no registra los archivos hotfix y los parches que sólo se han implementado en el servidor.

Esta función está disponible desde OfficeScan 8.0 Service Pack 1 con el parche 3.1.

- Los agentes actualizados de la versión 8.0 Service Pack 1 con la revisión 3.1 o posterior registran los archivos HotFix y las revisiones instalados de la versión 8.0 y posteriores.
- Los agentes actualizados de las versiones anteriores a la versión 8.0 Service Pack 1 con la revisión 3.1 registran los archivos HotFix y las revisiones instalados de la versión 10.0 y posteriores.

La información se almacena en las siguientes claves:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- Para los equipos que ejecuten plataformas del tipo x64:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Compruebe las siguientes claves:

- **Clave**: `HotFix_installed`

  Tipo: `REG_SZ`

  Valor: `<Hot fix or patch name>`
- **Clave**: `HotfixInstalledNum`

  Tipo: `DWORD`

  Valor: `<Hot fix or patch number>`

Componente de Reputación Web

Componente	Descripción
Motor de filtrado de URL	El motor de filtrado de URL facilita la comunicación entre OfficeScan y el servicio de filtrado de URL de Trend Micro. El servicio de filtrado de URL es un sistema que clasifica las URL y proporciona información de clasificación a OfficeScan.

Información general de actualizaciones

Todas las actualizaciones de los componentes parten de Trend Micro ActiveUpdate Server. Cuando las actualizaciones están disponibles, el servidor de OfficeScan y las fuentes de Smart Protection (el Smart Protection Server o la Red de Smart Protection) descargan los componentes actualizados. No hay coincidencias de descarga de componentes entre las fuentes de Smart Protection y el servidor de OfficeScan, ya que cada uno de ellos descarga un conjunto de componentes específico.

Nota

Puede configurar tanto el servidor de OfficeScan como el Smart Protection Server para que se actualicen a partir de una fuente que no sea Trend Micro ActiveUpdate Server. Para ello, tiene que configurar una fuente de actualización personalizada. Si necesita ayuda a la hora de configurar esta fuente de actualización, póngase en contacto con el proveedor de asistencia.

Actualización del servidor de OfficeScan y el agente de OfficeScan

El servidor de OfficeScan descarga la mayoría de los componentes que los agentes necesitan. El único componente que no descarga es el Smart Scan Pattern, que lo descargan las fuentes de Smart Protection.

Si el servidor de OfficeScan gestiona un número elevado de agentes, es posible que la actualización utilice una cantidad considerable de recursos informáticos, lo que afecta a la estabilidad y el rendimiento del servidor. Para solucionar este problema, OfficeScan cuenta con una función de agente de actualización que permite que determinados agentes compartan la tarea de distribución de actualizaciones a otros agentes.

En la siguiente tabla se describen las diferentes opciones de actualización de componentes del servidor y los agentes de OfficeScan, así como recomendaciones sobre su uso:

TABLA 6-1. Opciones de actualización del agente y el servidor

OPCIÓN DE ACTUALIZACIÓN	DESCRIPCIÓN	RECOMENDACIÓN
Servidor ActiveUpdate > **Servidor** > **Agente**	El servidor de OfficeScan recibe los componentes actualizados de Trend Micro ActiveUpdate Server (u otro origen de actualización) e inicia la actualización de los componentes de los agentes.	Utilice este método si no hay secciones con anchos de banda reducidos entre el servidor y los agentes de OfficeScan.
Servidor ActiveUpdate > **Servidor** > **Agentes de actualización** > **Agente**	El servidor de OfficeScan recibe los componentes actualizados desde el ActiveUpdate Server (u otro origen de actualización), e inicia la actualización de los componentes de los agentes. Los agentes que actúan como agentes de actualización notifican a los agentes que deben actualizar sus componentes.	Si no hay secciones con anchos de banda reducidos entre el servidor y los agentes de OfficeScan, utilice este método para equilibrar la carga de tráfico en la red.
Servidor ActiveUpdate > **Agentes de actualización** > **Agente**	Los agentes de actualización reciben componentes actualizados directamente de ActiveUpdate Server (u otro origen de actualización), y notifican a los agentes que deben actualizar sus componentes.	Utilice este método solo si tiene problemas al actualizar agentes de actualización desde el servidor de OfficeScan o desde otros agentes de actualización. En circunstancias normales, los agentes de actualización reciben las actualizaciones más rápido desde el servidor de OfficeScan o desde otros agentes de actualización que desde una fuente de actualización externa.

Opción de actualización	Descripción	Recomendación
Servidor ActiveUpdate > Agente	Los agentes de OfficeScan reciben los componentes actualizados directamente de ActiveUpdate Server (u otro origen de actualización).	Utilice este método solo si tiene problemas al actualizar los agentes del servidor de OfficeScan o los agentes de actualización. En circunstancias normales, los agentes reciben actualizaciones del servidor de OfficeScan o de los agentes de actualización más rápido que desde un origen de actualización externa.

Actualización de la fuente de Smart Protection

Una fuente de Smart Protection (el Smart Protection Server o la Red de Smart Protection) descarga Smart Scan Pattern. Los agentes Smart Scan no descargan este patrón. Los agentes envían consultas de exploración al origen de Smart Protection para comprobar las posibles amenazas del patrón.

Nota

Consulte *Fuentes de Smart Protection en la página 4-6* para obtener más información sobre las fuentes de Smart Protection.

En la siguiente tabla se describe el proceso de actualización de las fuentes de Smart Protection.

Tabla 6-2. Proceso de actualización de la fuente de Smart Protection

Proceso de actualización	Descripción
Servidor ActiveUpdate > Smart Protection Network	Trend Micro Smart Protection Network recibe actualizaciones de Trend Micro ActiveUpdate Server. Los agentes Smart Scan que no están conectados a la red de empresa envían consultas a Trend Micro Smart Protection Network.

Proceso de actualización	Descripción
Servidor ActiveUpdate > **Smart Protection Server**	Un Smart Protection Server (integrado o independiente) recibe actualizaciones de Trend Micro ActiveUpdate Server. Los agentes de Smart Protection que no están conectados a la red empresarial envían consultas al servidor de Smart Protection Server.
Smart Protection Network > **Smart Protection Server**	Un Smart Protection Server (integrado o independiente) recibe actualizaciones de la Trend Micro Smart Protection Network. Los agentes de Smart Protection que no están conectados a la red empresarial envían consultas al servidor de Smart Protection Server.

Actualizaciones del servidor de OfficeScan

El servidor de OfficeScan descarga los siguientes componentes y los implementa en los agentes:

Tabla 6-3. Componentes descargados por el servidor de OfficeScan

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Antivirus		
Smart Scan Agent Pattern	No	Sí
Patrón de virus	Sí	No
Patrón de IntelliTrap	Sí	Sí
Patrón de excepciones de IntelliTrap	Sí	Sí
Motor de exploración antivirus de 32 y 64 bits	Sí	Sí
Patrón de inspección de la memoria	Sí	Sí

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Patrón antimalware de inicio temprano de 32/64 bits	Sí	Sí
Motor de inteligencia contextual de 32/64 bits	Sí	Sí
Patrón de inteligencia contextual	Sí	Sí
Controlador de consultas de inteligencia contextual de 32/64 bits	Sí	Sí
Motor de exploración de amenazas avanzadas de 32/64 bits	Sí	Sí
Patrón de correlación de amenazas avanzadas	Sí	Sí
Antispyware		
Patrón de spyware y grayware	Sí	Sí
Patrón de supervisión activa de spyware	Sí	No
Motor de exploración de spyware/ grayware de 32/64 bits	Sí	Sí
Damage Cleanup Services		
Plantilla de Damage Cleanup	Sí	Sí
Motor de Damage Cleanup de 32 y 64 bits	Sí	Sí
Early Boot Cleanup Driver de 32/64 bits	Sí	Sí
Cortafuegos		
Patrón del cortafuegos habitual	Sí	Sí

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Componentes de supervisión de comportamiento		
Patrón de detección de la supervisión de comportamiento (32/64 bits)	Sí	Sí
Controlador básico de la supervisión del comportamiento de 32 y 64 bits	Sí	Sí
Servicio básico de la supervisión de comportamiento de 32 y 64 bits	Sí	Sí
Patrón de configuración de la supervisión de comportamiento	Sí	Sí
Patrón de aplicación de políticas	Sí	Sí
Patrón de firmas digitales	Sí	Sí
Patrón del activador de exploración de memoria (32/64 bits)	Sí	Sí
Patrón de supervisión de inspección del programa	Sí	Sí
Patrón de Damage Recovery	Sí	Sí
Conexiones sospechosas		
Lista de IP de C&C general	Sí	Sí
Patrón de regla de relevancia	Sí	Sí
Solución de explotación del explorador		
Patrón de prevención de explotación del explorador	Sí	Sí
Patrón unificado del analizador de secuencias de comando	Sí	Sí

Recordatorios y consejos acerca de las actualizaciones:

- Para permitir que el servidor implemente los componentes actualizados en los agentes, active la actualización automática de agentes. Para conocer más detalles, consulte *Actualizaciones automáticas del agente de OfficeScan en la página 6-41*. Si se desactiva la actualización automática de agentes, el servidor descarga las actualizaciones, pero no las implementa en los agentes.
- Un servidor de OfficeScan que solo utilice IPv6 no puede distribuir actualizaciones directamente a agentes que únicamente utilicen IPv4. Del mismo modo, un servidor de OfficeScan que solo utilice IPv4 no puede distribuir actualizaciones directamente a agentes que únicamente utilicen IPv6. Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que el servidor de OfficeScan distribuya las actualizaciones a los agentes.
- Trend Micro publica archivos de patrones regularmente para mantener actualizada la protección de los agentes. Dada la frecuencia con la que se publican actualizaciones de archivos de patrones, OfficeScan utiliza un mecanismo denominado «duplicación de componentes» que permite descargar archivos de patrones con mayor rapidez. Consulte *Duplicación de componentes del servidor de OfficeScan en la página 6-22* para obtener más información.
- Si utiliza un servidor proxy para conectarse a Internet, utilice la configuración del proxy para descargar las actualizaciones correctamente.
- En el Panel de la consola Web, agregue el componente **Actualizaciones del agente** para ver las versiones actuales de los componentes y determinar el número de agentes con componentes actualizados y obsoletos.

Fuentes de actualización del servidor de OfficeScan

Configure el servidor de OfficeScan para que descargue los componentes de Trend Micro ActiveUpdate Server o de otra fuente. Puede especificar otra fuente si el servidor de OfficeScan no consigue acceder directamente al servidor ActiveUpdate. Para ver una situación de ejemplo, consulte *Actualizaciones del servidor de OfficeScan aislado en la página 6-25*.

Después de descargar las actualizaciones disponibles, el servidor puede solicitar automáticamente a los agentes que actualicen sus componentes en función de la

configuración especificada en **Actualizaciones** > **Agentes** > **Actualización automática**. Si la actualización de componentes es crítica, haga que el servidor de modo notifique a todos los agentes a la vez. Para ello, vaya a **Actualizaciones** > **Agentes** > **Actualización manual**.

Nota

Si no especifica un programa de implementación o una configuración de actualización activada por suceso en **Actualizaciones** > **Agentes** > **Actualización automática**, el servidor descargará las actualizaciones pero no notificará a los agentes que se deben actualizar.

Compatibilidad con IPv6 para las actualizaciones de servidores de OfficeScan

Un servidor de OfficeScan que solo utilice IPv6 no puede actualizarse directamente desde fuentes de actualización que utilicen únicamente IPv4, como:

- Trend Micro ActiveUpdate Server
- Una fuente de actualización personalizada que solo utilice IPv4.

Del mismo modo, un servidor de OfficeScan que solo utilice IPv4 no puede actualizarse directamente desde fuentes de actualización que utilicen IPv6.

Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir al servidor que se conecte a las fuentes de actualización.

Proxy para las actualizaciones del servidor de OfficeScan

Configure los programas del servidor que se alojan en el equipo del servidor para que utilicen la configuración del proxy a la hora de descargar actualizaciones de Trend Micro ActiveUpdate Server. Los programas del servidor incluyen el servidor de OfficeScan y el Smart Protection Server Integrado.

Configurar el proxy

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Proxy**.
2. Haga clic en la pestaña **Proxy externo**.
3. Vaya a la sección **Actualizaciones del servidor de OfficeScan**.
4. Seleccione **Utilizar un servidor proxy para las actualizaciones de patrones, motores y licencias**.
5. Especifique el protocolo de proxy, el nombre del servidor o la dirección IPv4/IPv6, y el número de puerto.
6. Si el servidor proxy necesita autenticación, escriba el nombre de usuario y la contraseña.
7. Haga clic en **Guardar**.

Configurar la fuente de actualización del servidor

Procedimiento

1. Vaya a **Actualizaciones** > **Servidor** > **Origen de actualización**.
2. Seleccione la ubicación desde donde desea descargar las actualizaciones de los componentes.

   Si selecciona el servidor ActiveUpdate, asegúrese de que el servidor tiene conexión a Internet y, en el caso de utilizar un servidor proxy, compruebe si la conexión a Internet se puede establecer utilizando la configuración del proxy. Para conocer más detalles, consulte *Proxy para las actualizaciones del servidor de OfficeScan en la página 6-20*.

   Si selecciona una fuente de actualización personalizada, configure el entorno correspondiente y actualice los recursos de esta fuente de actualización. Además, asegúrese de que existe conexión entre el equipo servidor y la fuente de

actualización. Si necesita ayuda a la hora de configurar una fuente de actualización, póngase en contacto con el proveedor de asistencia.

Nota

El servidor de OfficeScan utiliza la duplicación de componentes cuando descarga componentes de la fuente de actualización. Consulte *Duplicación de componentes del servidor de OfficeScan en la página 6-22* para obtener más información.

3. Haga clic en **Guardar**.

Duplicación de componentes del servidor de OfficeScan

Cuando la última versión de un archivo de patrones completo está disponible para su descarga desde el servidor ActiveUpdate de Trend Micro, también lo están 14 "patrones incrementales". Los patrones incrementales con versiones reducidas del archivo de patrones completo que representan la diferencia entre la última versión del archivo de patrones completo y la versión anterior. Por ejemplo, si la última versión es 175, el patrón incremental v_173.175 contiene las firmas de la versión 175 que no se encuentran en la versión 173 (la versión 173 es la versión anterior del archivo de patrones completo, ya que los números de patrones se publican con incrementos de 2). El patrón incremental v_171.175 contiene las firmas de la versión 175 que no se encuentran en la versión 171.

Para reducir el tráfico de red generado al descargar el último patrón, OfficeScan ejecuta una duplicación de componentes, que es un método de actualización de componentes en el que el servidor de OfficeScan o el agente de actualización solo descarga patrones incrementales. Consulte *Duplicación de los componentes del agente de actualización en la página 6-65* para obtener información acerca de cómo realizan los agentes de actualización la duplicación de los componentes.

La duplicación de componentes se aplica a los componentes siguientes:

- Patrón de virus
- Smart Scan Agent Pattern
- Plantilla de Damage Cleanup

- Patrón de excepciones de IntelliTrap
- Patrón de spyware y grayware
- Patrón de supervisión activa de spyware

Escenario de duplicación de componentes

Para entender mejor la duplicación de componentes del servidor, consulte el siguiente escenario:

TABLA 6-4. Situación de duplicación de componentes del servidor

Patrones completos en el servidor de OfficeScan	Versión actual: 171 Otras versiones disponibles: 169	167	165	161	159	
Última versión en el servidor ActiveUpdate	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. El servidor de OfficeScan compara la versión actual de los patrones completos con la última versión que hay en el servidor ActiveUpdate. Si la diferencia entre ambas versiones es 14 o menos, el servidor solo descarga el patrón incremental que representa la diferencia entre ambas versiones.

   Nota

   Si la diferencia es mayor que 14, el servidor descarga automáticamente la versión completa del archivo de patrones y 14 patrones incrementales.

   Para ilustrarlo según los datos del ejemplo:

   - La diferencia entre las versiones 171 y 175 es 2. Dicho de otro modo, el servidor no tiene las versiones 173 y 175.
   - El servidor descarga el patrón incremental 171.175. El patrón incremental representa la diferencia entre las versiones 171 y 175.

2. El servidor combina el patrón incremental con su patrón completo actual para general el último patrón completo.

   Para ilustrarlo según los datos del ejemplo:

   - En el servidor, OfficeScan combina la versión 171 con el patrón incremental 171.175 para generar la versión 175.
   - El servidor tiene 1 patrón incremental (171.175) y el último patrón completo (versión 175).

3. El servidor genera patrones incrementales a partir de los demás patrones completos disponibles en el servidor. Si el servidor no genera estos patrones incrementales, los agentes que no pudieron descargar los patrones incrementales anteriores descargarán automáticamente el archivo de patrones completo, de modo que se generará más tráfico de red.

   Para ilustrarlo según los datos del ejemplo:

   - Dado que el servidor tiene las versiones de patrones 169, 167, 165, 163, 161, 159, puede generar los siguientes patrones incrementales:

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - El servidor no necesita utilizar la versión 171 porque ya tiene el patrón incremental 171.175.
   - El servidor tiene ahora 7 patrones incrementales:

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Este servidor conserva las últimas 7 versiones de patrones completos (versiones 175, 171, 169, 167, 165, 163, 161). Elimina cualquier versión anterior (versión 159).

4. El servidor compara sus patrones incrementales actuales con los patrones incrementales disponibles en el servidor ActiveUpdate. A continuación, descarga los patrones incrementales que no tiene.

   Para ilustrarlo según los datos del ejemplo:

   - El servidor ActiveUpdate tiene 14 patrones incrementales:

173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- El servidor de OfficeScan tiene 7 patrones incrementales:

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- El servidor de OfficeScan descarga 7 patrones incrementales adicionales:

  173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- Ahora el servidor tiene todos los patrones incrementales disponibles en el servidor ActiveUpdate.

5. El último patrón completo y los 14 patrones incrementales están a disposición de los agentes.

Actualizaciones del servidor de OfficeScan aislado

Si el servidor de OfficeScan pertenece a una red completamente aislada de las fuentes externas, puede mantener los componentes del servidor actualizados mediante una fuente interna que contenga los componentes más recientes.

En este tema se describen las tareas necesarias para actualizar un servidor de OfficeScan aislado.

Actualización de un servidor de OfficeScan aislado

Este procedimiento se incluye para que le sirva como referencia. Si no consigue llevar a cabo todas las tareas de este procedimiento, consulte a su proveedor de asistencia para que le indique los pasos detallados de cada tarea.

Procedimiento

1. Identifique la fuente de actualización, por ejemplo Trend Micro Control Manager o un equipo host cualquiera. La fuente de actualización debe tener:

   - Una conexión a Internet fiable para poder descargar los componentes más recientes de Trend Micro ActiveUpdate Server. Sin conexión a Internet, la única forma de que la fuente de actualización cuente con los componentes

más recientes es que usted mismo los obtenga de Trend Micro y, a continuación, los copie en la fuente de actualización.

- Una conexión operativa con el servidor de OfficeScan. Defina los parámetros del proxy si existe un servidor proxy entre el servidor de OfficeScan y la fuente de actualización. Para conocer más detalles, consulte *Proxy para las actualizaciones del servidor de OfficeScan en la página 6-20*.
- Espacio en disco suficiente para los componentes descargados.

2. Dirija el servidor de OfficeScan a la nueva fuente de actualización. Para conocer más detalles, consulte *Fuentes de actualización del servidor de OfficeScan en la página 6-19*.

3. Identifique los componentes que el servidor implementa en los agentes. Para obtener una lista de los componentes implementables, consulte *Actualizaciones del agente de OfficeScan en la página 6-30*.

Consejo

Una de las formas de determinar si un componente se está implementando en los agentes es ir a la pantalla **Resumen de actualización** de la consola Web (**Actualizaciones** > **Resumen**). En esta pantalla, la velocidad de actualización de un componente que se está implementando será siempre mayor que el 0%.

4. Determine la frecuencia de la descarga de componentes. Los archivos de patrones se actualizan con frecuencia (algunos de ellos a diario), por lo que es recomendable actualizarlos con regularidad. En el caso de motores y unidades, puede solicitar a su proveedor de asistencia que le notifique acerca de las actualizaciones más importantes.

5. En la fuente de actualización:

   a. Conecte con el servidor ActiveUpdate. La URL del servidor depende de la versión de OfficeScan.

   b. Descargue los elementos siguientes:

      - El archivo `server.ini`. Este archivo contiene información acerca de los componentes más recientes.
      - Los componentes que ha identificado en el paso 3.

c. Guarde los elementos descargados en un directorio de la fuente de actualización.

6. Realice una actualización manual del servidor de OfficeScan. Para conocer más detalles, consulte *Actualizar el servidor de OfficeScan de forma manual en la página 6-27*.

7. Repita del paso 5 al paso 6 cada vez que necesite actualizar componentes.

Métodos de actualización del servidor de OfficeScan

Actualice los componentes del servidor de OfficeScan de forma manual o configure un programa de actualización.

Para permitir que el servidor implemente los componentes actualizados en los agentes, active la actualización automática de agentes. Para conocer más detalles, consulte *Actualizaciones automáticas del agente de OfficeScan en la página 6-41*. Si se desactiva la actualización automática de agentes, el servidor descarga las actualizaciones, pero no las implementa en los agentes.

Los métodos de actualización son:

- **Actualización manual del servidor**: cuando una actualización es crítica, realice una actualización manual para que las actualizaciones se puedan incorporar al servidor inmediatamente. Consulte *Actualizar el servidor de OfficeScan de forma manual en la página 6-27* para obtener más información.
- **Actualización programada del servidor**: el servidor de OfficeScan se conecta al origen de actualización el día y la hora programados para obtener los componentes más recientes. Consulte *Programación de actualizaciones para el servidor de OfficeScan en la página 6-28* para obtener más información.

Actualizar el servidor de OfficeScan de forma manual

Actualice manualmente los componentes del servidor de OfficeScan después de instalar o actualizar el servidor y siempre que haya una epidemia.

Procedimiento

1. Vaya a **Actualizaciones** > **Servidor** > **Actualización manual**.
2. Seleccione los componentes que desee actualizar.
3. Haga clic en **Actualizar**.

   El servidor descargará los componentes actualizados.

Programación de actualizaciones para el servidor de OfficeScan

Configure el servidor de OfficeScan para que compruebe de forma regular su fuente de actualización y descargue automáticamente las actualizaciones disponibles. Puesto que los agentes suelen obtener las actualizaciones del servidor, utilizar la actualización programada es una forma fácil y eficaz de garantizar que la protección frente a riesgos de seguridad está siempre actualizada.

Procedimiento

1. Vaya a **Actualizaciones** > **Servidor** > **Actualización programada**.
2. Seleccione **Activar la actualización programada del servidor de OfficeScan**.
3. Seleccione los componentes que desee actualizar.
4. Especifique el programa de actualización.

   Para actualizaciones diarias, semanales y mensuales el periodo de tiempo corresponde al número de horas durante las que OfficeScan realizará la actualización. OfficeScan se actualizará en cualquier momento durante este periodo.
5. Haga clic en **Guardar**.

Registros de actualización del servidor de OfficeScan

Compruebe los registros de actualización del servidor para determinar si hay algún problema a la hora de actualizar determinados componentes. En los registros se incluyen las actualizaciones de los componentes del servidor de OfficeScan.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de los registros de actualización

Procedimiento

1. Vaya a **Registros** > **Actualización del servidor**.
2. Compruebe la columna **Resultado** para ver si hay componentes que no se han actualizado.
3. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Actualizaciones del Smart Protection Server Integrado

El Smart Protection Server integrado descarga dos componentes: el Smart Scan Pattern y la Lista de bloqueo Web. Para obtener información detallada acerca de estos componentes y cómo actualizarlos, consulte *Administración del Smart Protection Server Integrado en la página 4-19*.

Actualizaciones del agente de OfficeScan

Para garantizar la protección de los agentes frente a los últimos riesgos de seguridad, actualice los componentes del agente de forma regular.

Antes de actualizar los agentes, compruebe si el origen de actualización (el servidor de OfficeScan o un origen de actualización personalizado) tiene los componentes más recientes. Para obtener información sobre cómo actualizar el servidor de OfficeScan, consulte *Actualizaciones del servidor de OfficeScan en la página 6-16*.

En la siguiente tabla se recogen todos los componentes que implementan las fuentes de actualización en los agentes y los componentes que se utilizan en un método de exploración concreto.

TABLA 6-5. Componentes de OfficeScan implementados en los agentes

COMPONENTE	DISTRIBUCIÓN	
	AGENTES DE EXPLORACIÓN CONVENCIONAL	AGENTES SMART SCAN
Antivirus		
Smart Scan Agent Pattern	No	Sí
Patrón de virus	Sí	No
Patrón de IntelliTrap	Sí	Sí
Patrón de excepciones de IntelliTrap	Sí	Sí
Motor de exploración antivirus de 32 y 64 bits	Sí	Sí
Patrón de inspección de la memoria	Sí	Sí
Patrón antimalware de inicio temprano de 32/64 bits	Sí	Sí
Motor de inteligencia contextual de 32/64 bits	Sí	Sí

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Patrón de inteligencia contextual	Sí	Sí
Controlador de consultas de inteligencia contextual de 32/64 bits	Sí	Sí
Motor de exploración de amenazas avanzadas de 32/64 bits	Sí	Sí
Patrón de correlación de amenazas avanzadas	Sí	Sí
Antispyware		
Patrón de spyware y grayware	Sí	Sí
Patrón de supervisión activa de spyware	Sí	No
Motor de exploración de spyware/ grayware de 32/64 bits	Sí	Sí
Damage Cleanup Services		
Plantilla de Damage Cleanup	Sí	Sí
Motor de Damage Cleanup de 32 y 64 bits	Sí	Sí
Early Boot Cleanup Driver de 32/64 bits	Sí	Sí
Servicios de reputación Web		
Motor de filtrado de URL	Sí	Sí
Cortafuegos		
Patrón del cortafuegos habitual	Sí	Sí

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Controlador del cortafuegos habitual de 32/64 bits	Sí	Sí
Componentes de supervisión de comportamiento		
Patrón de detección de la supervisión de comportamiento (32/64 bits)	Sí	Sí
Controlador básico de la supervisión del comportamiento de 32 y 64 bits	Sí	Sí
Servicio básico de la supervisión de comportamiento de 32 y 64 bits	Sí	Sí
Patrón de configuración de la supervisión de comportamiento	Sí	Sí
Patrón de aplicación de políticas	Sí	Sí
Patrón de firmas digitales	Sí	Sí
Patrón del activador de exploración de memoria (32/64 bits)	Sí	Sí
Patrón de supervisión de inspección del programa	Sí	Sí
Patrón de Damage Recovery	Sí	Sí
Conexiones sospechosas		
Lista de IP de C&C general	Sí	Sí
Patrón de regla de relevancia	Sí	Sí
Solución de explotación del explorador		
Patrón de prevención de explotación del explorador	Sí	Sí

Componente	Distribución	
	Agentes de exploración convencional	Agentes Smart Scan
Patrón unificado del analizador de secuencias de comando	Sí	Sí

Orígenes de actualización de los agentes de OfficeScan

Los agentes pueden obtener actualizaciones del origen de actualización estándar (el servidor de OfficeScan) o componentes específicos de orígenes de actualización personalizados, como Trend Micro ActiveUpdate Server. Para conocer más detalles, consulte *Origen de actualización estándar de los agentes de OfficeScan en la página 6-34* y *Orígenes de actualización personalizadas para los agentes de OfficeScan en la página 6-35*.

IPv6 Support for actualizaciones del agente de OfficeScan

Un agente que solo utiliza IPv6 no puede actualizarse directamente desde orígenes de actualización que utilizan únicamente IPv4, como:

- Un servidor de OfficeScan que solo utilice IPv4
- Un agente de actualización que solo utilice IPv4
- Una fuente de actualización personalizada que solo utilice IPv4.
- Trend Micro ActiveUpdate Server

De modo similar, un agente que solo utiliza IPv4 no puede actualizarse directamente desde orígenes de actualización que utilizan únicamente IPv6, como un servidor o un agente de actualización de OfficeScan de solo IPv6.

Se necesita un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que los agentes se conecten a los orígenes de actualización.

Origen de actualización estándar de los agentes de OfficeScan

El servidor de OfficeScan es el origen de actualización estándar de los agentes.

Si no se puede acceder al servidor de OfficeScan, los agentes no tendrán origen de copia de seguridad y, por tanto, quedarán obsoletos. Para actualizar los agentes que no pueden acceder al servidor de OfficeScan, Trend Micro recomienda usar Agent Packager. Utilice esta herramienta para crear un paquete con los componentes más recientes en el servidor y, a continuación, ejecútelo en los agentes.

Nota

La dirección IP del agente (IPv4 o IPv6) determina si se puede establecer la conexión con el servidor de OfficeScan. Para obtener más información sobre la compatibilidad de IPv6 con las actualizaciones de agente, consulte *IPv6 Support for actualizaciones del agente de OfficeScan en la página 6-33*.

Configurar el origen de actualización estándar de los agentes de OfficeScan

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Origen de actualización**.
2. Seleccione **Fuente de actualización estándar (actualizar desde el servidor de OfficeScan)**.
3. Haga clic en **Notificar a todos los agentes**.

Proceso de actualización del agente de OfficeScan

Nota

En este tema se describe el proceso de actualización de los Agentes de OfficeScan. Los procesos de actualización de los agentes de actualización se tratan en *Origen de actualización estándar de los agentes de OfficeScan en la página 6-34*.

Si configura los Agentes de OfficeScan de modo que se actualicen directamente desde el servidor de OfficeScan, el proceso de actualización se realiza de la siguiente forma:

1. El Agente de OfficeScan obtiene las actualizaciones desde el servidor de OfficeScan.

2. Si no se puede actualizar desde el servidor de OfficeScan, el Agente de OfficeScan intenta conectar directamente con Trend Micro ActiveUpdate Server si la opción **Los agentes de OfficeScan descargan actualizaciones desde Trend Micro ActiveUpdate Server** está activada en **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones (pestaña)** > **Configuración de actualización**.

Nota

Solo los componentes se pueden actualizar desde el servidor ActiveUpdate. La configuración de dominios, los programas y los archivos hotfix solo se pueden descargar del servidor de OfficeScan o los agentes de actualización. Puede acelerar el proceso de actualización configurando los Agentes de OfficeScan de modo que solo descarguen archivos de patrones de ActiveUpdate Server. Para obtener más información, consulte *ActiveUpdate Server como el origen de actualización del agente de OfficeScan en la página 6-40*.

Orígenes de actualización personalizadas para los agentes de OfficeScan

Además del servidor de OfficeScan, los Agentes de OfficeScan cuentan con orígenes de actualización personalizados para actualizarse. Los orígenes de actualización personalizados ayudan a reducir el tráfico de actualización de los agentes que se envía al servidor de OfficeScan y permite a los Agentes de OfficeScan que no se pueden conectar al servidor de OfficeScan actualizarse convenientemente. Especifique las fuentes de actualización personalizadas en la Lista de fuentes de actualización personalizadas, en la que se pueden incluir un máximo de 1.024 fuentes de actualización.

Consejo

Trend Micro recomienda que se asignen algunos Agentes de OfficeScan como agentes de actualización y que se los incluya en la lista.

Configuración de orígenes de actualización personalizados para agentes de OfficeScan

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Origen de actualización**.
2. Seleccione **Fuente de actualización personalizada** y haga clic en **Añadir**.
3. En la pantalla que aparece, especifique las direcciones IP de los agentes. Puede escribir un intervalo de direcciones IPv4, y un prefijo y una longitud de IPv6.
4. Especifique la fuente de actualización. Puede seleccionar un Agente de actualización si ha asignado alguno o escribir la URL de una fuente determinada.

   Nota

   Asegúrese de que los Agentes de OfficeScan se pueden conectar al origen de actualización mediante sus direcciones IP. Por ejemplo, si ha especificado un intervalo de direcciones IPv4, la fuente de actualización debe tener una dirección IPv4. Si ha especificado un prefijo y una longitud de IPv6, la fuente de actualización debe tener una dirección IPv6. Para obtener más información sobre la compatibilidad de IPv6 con las actualizaciones de agente, consulte *Orígenes de actualización de los agentes de OfficeScan en la página 6-33*.

5. Haga clic en **Guardar**.
6. Lleve a cabo tareas varias en la pantalla.

   a. Seleccione una de las siguientes configuraciones. Para obtener información detallada acerca del modo de funcionamiento de estas configuraciones, consulte *Proceso de actualización del agente de OfficeScan en la página 6-34*.

   - **Los agentes de actualización actualizan los componentes, la configuración del dominio, los programas del agente y los archivos Hotfix solo desde el servidor de OfficeScan**
   - Los agentes de OfficeScan actualizan los siguientes elementos desde el servidor de OfficeScan si los orígenes personalizados no se encuentran o no están disponibles:

- **Componentes**
- **Configuración del dominio**
- **Programas y archivos Hotfix del agente de OfficeScan**

b. Si ha especificado al menos un agente de actualización como origen, haga clic en **Informe analítico del agente de actualización** para generar un informe que indique el estado de actualización de los agentes. Si desea obtener información detallada acerca del informe, consulte *Informe analítico del agente de actualización en la página 6-67*.

c. Puede editar una fuente de actualización haciendo clic en el enlace del intervalo de direcciones IP. Modifique la configuración en la pantalla que aparece y haga clic en **Guardar**.

d. Para eliminar una fuente de actualización de la lista, active la casilla de verificación y haga clic en **Eliminar**.

e. Para mover una fuente de actualización, haga clic en la flecha hacia arriba/abajo. Las fuentes solo se pueden mover de una en una.

7. Haga clic en **Notificar a todos los agentes**.

Proceso de actualización del agente de OfficeScan

Nota

En este tema se describe el proceso de actualización de los Agentes de OfficeScan. Los procesos de actualización de los agentes de actualización se tratan en *Fuentes de actualización personalizadas para los agentes de actualización en la página 6-63*.

Una vez que haya establecido y guardado la lista de fuentes de actualización personalizada, el proceso de actualización se realizará de la siguiente manera:

1. El Agente de OfficeScan se actualiza a partir del primer origen de la lista.
2. Si no se puede realizar la actualización desde el primer origen de la lista, el Agente de OfficeScan pasa a la segunda y así sucesivamente.

3. Si no se puede actualizar desde ningún origen, el Agente de OfficeScan comprueba la siguiente configuración de la pantalla **Origen de actualización**:

TABLA 6-6. Configuración adicional para las fuentes de actualización personalizadas

PARÁMETRO	DESCRIPCIÓN
Los agentes de actualización actualizan los componentes, la configuración del dominio, los programas del agente y los archivos Hotfix solo desde el servidor de OfficeScan	Si esta configuración está activada, los agentes de actualización se actualizan directamente desde el servidor de OfficeScan y omiten la Lista de fuentes de actualización personalizadas. Si está desactivada, los agentes de actualización aplican la configuración del origen de actualización personalizado que se ha configurado para agentes normales.
Los agentes de OfficeScan actualizan los siguientes elementos desde el servidor de OfficeScan si los orígenes personalizados no se encuentran o no están disponibles:	

PARÁMETRO	DESCRIPCIÓN
Componentes	Si se activa esta opción, el agente actualiza los componentes desde el servidor de OfficeScan. Si no está activada, el agente trata de conectarse directamente al Trend Micro ActiveUpdate Server en el caso de darse cualquiera de estas circunstancias: • La opción **Los agentes de OfficeScan descargan actualizaciones desde Trend Micro ActiveUpdate Server** está activada en **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones (pestaña)** > **Configuración de actualización**. • El servidor ActiveUpdate Server no está incluido en la lista de fuentes de actualización personalizadas. **Nota** Solo los componentes se pueden actualizar desde el servidor ActiveUpdate. La configuración de dominios, los programas y los archivos hotfix solo se pueden descargar del servidor de OfficeScan o los agentes de actualización. Puede acelerar el proceso de actualización configurando los agentes de modo que solo descarguen archivos de patrones de ActiveUpdate Server. Para obtener más información, consulte *ActiveUpdate Server como el origen de actualización del agente de OfficeScan en la página 6-40*.
Configuración del dominio	Si se activa esta opción, el agente actualiza la configuración del nivel del dominio desde el servidor de OfficeScan.
Programas y archivos Hotfix del agente de OfficeScan	Si se activa esta opción, el agente actualiza los programas y archivos HotFix desde el servidor de OfficeScan.

4. Si no se puede realizar la actualización desde ninguno de los orígenes posibles, el agente abandona el proceso de actualización.

ActiveUpdate Server como el origen de actualización del agente de OfficeScan

Si los Agentes de OfficeScan descargan las actualizaciones directamente desde Trend Micro ActiveUpdate Server, puede limitar la descarga solo a los archivos de patrones para reducir el ancho de banda que se consume durante las actualizaciones y acelerar el proceso de actualización.

Los motores de exploración y otros componentes no se actualizan con tanta frecuencia como los archivos de patrones, lo que constituye una razón más para limitar la descarga únicamente a los patrones.

Un agente que solo utilice IPv6 no puede actualizarse directamente desde Trend Micro ActiveUpdate Server. Se necesita un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que los Agentes de OfficeScan se conecten al servidor ActiveUpdate.

Limitación de las descargas del ActiveUpdate Server

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Sistema**.
3. Vaya a la sección **Actualizaciones**.
4. Seleccione **Descargar solo los archivos de patrones del servidor ActiveUpdate al llevar a cabo las actualizaciones**.

Métodos de actualización de los agentes de OfficeScan

Los Agentes de OfficeScan que actualizan componentes desde el servidor de OfficeScan o un origen de actualización personalizado pueden utilizar los siguientes métodos de actualización:

- **Actualizaciones automáticas**: la actualización del agente se ejecuta automáticamente cuando ocurren determinados sucesos o en función de un

programa. Para conocer más detalles, consulte *Actualizaciones automáticas del agente de OfficeScan en la página 6-41*.

- **Actualizaciones manuales**: si se trata de una actualización crítica, utilice la actualización manual para notificar a los agentes de manera inmediata de que deben actualizar el componente. Para conocer más detalles, consulte *Actualizaciones manuales del agente en la página 6-48*.

- **Actualizaciones según derechos**: los usuarios con derechos de actualización tienen mayor control sobre la forma en la que se actualiza el Agente de OfficeScan en sus equipos. Para conocer más detalles, consulte *Configurar los derechos y otras configuraciones de la actualización en la página 6-50*.

Actualizaciones automáticas del agente de OfficeScan

La opción Actualización automática le evita tener que informar a todos los agentes de que deben actualizarse y elimina el riesgo de que los componentes de los equipos agente no estén actualizados.

Además de estos componentes, los Agentes de OfficeScan también reciben los archivos de configuración actualizados durante la actualización automática. Los agentes necesitan los archivos de configuración para aplicar la nueva configuración. Cada vez que se modifica la configuración de OfficeScan desde la consola Web también se modifican los archivos de configuración. Para determinar la frecuencia con la que se aplican los archivos de configuración a los agentes, consulte el paso 3 *Configuración de las actualizaciones automáticas del agente de OfficeScan en la página 6-43*.

Nota

Puede configurar los agentes para que utilicen la configuración del proxy durante la actualización automática. Consulte *Proxy para las actualizaciones de componentes del agente de OfficeScan en la página 6-53* para obtener más información.

Existen dos tipos de actualizaciones automáticas:

- *Actualizaciones activadas por suceso en la página 6-42*
- *Actualizaciones según programa en la página 6-43*

Actualizaciones activadas por suceso

Después de descargar los componentes más recientes, el servidor puede enviar notificaciones a los agentes en línea (así como a los agentes sin conexión en el momento en el que reinician y se conectan al servidor) para que actualicen sus componentes. Opcionalmente, es posible iniciar la función Explorar ahora (exploración manual) en los endpoints del Agente de OfficeScan después de la actualización.

TABLA 6-7. Opciones de actualización activada por suceso

OPCIÓN	DESCRIPCIÓN
Iniciar la actualización de los componentes en los agentes inmediatamente después de que el servidor de OfficeScan descargue un componente nuevo	El servidor notifica a los agentes que deben actualizarse en el momento en el que este completa una actualización. Los agentes que se actualizan con frecuencia solo tienen que descargar patrones incrementales, lo que reduce el tiempo que lleva la actualización (consulte *Duplicación de componentes del servidor de OfficeScan en la página 6-22* para obtener más información sobre los patrones incrementales). No obstante, las actualizaciones frecuentes pueden afectar negativamente al rendimiento del servidor, especialmente si se actualiza un gran número de agentes al mismo tiempo. Si existen agentes que están en modo independiente y también quiere actualizarlos, seleccione **Incluir agentes independientes y sin conexión**. Consulte *Derecho del modo independiente del Agente de OfficeScan en la página 15-20* para obtener más información acerca del modo independiente.
Permitir que los agentes inicien la actualización de los componentes después de reiniciarse y conectarse al servidor de OfficeScan (se excluyen los agentes independientes)	Un agente que haya perdido una actualización descarga los componentes inmediatamente después de establecer la conexión con el servidor. El agente puede perder actualizaciones si está desconectado o si el endpoint en el que está instalado no se está ejecutando.

OPCIÓN	DESCRIPCIÓN
Ejecutar la función Explorar ahora después de la actualización (excepto los agentes independientes)	El servidor informa a los agentes de que deben realizar una exploración después de una actualización activada por suceso. Considere habilitar esta opción si como respuesta a un riesgo de seguridad que se ha extendido por la red se ha ejecutado una actualización en concreto.

Nota

Si el servidor de OfficeScan no puede enviar correctamente una notificación de actualización a los agentes después de descargar los componentes, la volverá a enviar de forma automática al cabo de 15 minutos. El servidor seguirá enviando las notificaciones de actualización un máximo de cinco veces hasta que el agente responda. Si al quinto intento no obtiene respuesta, el servidor dejará de enviar notificaciones. Si selecciona la opción de actualizar componentes cuando los agentes se reinicien y conecten con el servidor, continuará la actualización de componentes.

Actualizaciones según programa

Ejecutar actualizaciones programadas es un derecho. Primero, seleccione los Agentes de OfficeScan que tendrán el derecho de ejecutar actualizaciones en función de un programa.

Nota

Para utilizar la actualización según programa con Traducción de direcciones de red, consulte *Configuración de las actualizaciones programadas del agente de OfficeScan con NAT en la página 6-45*.

Configuración de las actualizaciones automáticas del agente de OfficeScan

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Actualización automática**.
2. Seleccione los sucesos para una **actualización activada por suceso**:

- **Iniciar la actualización de los componentes en los agentes inmediatamente después de que el servidor de OfficeScan descargue un componente nuevo**
  - **Incluir agentes(s) independientes y sin conexión**
- **Permitir que los agentes inicien la actualización de los componentes después de reiniciarse y conectarse al servidor de OfficeScan (se excluyen los agentes independientes)**
- **Ejecutar la función Explorar ahora después de la actualización (excepto los agentes independientes)**

Para obtener más información sobre las distintas opciones disponibles, consulte *Actualizaciones activadas por suceso en la página 6-42*.

3. Configure el programa para una **actualización según programa**.

- **Minutos** u **Horas**

  La opción **Actualizar las configuraciones del agente solo una vez al día** está disponible al programar actualizaciones con una frecuencia basada en horas o minutos. El archivo de configuración contiene todos los ajustes del Agente de OfficeScan configurados mediante la consola Web.

  Consejo

  Trend Micro actualiza regularmente los componentes; no obstante, es probable que la configuración de OfficeScan se modifique con menor frecuencia. La actualización de los archivos de configuración con los componentes consume más ancho de banda y aumenta el tiempo que necesita OfficeScan para completar la actualización. Por este motivo, Trend Micro le recomienda que actualice las configuraciones de los agentes solo una vez al día.

- **Diaria** o **Semanal**

  Especifique la hora de la actualización y el período de tiempo en el que el servidor de OfficeScan informará a los agentes de que deben actualizar los componentes.

Consejo

Gracias a esta configuración, los agentes en línea no tendrán que conectarse simultáneamente al servidor a la hora de inicio especificada y se reduce, por tanto, la cantidad de tráfico dirigida al servidor. Por ejemplo, si la hora de inicio se define en 12 m. y el período de tiempo es de 2 horas, OfficeScan informa de manera aleatoria a los agentes conectados de que deben actualizar los componentes desde las 12 m. hasta las 2 p.m.

Nota

Una vez configurado el programa de la actualización, active el programa en los agentes seleccionados.

Para obtener más información sobre cómo activar las actualizaciones según programa, consulte el paso 4 de *Configurar los derechos y otras configuraciones de la actualización en la página 6-50*.

4. Haga clic en **Guardar**.

   OfficeScan no puede notificar a los agentes sin conexión de manera inmediata. Seleccione **Permitir que los agentes inicien la actualización de los componentes después de reiniciarse y conectarse al servidor de OfficeScan (se excluyen los agentes independientes)** para actualizar los agentes sin conexión que se conecten después de que se haya agotado el período de tiempo. Los agentes sin conexión que no tengan esta configuración activada actualizarán los componentes durante la próxima actualización programada o de forma manual.

Configuración de las actualizaciones programadas del agente de OfficeScan con NAT

Si la red local utiliza NAT, pueden surgir los siguientes problemas:

- Los Agentes de OfficeScan aparecen desconectados en la consola Web.
- El servidor de OfficeScan no puede informar correctamente a los agentes de las actualizaciones y los cambios de configuración.

Solucione estos problemas implementando los componentes y archivos de configuración actualizados del servidor en el Agente de OfficeScan mediante una actualización programada tal como se describe a continuación.

Procedimiento

- Antes de instalar el Agente de OfficeScan en los equipos del agente:

  a. Configure el programa de actualizaciones del agente en la sección **Actualización según programa** de **Actualizaciones** > **Agentes** > **Actualización automática**.

  b. Conceda a los agentes el derecho a activar una actualización programada en **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **pestaña Derechos** > **Actualizaciones de los componentes**.

- Si los Agentes de OfficeScan ya existen en los equipos del agente:

  a. Conceda a los agentes el derecho a ejecutar la función "Actualizar ahora" en **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **pestaña Derechos** > **Actualizaciones de los componentes**.

  b. Pida a los usuarios que actualicen manualmente los componentes del endpoint del agente (haciendo clic con el botón derecho del ratón en el icono del Agente de OfficeScan en la bandeja del sistema y haciendo clic en "Actualizar ahora") para obtener la configuración actualizada.

Cuando los Agentes de OfficeScan realicen una actualización, se actualizarán tanto los componentes como los archivos de configuración.

Uso de la herramienta de actualización programada de dominios

El programa de actualizaciones configurado en las actualizaciones automáticas de agente solo se aplica a agentes con derechos de actualización programada. En el caso de otros agentes, puede establecer un programa de actualización independiente. Para ello, tendrá que configurar un programa por dominios del árbol de agentes. Todos los agentes que pertenezcan a este dominio aplicarán el programa.

Nota

No se puede establecer un programa de actualización para un agente o subdominio específico. Todos los subdominios aplican el programa configurado para su dominio principal.

Procedimiento

1. Registre los nombres de dominio del árbol de agentes y actualice los programas.
2. Vaya a *carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\DomainScheduledUpdate`.
3. Copie los siguientes archivos en la `<Carpeta de instalación del servidor>\PCCSRV`:
   - `DomainSetting.ini`
   - `dsu_convert.exe`
4. Abra `DomainSetting.ini` con un editor de texto como el Bloc de notas.
5. Especifique un dominio del árbol de agentes y configure el programa de actualización para el dominio. Repita este paso para añadir más dominios.

   Nota

   En el archivo `.ini` se incluyen instrucciones de configuración detalladas.
6. Guarde `DomainSetting.ini`.
7. Abra una línea de comandos y cambie al directorio de la carpeta `PCCSRV`.
8. Escriba el siguiente comando y pulse `Intro`.

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. En la consola Web, vaya a **Agentes** > **Configuración global para los agentes**.
10. Haga clic en **Guardar**.

Actualizaciones manuales del agente

Actualice manualmente los componentes del Agente de OfficeScan cuando estén obsoletos y siempre que haya una epidemia. Los componentes del Agente de OfficeScan pasan a estar obsoletos cuando Agente de OfficeScan no puede actualizar los componentes desde el origen de actualización durante un período de tiempo prolongado.

Además de estos componentes, los Agentes de OfficeScan también reciben los archivos de configuración actualizados de manera automática durante la actualización manual. Los Agentes de OfficeScan necesitan los archivos de configuración para aplicar la nueva configuración. Cada vez que se modifica la configuración de OfficeScan desde la consola Web también se modifican los archivos de configuración.

Nota

Además de iniciar actualizaciones manuales, puede conceder a los usuarios derechos para ejecutar actualizaciones manuales (también denominado **Actualizar ahora** en los endpointsdel Agente de OfficeScan). Para conocer más detalles, consulte *Configurar los derechos y otras configuraciones de la actualización en la página 6-50*.

Actualización manual de agente de OfficeScan

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Actualización manual**.
2. En la parte superior de la pantalla aparecen los componentes que están disponibles actualmente en el servidor de OfficeScan y la fecha en la que se actualizaron por última vez. Asegúrese de que los componentes están actualizados antes de enviar las notificaciones a los agentes para que realicen la actualización.

   Nota

   Actualice manualmente los componentes obsoletos del servidor.

   Consulte *Actualizaciones manuales del agente en la página 6-48* para obtener más información.

3. Para actualizar solo agentes con componentes obsoletos:

   a. Haga clic en **Seleccionar agentes con componentes obsoletos**.

   b. (Opcional) Seleccione **Incluir agentes independientes y sin conexión**:

      - Para actualizar agentes independientes con conexión operativa al servidor.
      - Para actualizar los agentes sin conexión cuando se conectan.

   c. Haga clic en **Iniciar actualización**.

> **Nota**
>
> El servidor busca aquellos agentes cuyos componentes sean de versiones anteriores a las versiones que hay en el servidor y, a continuación, notifica a estos agentes que deben actualizarse. Para comprobar el estado de la notificación, vaya a la pantalla **Actualizaciones** > **Resumen**.

4. Para actualizar los agentes de su elección:

   a. Seleccione **Seleccionar agentes manualmente**.

   b. Haga clic en **Seleccionar**.

   c. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.

   d. Haga clic en **Iniciar actualización**.

> **Nota**
>
> El servidor empezará a notificar a cada agente que debe descargar los componentes actualizados. Para comprobar el estado de la notificación, vaya a la pantalla **Actualizaciones** > **Resumen**.

Configurar los derechos y otras configuraciones de la actualización

Defina la configuración de la actualización y conceda a los usuarios del agente determinados derechos, como realizar actualizaciones programadas y utilizar la opción "Actualizar ahora".

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y defina las siguientes opciones de la sección **Configuración de la actualización**:

OPCIÓN	DESCRIPCIÓN
Los agentes de OfficeScan descargan actualizaciones desde Trend Micro ActiveUpdate Server.	Cuando se inician las actualizaciones, los Agentes de OfficeScan obtienen primero las actualizaciones del origen de actualización especificado en la pantalla **Actualizaciones** > **Agentes** > **Origen de actualización**. Si la actualización no se ha realizado correctamente, los agentes intentarán actualizarse desde el servidor de OfficeScan. Si selecciona esta opción, los agentes pueden intentar actualizarse desde Trend Micro ActiveUpdate Server si no se ha realizado correctamente la actualización desde el servidor de OfficeScan. **Nota** Un agente que solo utilice IPv6 no puede actualizarse directamente desde Trend Micro ActiveUpdate Server. Se necesita un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que los agentes se conecten al servidor ActiveUpdate.
Activar las actualizaciones según	Si se selecciona esta opción, todos los Agentes de OfficeScan se configuran para activar las actualizaciones según programa de forma predeterminada. Los usuarios con el derecho **Activar/**

Opción	Descripción
programa en los agentes de OfficeScan	**desactivar las actualizaciones según programa** pueden sobrescribir esta configuración. Para obtener más información sobre cómo configurar el programa de actualización, consulte *Configuración de las actualizaciones automáticas del agente de OfficeScan en la página 6-43*.
Los agentes de OfficeScan pueden actualizar componentes pero no pueden actualizar el programa del agente ni implementar archivos Hotfix.	Esta opción permite que continúen las actualizaciones de los componentes, pero impide la implementación de archivos HotFix y la actualización del Agente de OfficeScan. **Nota** Desactivar esta opción puede afectar al rendimiento del servidor de forma considerable, ya que todos los agentes se conectarán a él al mismo tiempo para actualizar o instalar un archivo HotFix.

5. Haga clic en la pestaña **Derechos** y configure las siguientes opciones de la sección **Actualización de los componentes**:

Opción	Descripción
Ejecutar "Actualizar ahora"	Los usuarios con este derecho pueden actualizar componentes a petición. Para ello, tienen que hacer clic con el botón derecho en el icono del Agente de OfficeScan en la bandeja del sistema y seleccionar la opción **Actualizar ahora**. **Nota** Los usuarios del Agente de OfficeScan pueden utilizar la configuración del proxy durante la operación "Actualizar ahora". Consulte *Derechos de configuración del proxy para agentes en la página 15-57* para obtener más información.
Activar/ desactivar las	Seleccionar esta opción permite a los usuarios del Agente de OfficeScan activar y desactivar las actualizaciones programadas mediante el menú contextual del Agente de OfficeScan, lo que

Opción	Descripción
actualizaciones según programa	puede reemplazar la configuración **Activar las actualizaciones según programa**. **Nota** Para que el elemento aparezca en el menú del Agente de OfficeScan, los administradores deben seleccionar primero la configuración **Activar las actualizaciones según programa en los agentes de OfficeScan** de la pestaña **Otras configuraciones**.

6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración del espacio en disco reservado para las actualizaciones de los agentes de OfficeScan

OfficeScan puede asignar una determinada cantidad de espacio en disco en el agente para archivos HotFix, archivos de patrones, motores de exploración y actualizaciones de programas. OfficeScan reserva 60 MB de espacio en disco de manera predeterminada.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Sistema**.

3. Vaya a la sección **Actualizaciones**.
4. Seleccione **Reservar __ MB de espacio para las actualizaciones**.
5. Seleccione la cantidad de espacio en disco.
6. Haga clic en **Guardar**.

Proxy para las actualizaciones de componentes del agente de OfficeScan

Los Agentes de OfficeScan pueden utilizar la configuración del proxy durante las actualizaciones automáticas o si tienen el derecho correspondiente a la opción "Actualizar ahora".

TABLA 6-8. Configuración del proxy utilizada durante la actualización de componentes del agente de OfficeScan

MÉTODO DE ACTUALIZACIÓN	CONFIGURACIÓN DEL PROXY UTILIZADA	UTILIZACIÓN
Actualización automática	• Configuración automática del proxy. Para conocer más detalles, consulte *Configuración automática del proxy del agente de OfficeScan en la página 15-59*. • Configuración del proxy interno. Para conocer más detalles, consulte *Proxy interno para agentes de OfficeScan en la página 15-54*.	1. Para actualizar los componentes, los Agentes de OfficeScan primero utilizarán la configuración automática del proxy. 2. Si la configuración del proxy automática no está activada, se utilizará la configuración del proxy interno. 3. Si ambas están desactivadas, los agentes no utilizarán ninguna configuración del proxy.

MÉTODO DE ACTUALIZACIÓN	CONFIGURACIÓN DEL PROXY UTILIZADA	UTILIZACIÓN
Actualizar ahora	• Configuración automática del proxy. Para conocer más detalles, consulte *Configuración automática del proxy del agente de OfficeScan en la página 15-59*. • Configuración del proxy definida por el usuario. Puede conceder el derecho de definir la configuración del proxy a los usuarios de agente. Para conocer más detalles, consulte *Derechos de configuración del proxy para agentes en la página 15-57*.	1. Para actualizar los componentes, los Agentes de OfficeScan primero utilizarán la configuración automática del proxy. 2. Si la configuración del proxy automática no está activada, se utilizará la configuración del proxy definida por el usuario. 3. Si ambas están desactivadas, o bien si la configuración automática del proxy está desactivada y los usuarios de los agentes no tienen el derecho necesario, los agentes no utilizarán ningún proxy durante la actualización de componentes.

Configuración de las notificaciones de actualización del agente de OfficeScan

OfficeScan notifica a los usuarios de agente cuando se dan circunstancias relacionadas con sucesos.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Control de agentes**.
3. Vaya a la sección **Configuración de las alertas**.

4. Seleccione las siguientes opciones:

   - **Mostrar el icono de alerta en la barra de tareas de Windows si no se actualiza el archivo de patrón de virus al cabo de __ días**: Aparece un icono de alerta en la barra de tareas de Windows para recordar a los usuarios que actualicen un patrón de virus que no se ha actualizado en el número de días especificado. Para actualizar el patrón, utilice uno de los métodos de actualización tratados en *Métodos de actualización de los agentes de OfficeScan en la página 6-40*.

     Todos los agentes gestionados por el servidor aplicarán esta configuración.

   - **Mostrar un mensaje de notificación si el endpoint necesita reiniciarse para cargar un controlador en modo kernel**: tras instalar un archivo HotFix o un paquete de actualización que contenga una nueva versión de un controlador en modo kernel, es posible que la versión anterior del controlador siga instalada en el endpoint. El único modo de descargar la versión anterior y cargar la nueva es reiniciar el endpoint. Cuando se reinicie el endpoint, la nueva versión se instalará automáticamente y no habrá que reiniciar de nuevo.

     Se muestra el mensaje de notificación inmediatamente después de que un endpoint del agente instale el archivo HotFix o el paquete de actualización.

5. Haga clic en **Guardar**.

Visualizar los registros de actualización de agentes de OfficeScan

Compruebe los registros de actualización de agentes para determinar si existen problemas para actualizar el patrón de virus de los agentes.

Nota

En esta versión del producto, solo se pueden consultar desde la consola Web los registros de las actualizaciones de Patrón de virus.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para

obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Actualización de componentes del agente**.
2. Para ver el número de actualizaciones de agentes, haga clic en la opción **Mostrar** en la columna **Progreso**. En la pantalla **Progreso de la actualización de componentes** que aparece, se muestra tanto el número de agentes actualizados en intervalos de 15 minutos como el número total de agentes actualizados.
3. Para ver los agentes que han actualizado el patrón de virus, haga clic en la opción **Mostrar** en la columna **Detalles**.
4. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Aplicación de las actualizaciones de los agentes de OfficeScan

Utilice la conformidad con las normas de seguridad para garantizar que los agentes tienen los últimos componentes. La función de conformidad con las normas de seguridad determina las incoherencias de los componentes entre el servidor y los agentes de OfficeScan. Las incoherencias ocurren, por lo general, cuando los agentes no se pueden conectar al servidor para actualizar componentes. Si el agente obtiene una actualización proveniente de otro origen (como ActiveUpdate Server), es posible que un componente del agente sea más nuevo que el del servidor.

Para obtener más información, consulte *Conformidad con las normas de seguridad para agentes administrados en la página 15-63*.

Recuperar componentes de los agentes de OfficeScan

La recuperación significa volver a la versión anterior del patrón de virus, Smart Scan Agent Pattern y el motor de escaneo de virus. Si estos componentes no funcionan

correctamente, recupere las versiones anteriores. OfficeScan conserva la versión actual y las versiones anteriores del motor de exploración antivirus y las últimas cinco versiones del patrón de virus y Smart Scan Agent Pattern.

Nota

Sólo se pueden recuperar los componentes anteriormente mencionados.

OfficeScan utiliza distintos motores de exploración para los agentes que se ejecutan en plataformas de 32 bits y de 64 bits. Estos motores de exploración deben recuperarse por separado. El procedimiento de recuperación es idéntico para todos los tipos de motores de exploración.

Procedimiento

1. Vaya a **Actualizaciones** > **Recuperar**
2. Haga clic en **Sincronizar con el servidor** en la sección correspondiente.
   a. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
   b. Haga clic en **Recuperar**.
   c. Haga clic en **Ver registros de la actualización** para comprobar el resultado o en **Atrás** para volver a la pantalla Recuperar.
3. Si hay una versión anterior del archivo de patrones en el servidor, haga clic en **Recuperar versiones del servidor y el agente** para recuperar el archivo de patrones del servidor y el agente.

Ejecutar la herramienta Touch para archivos HotFix de los agentes de OfficeScan

La herramienta Touch sincroniza la marca de hora de un archivo con la de otro archivo, o bien con la hora del sistema del endpoint. Si intenta implementar sin éxito un archivo hotfix en el servidor de OfficeScan, utilice la herramienta Touch para cambiar la marca

de hora de dicho archivo. De esta forma, OfficeScan interpretará que el archivo hotfix es nuevo y hará que el servidor intente instalarlo de nuevo automáticamente.

Procedimiento

1. En el servidor de OfficeScan, vaya a la *carpeta de instalación del servidor*`>\PCCSRV\Admin\Utility\Touch`.

2. Copie `TMTouch.exe` en la carpeta que contiene el archivo que desea modificar. Si sincroniza la marca de hora del archivo con la de otro archivo, coloque ambos archivos en la misma ubicación con ayuda de la herramienta Touch.

3. Abra un símbolo del sistema y desplácese hasta la ubicación de la herramienta Touch.

4. Escriba lo siguiente:

   ```
   TmTouch.exe <nombre del archivo de destino> <nombre del archivo de origen>
   ```

   Donde:

   - `<nombre del archivo de destino>` es el nombre del archivo hotfix cuya marca de hora desea modificar
   - `<nombre del archivo de origen>` es el nombre del archivo cuya marca de hora desea replicar

   Nota

   Si no especifica ningún nombre de archivo de origen, la herramienta establecerá la marca de hora del archivo de destino según la hora del sistema del endpoint. Utilice el carácter de comodín (*) para el archivo de destino, pero no para el nombre del archivo de origen.

5. Para comprobar que se haya modificado la marca de hora, escriba `dir` en el símbolo del sistema o compruebe las propiedades del archivo en el Explorador de Windows.

Agentes de actualización

Para distribuir la tarea de implementación de componentes o configuraciones de dominio, o bien programas y archivos HotFix del agente en los Agentes de OfficeScan, asigne algunos Agentes de OfficeScan para que actúen como agentes de actualización u orígenes de actualización de otros agentes. De esta forma se garantiza que los agentes reciben actualizaciones cuando corresponde, sin dirigir una cantidad considerable de tráfico de red al servidor de OfficeScan.

Si la red está dividida por ubicación y el enlace de red entre estas divisiones está sometido a una gran carga de tráfico, asigne al menos un agente de actualización para cada ubicación.

Nota

Los Agentes de OfficeScan que se asignan para actualizar componentes desde un agente de actualización solo reciben componentes y configuraciones actualizados del agente de actualización. Aun así, todos los Agentes de OfficeScan informan al servidor de OfficeScan sobre su estado.

Requisitos del sistema del agente de actualización

Visite el siguiente sitio Web para obtener una lista completa de los requisitos del sistema:

http://docs.trendmicro.com/es-es/enterprise/officescan.aspx

Configuración del agente de actualización

El proceso de configuración del agente de actualización consta de dos pasos:

1. Asigne el Agente de OfficeScan como un agente de actualización para determinados componentes.

2. Especifique los agentes que se actualizarán desde este agente de actualización.

Nota

El número de conexiones de agente simultáneas que puede gestionar un solo agente de actualización depende de las especificaciones de hardware del endpoint.

Asignación de agentes de OfficeScan como agentes de actualización

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, seleccione los agentes que se designarán como agentes de actualización.

Nota

No es posible seleccionar el icono del dominio raíz, ya que esto convertiría todos los agentes en agentes de actualización. Un agente de actualización que solo utiliza IPv6 no puede distribuir las actualizaciones directamente a agentes que solo utilizan IPv4. De modo similar, un agente de actualización que solo utiliza IPv4 no puede distribuir las actualizaciones directamente a agentes que solo utilizan IPv6. Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que el agente de actualización distribuya las actualizaciones a los agentes.

3. Haga clic en **Configuración** > **Configuración del agente de actualización**.
4. Seleccione los elementos que pueden compartir los agentes de actualización.
   - Actualizaciones de los componentes
   - Configuración del dominio
   - Programas y archivos Hotfix del agente de OfficeScan
5. Haga clic en **Guardar**.

Especificación de los agentes de OfficeScan que se actualizan desde un agente de actualización

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Origen de actualización**.
2. En **Fuente de actualización personalizada**, haga clic en **Agregar**.
3. En la pantalla que aparece, especifique las direcciones IP de los agentes. Puede escribir un intervalo de direcciones IPv4, y un prefijo y una longitud de IPv6.
4. En el campo **Agente de actualización**, seleccione el agente de actualización que desea asignar a los agentes.

   Nota

   Asegúrese de que los agentes se pueden conectar al agente de actualización mediante sus direcciones IP. Por ejemplo, si ha especificado un intervalo de direcciones IPv4, el agente de actualización debe tener una dirección IPv4. Si ha especificado un prefijo y una longitud de IPv6, el agente de actualización debe tener una dirección IPv6.

5. Haga clic en **Guardar**.

Fuentes de actualización para los agentes de actualización

Los agentes de actualización pueden obtener las actualizaciones de varias fuentes, como el servidor de OfficeScan o una fuente de actualización personalizada. Configure la fuente de actualización en la pantalla Fuente de actualización de la consola Web.

Compatibilidad con IPv6 de los agentes de actualización

Un agente de actualización que solo utilice IPv6 no puede actualizarse directamente desde fuentes de actualización que utilicen únicamente IPv4, como:

- Un servidor de OfficeScan que solo utilice IPv4

- Una fuente de actualización personalizada que solo utilice IPv4.
- Trend Micro ActiveUpdate server

Del mismo modo, un agente de actualización que solo utilice IPv4 no puede actualizarse directamente desde fuentes de actualización que utilicen únicamente IPv6, como un servidor de OfficeScan de solo IPv6.

Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir al agente de actualización que se conecte a las fuentes de actualización.

Fuente de actualización estándar para los agentes de actualización

El servidor de OfficeScan es la fuente de actualización estándar para los agentes de actualización. Si configura los agentes para actualizarse directamente desde el servidor de OfficeScan, el proceso de actualización se realiza de la forma siguiente:

1. El agente de actualización obtiene las actualizaciones del servidor de OfficeScan.
2. Si no se puede actualizar desde el servidor de OfficeScan, el agente intenta conectarse directamente con Trend Micro ActiveUpdate Server en el caso de darse cualquiera de estas circunstancias:
   - En **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones** > **Configuración de actualización**, la opción **Los agentes de OfficeScan descargan actualizaciones desde Trend Micro ActiveUpdate Server** está activada.
   - El servidor ActiveUpdate Server es la primera entrada en la lista de fuentes de actualización personalizadas.

Consejo

Coloque el servidor ActiveUpdate al principio de la lista sólo si tiene problemas a la hora de llevar a cabo las actualizaciones desde el servidor de OfficeScan. Cuando los agentes de actualización se actualizan directamente desde el servidor ActiveUpdate, se utiliza un ancho de banda considerable entre la red e Internet.

3. Si no se puede realizar la actualización desde ninguna de las fuentes posibles, el agente de actualización abandona el proceso de actualización.

Fuentes de actualización personalizadas para los agentes de actualización

Además del servidor de OfficeScan, los agentes de actualización cuentan con fuentes de actualización personalizadas para actualizarse. Los orígenes de actualización personalizados reducen el tráfico de actualización del agente que se envía al servidor de OfficeScan. Especifique las fuentes de actualización personalizadas en la Lista de fuentes de actualización personalizadas, en la que se pueden incluir un máximo de 1.024 fuentes de actualización. Consulte *Orígenes de actualización personalizadas para los agentes de OfficeScan en la página 6-35* para ver los pasos que hay que realizar para configurar la lista.

Nota

Para que los agentes de actualización se conecten a los orígenes de actualización personalizados, asegúrese de que la opción **Los agentes de actualización actualizan los componentes, la configuración del dominio, los programas del agente y los archivos Hotfix solo desde el servidor de OfficeScan** está desactivada en la pantalla **Origen de actualización de agentes** (**Actualizaciones** > **Agentes** > **Origen de actualización**).

Una vez que ha establecido y guardado la lista, el proceso de actualización se realiza de la siguiente manera:

1. El agente de actualización se actualiza a partir de la primera entrada de la lista.

2. Si no se puede realizar la actualización desde la primera entrada de la lista, el agente de actualización pasa a la segunda y así sucesivamente.

3. Si no se puede realizar la actualización a partir de ninguna de las entradas, el agente prueba las siguientes opciones del encabezado **Los agentes de OfficeScan actualizan los siguientes elementos desde el servidor de OfficeScan si los orígenes personalizados no se encuentran o no están disponibles**:

    - **Componentes**: si está activada esta opción, el agente de actualización se actualiza desde el servidor de OfficeScan.

Si la opción no está activada, el agente trata de conectarse directamente a Trend Micro ActiveUpdate Server en el caso de darse cualquiera de estas circunstancias:

Nota

Sólo se pueden actualizar los componentes desde el servidor ActiveUpdate. La configuración de dominios, los programas y los archivos hotfix sólo se pueden descargar del servidor o los agentes de actualización.

- En **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones** > **Configuración de actualización**, la opción **Los agentes descargan actualizaciones desde Trend Micro ActiveUpdate Server** está activada.
- El servidor ActiveUpdate Server no está incluido en la lista de fuentes de actualización personalizadas.

- **Configuración del dominio**: si está activada esta opción, el agente de actualización se actualiza desde el servidor de OfficeScan.
- **Programas y archivos HotFix del agente de OfficeScan**: si está activada esta opción, el agente de actualización se actualiza desde el servidor de OfficeScan.

4. Si no se puede realizar la actualización desde ninguna de las fuentes posibles, el agente de actualización abandona el proceso de actualización.

El proceso de actualización es diferente si la opción **Origen de actualización estándar (actualizar desde el servidor de OfficeScan)** está activada y el servidor de OfficeScan solicita al agente que actualice los componentes. El proceso es el siguiente:

1. El agente se actualiza directamente a partir del servidor de OfficeScan e ignora la lista de fuentes de actualización.
2. Si no se puede actualizar desde el servidor, el agente intenta conectarse directamente con Trend Micro ActiveUpdate Server en el caso de darse cualquiera de estas circunstancias:

- En **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones** > **Configuración de actualización**, la opción **Los agentes de OfficeScan descargan actualizaciones desde Trend Micro ActiveUpdate Server** está activada.
- El servidor ActiveUpdate Server es la primera entrada en la lista de fuentes de actualización personalizadas.

Consejo

Coloque el servidor ActiveUpdate al principio de la lista sólo si tiene problemas a la hora de llevar a cabo las actualizaciones desde el servidor de OfficeScan. Cuando los Agentes de OfficeScan se actualizan directamente desde el ActiveUpdate Server, se utiliza un ancho de banda considerable entre la red e Internet.

3. Si no se puede realizar la actualización desde ninguna de las fuentes posibles, el agente de actualización abandona el proceso de actualización.

Configuración de la fuente de actualización para el agente de actualización

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Origen de actualización**.
2. Seleccione si desea que la actualización se realice a partir de la fuente de actualización estándar para los agentes de actualización (servidor de OfficeScan) o la fuente de actualización personalizada para los agentes de actualización.
3. Haga clic en **Notificar a todos los agentes**.

Duplicación de los componentes del agente de actualización

Al igual que el servidor de OfficeScan, los agentes de actualización también utilizan la duplicación de componentes durante la actualización de componentes. Consulte

Duplicación de componentes del servidor de OfficeScan en la página 6-22 para obtener información sobre cómo realiza el servidor la duplicación de componentes.

El proceso de duplicación de componentes para los agentes de actualización es el siguiente:

1. El agente de actualización compara su versión actual de patrones completos con la última versión en la fuente de actualización. Si la diferencia entre ambas versiones es 14 o menos, el agente de actualización descarga el patrón incremental que representa la diferencia entre ambas versiones.

   Nota

   Si la diferencia es mayor que 14, el agente de actualización descarga automáticamente la versión completa del archivo de patrones.

2. El agente de actualización combina el patrón incremental descargado con su patrón completo actual para generar el último patrón completo.
3. El agente de actualización descarga todos los demás patrones incrementales en la fuente de actualización.
4. El patrón completo más reciente y todos los patrones incrementales están a disposición de los agentes.

Métodos de actualización para los agentes de actualización

Los agentes de actualización utilizan los mismos métodos disponibles para los agentes normales. Para conocer más detalles, consulte *Métodos de actualización de los agentes de OfficeScan en la página 6-40*.

También puede utilizar la herramienta de configuración de actualizaciones programadas para activar y configurar las actualizaciones programadas en un agente de actualización que se haya instalado mediante Agent Packager.

Nota

Esta herramienta no está disponible si el agente de actualización se ha instalado utilizando otros métodos de instalación. Consulte el apartado *Consideraciones sobre la implementación en la página 5-13* para obtener más información.

Uso de la herramienta de configuración de actualizaciones programadas

Procedimiento

1. En el endpoint del agente de actualización, vaya a la <*Carpeta de instalación del agente*>.
2. Haga doble clic en `SUCTool.exe` para ejecutar la herramienta. Se abrirá la consola de la herramienta de configuración de actualizaciones programadas.
3. Seleccione **Activar la actualización programada**.
4. Especifique la frecuencia y la hora de la actualización.
5. Haga clic en **Aplicar**.

Informe analítico del agente de actualización

Genere el informe analítico del agente de actualización para analizar la infraestructura de actualización y determinar los agentes que descargan actualizaciones parciales de los agentes de actualización y de otros orígenes de actualización.

Nota

El informe incluye todos los Agentes de OfficeScan que se han configurado para recibir actualizaciones parciales de un agente de actualización. Si ha delegado la tarea de administrar uno o varios dominios en otros administradores, estos también verán los Agentes de OfficeScan que se han configurado para recibir actualizaciones parciales de los agentes de actualización que pertenecen a los dominios que no administran.

OfficeScan exporta el Informe analítico del agente de actualización a un archivo de valores separados por comas (`.csv`).

Este informe contiene la siguiente información:

- Agente de OfficeScan endpoint
- Dirección IP
- Ruta del árbol de agentes
- Fuente de actualización
- Si los agentes descargan los siguientes elementos de los agentes de actualización:
    - Componentes
    - Configuración del dominio
    - Programas y archivos HotFix del Agente de OfficeScan

Importante

El informe analítico del agente de actualización solo muestra los Agentes de OfficeScan que se han configurado para recibir actualizaciones parciales de un agente de actualización. Los Agentes de OfficeScan que se han configurado para realizar actualizaciones completas desde un agente de actualización (incluidos componentes, configuración de dominios, programas del Agente de OfficeScan y archivos HotFix) no aparecen en el informe.

Para obtener información detallada acerca de cómo generar el informe, consulte *Orígenes de actualización personalizadas para los agentes de OfficeScan en la página 6-35*.

Resumen de la actualización de componentes

La consola Web tiene una pantalla, **Actualizar resumen** (vaya a **Actualizaciones** > **Resumen**), que le informa del estado de actualización de componentes general y le permite actualizar los componentes obsoletos. Si habilita al servidor para que realice actualizaciones programadas, en la pantalla también aparecerá el programa de la próxima actualización.

Actualice la pantalla periódicamente para ver el último estado de actualización de los componentes.

Nota

Para ver las actualizaciones de los componentes del servidor Smart Protection Server integrado, vaya a **Administración** > **Smart Protection** > **Servidor integrado**.

Estado de la actualización de los agentes de OfficeScan

Si ha iniciado una actualización de componentes en los agentes, consulte la siguiente información de esta sección:

- Número de agentes notificados para actualizar componentes.
- Número de agentes que ya estén en la cola de notificaciones, pero que todavía no las han recibido. Para cancelar la notificación de estos agentes, haga clic en **Cancelar la notificación**.

Componentes

En la tabla **Actualizar estado**, consulte el estado de las actualizaciones de cada uno de los componentes que el servidor de OfficeScan descarga y distribuye.

Consulte la versión actual y la fecha de la última actualización de cada componente. Haga clic en el enlace numerado para ver los agentes que tienen componentes obsoletos. Actualice manualmente los agentes que tengan componentes obsoletos.

Capítulo 7

Buscando riesgos de seguridad

En este capítulo se describe cómo proteger los endpoints frente a riesgos de seguridad mediante la exploración basada en archivos.

Los temas que se incluyen son:

- *Acerca de los riesgos de seguridad en la página 7-2*
- *Tipos de métodos de exploración en la página 7-9*
- *Tipos de exploración en la página 7-15*
- *Configuración común para todos los tipos de exploración en la página 7-28*
- *Derechos y otras configuraciones de la exploración en la página 7-59*
- *Configuración general de la exploración en la página 7-75*
- *Notificaciones de riesgos de seguridad en la página 7-87*
- *Registros de riesgos de seguridad en la página 7-98*
- *Epidemias de riesgos de seguridad en la página 7-114*

Acerca de los riesgos de seguridad

Riesgo de seguridad es el término que se usa para denominar a virus/malware, así como a spyware/grayware. OfficeScan protege los endpoints de riesgos de seguridad mediante la exploración de archivos y la ejecución de una acción específica por cada riesgo de seguridad detectado. La detección de un gran número de riesgos de seguridad en un corto período de tiempo es señal de epidemia. OfficeScan puede ayudar a contener las epidemias aplicando políticas de prevención de epidemias y aislando los endpoints infectados hasta que se encuentran completamente fuera de peligro. Las notificaciones y los registros le ayudan a realizar un seguimiento de los riesgos de seguridad y le alertan en caso de que sea necesario llevar a cabo una acción inmediata.

Virus y malware

Existen decenas de miles de virus/malware, una cifra que va en aumento cada día. Aunque eran más comunes en DOS o Windows, los virus de endpoint actuales pueden dañar seriamente los sistemas mediante el aprovechamiento de las vulnerabilidades de las redes corporativas, sistemas de correo electrónico y sitios Web.

TABLA 7-1. Tipos de virus/malware

TIPO DE VIRUS/ MALWARE	DESCRIPCIÓN
Programa de broma	Los programas de broma son programas similares a virus que suelen manipular el aspecto de los elementos de la pantalla de un endpoint.
Otros	«Otros» incluye virus/malware no clasificados bajo ninguno de los tipos de virus/malware.
Packer	Los packers son programas ejecutables comprimidos y/o cifrados de Windows o Linux™, y a menudo se trata de caballos de Troya. Los archivos ejecutables comprimidos hacen que los packers sean más difíciles de detectar para los productos antivirus.

Tipo de virus/ malware	Descripción
Rootkit	Los rootkits son programas (o conjuntos de programas) que instalan y ejecutan código en un sistema sin el consentimiento o conocimiento del usuario final. Usan técnicas de ocultación para mantener una presencia continua e indetectable en el equipo. Los rootkits no infectan los equipos, sino que buscan proporcionar un entorno indetectable para que el código maligno se ejecute. Se instalan en los sistemas a través de la ingeniería social, al ejecutarse el malware o simplemente al navegar por un sitio Web malicioso. Una vez que se instalan, el atacante puede llevar a cabo prácticamente cualquier función en el sistema, entre ellas el acceso remoto, la interceptación, así como la ocultación de procesos, archivos, claves de registro y canales de comunicación.
Virus de prueba	Los virus de prueba son archivos de texto inerte que actúan como un virus real y que se pueden detectar con un software de exploración antivirus. Utilice los virus de prueba, como la secuencia de comandos de prueba EICAR, para comprobar que la instalación antivirus funciona correctamente.
Caballo de Troya	Un caballo de Troya suele usar los puertos para obtener acceso a los equipos o los equipos ejecutables. Los troyanos no se replican sino que residen en los sistemas para realizar acciones maliciosas como abrir puertos para que accedan hackers. Las soluciones antivirus tradicionales pueden detectar y eliminar virus pero no troyanos, en especial los que ya se están ejecutando en el sistema.

Tipo de virus/ malware	Descripción
Virus	Los virus son programas que se replican. Para ello, el virus tiene que adjuntarse a otros archivos de programa y ejecutarse siempre que se ejecute el programa host, incluyendo: • **Código malicioso de ActiveX**: código que reside en páginas Web que ejecutan controles ActiveX™. • **Virus de sector de arranque**: virus que infecta el sector de arranque de una partición o un disco. • **Infector de archivos COM y EXE**: Programa ejecutable con una extensión `.com` o `.exe`. • **Código malicioso de Java**: código vírico independiente del sistema operativo escrito o incrustado en Java™. • **Virus de macro**: virus codificado como una macro de aplicación que suele incluirse en un documento. • Virus **VBScript**, **JavaScript** o **HTML**: virus que reside en páginas Web y que se descarga a través de un explorador. • **Gusano**: Programa completo o conjunto de programas que propaga copias funcionales de sí mismo o de sus segmentos a otros sistemas del endpoint, generalmente por correo electrónico.
Virus de red	Un virus que se propaga por una red no es, en sentido estricto, un virus de red. Sólo algunos tipos de virus o malware, como los gusanos, pueden calificarse como virus de red. Concretamente, los virus de red utilizan los protocolos de red como TCP, FTP, UDP y HTTP y los protocolos de correo electrónico para replicarse. Generalmente no alteran los archivos del sistema ni modifican los sectores de arranque de los discos duros. En vez de ello, los virus de red infectan la memoria de los agente endpoints y los obligan a desbordar la red con tráfico, lo que puede originar una ralentización del sistema e incluso el colapso completo de la red. Puesto que los virus de red residen en la memoria, los métodos de exploración basados en E/S no suelen detectarlos.

TIPO DE VIRUS/ MALWARE	DESCRIPCIÓN
Virus/Malware probable	Los virus/malware probables son archivos sospechosos que tienen algunas características de virus/malware. Para obtener información detallada, consulte la Enciclopedia de virus de Trend Micro: http://about-threats.trendmicro.com/es/threatencyclopedia#malware **Nota** No se puede limpiar cuando se trata de un posible virus o malware, pero sí se puede configurar la acción de exploración.

Spyware y grayware

Además de los virus/malware, los Endpoints están expuestos a otras posibles amenazas. Spyware/grayware es el término con el que se hace referencia a las aplicaciones o los archivos no clasificados como virus o troyanos, pero que, igualmente, pueden afectar negativamente al rendimiento de los endpoints de la red y generar importantes riesgos legales, de seguridad y confidencialidad para la organización. Es frecuente que el spyware/grayware lleve a cabo una serie de acciones no deseadas y de carácter amenazante como, por ejemplo, molestar a los usuarios con ventanas emergentes, registrar las pulsaciones de teclas de los usuarios o exponer las vulnerabilidades de endpoint a posibles ataques.

Si detecta alguna aplicación o archivo que OfficeScan no pueda detectar como grayware pero que sea sospechoso de serlo, envíelo a Trend Micro para su análisis:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

TIPO	DESCRIPCIÓN
Spyware	recopila datos, como nombres de usuarios y contraseñas de cuentas, y los envía a otras personas.

Tipo	Descripción
Adware	muestra publicidad y recopila datos, como las preferencias de navegación por Internet de un usuario, para enviar anuncios al usuario mediante el explorador Web.
Marcador telefónico	modifica la configuración de Internet del endpoint para forzar al endpoint a que marque números de teléfono preconfigurados a través de un módem. Suelen ser números de servicios de pago por llamada o números internacionales que pueden ocasionar gastos importantes a la organización.
Programa de broma	provoca comportamientos anómalos en el endpoint, como el cierre y la apertura de la bandeja de la unidad de CD-ROM o la visualización de numerosos cuadros de mensaje.
Herramienta de hackers	ayuda a los hackers a introducirse en los equipos.
Herramienta de acceso remoto	ayuda a los hackers a acceder y controlar de forma remota otros equipos.
Aplicación de robo de contraseñas	permite a los hackers descifrar nombres de usuario y contraseñas de cuentas.
Otros	otros tipos de programas potencialmente dañinos.

Cómo el spyware/grayware se introduce en la red

A menudo, el spyware/grayware se introduce en una red corporativa cuando los usuarios descargan software legítimo que incluye aplicaciones de grayware en el paquete de instalación. La mayoría de los programas de software incluyen un acuerdo de licencia para el usuario final que se debe aceptar antes de iniciar la descarga. Este acuerdo incluye información sobre la aplicación y su uso previsto para recopilar datos personales; sin embargo, los usuarios no suelen percatarse de esta información o no comprenden la jerga legal.

Riesgos y amenazas potenciales

La existencia de spyware y otros tipos de grayware en la red puede propiciar los problemas siguientes:

TABLA 7-2. Riesgos y amenazas potenciales

RIESGO O AMENAZA	DESCRIPCIÓN
Reducción del rendimiento de los endpoints	Para realizar sus tareas, las aplicaciones de spyware o grayware a menudo requieren numerosos recursos de la CPU y la memoria del sistema.
Aumento de los bloqueos del explorador de Internet	Algunos tipos de grayware, como el adware, suelen mostrar información en un cuadro o ventana del explorador. En función de la interacción del código de estas aplicaciones con los procesos del sistema, el grayware puede ocasionar que los exploradores se bloqueen y que incluso sea necesario reiniciar el endpoint.
Disminución de la eficacia del usuario	Al tener que cerrar frecuentemente anuncios emergentes y soportar los efectos negativos de los programas de broma, los usuarios se distraerán innecesariamente de sus tareas principales.
Degradación del ancho de banda de la red	Las aplicaciones de spyware o grayware transmiten regularmente los datos recopilados a otras aplicaciones que se ejecutan en la red o en otras ubicaciones externas.
Pérdida de información personal y corporativa	La información que recopilan las aplicaciones de spyware o grayware no se limita a la lista de sitios Web que visitan los usuarios. El spyware/grayware también puede recopilar las credenciales del usuario como, por ejemplo, las utilizadas para acceder a las cuentas de la banca en línea y a las redes corporativas.
Mayor riesgo de responsabilidad legal	Si los hackers secuestran los recursos de los endpoints de la red, pueden utilizar los equipos del agente para iniciar ataques o instalar spyware/grayware en otros equipos externos de la red. La participación de los recursos de la red en estas actividades puede responsabilizar legalmente a una empresa de los perjuicios ocasionados por otras personas.

Protección frente a spyware/grayware y otras amenazas

Hay muchas medidas que puede tomar para impedir la instalación de spyware/grayware en su endpoint. Trend Micro sugiere lo siguiente:

- Configurar todos los tipos de exploración (Exploración manual, Exploración en tiempo real, Exploración programada y Explorar ahora) para buscar y eliminar archivos y aplicaciones de spyware/grayware. Consulte el apartado *Tipos de exploración en la página 7-15* para obtener más información.
- Enseñar a los usuarios de agente para que siempre hagan lo siguiente:
  - Leer el contrato de licencia de usuario final (CLUF) y la documentación incluida con las aplicaciones que descarguen e instalen en los equipos.
  - Hacer clic en **No** en los mensajes que soliciten autorización para descargar e instalar software salvo que los usuarios de agente estén seguros de que el creador del mismo y el sitio Web que visitan sean de confianza.
  - Hacer caso omiso del correo electrónico comercial no solicitado (spam), sobre todo si en él se solicita a los usuarios que hagan clic en un botón o hiperenlace.
- Configurar el explorador Web con un nivel estricto de seguridad. Trend Micro recomienda exigir a los exploradores Web que avisen a los usuarios antes de instalar controles ActiveX.
- Si se utiliza Microsoft Outlook, definir la configuración de seguridad para que Outlook no descargue automáticamente los elementos HTML tales como las imágenes enviadas a través de mensajes spam.
- No permitir el uso de servicios para compartir archivos de igual a igual. El spyware y otras aplicaciones de grayware pueden enmascararse como otros tipos de archivo que los usuarios suelen querer descargar como archivos de música MP3.
- Revisar periódicamente el software instalado en los equipos de agente en busca de aplicaciones que puedan ser spyware u otras formas de grayware.
- Mantener actualizados los sistemas operativos Windows con las últimas revisiones de seguridad de Microsoft. Consulte el sitio Web de Microsoft para obtener más información.

Tipos de métodos de exploración

Los Agentes de OfficeScan pueden utilizar uno de los dos métodos de exploración cuando realizan una exploración en busca de riesgos de seguridad. Los métodos de exploración son smart scan y la exploración convencional.

- **Smart Scan**

  En este documento, los agentes que utilizan Smart Scan se denominan **agentes Smart Scan**. Los agentes Smart Scan se benefician de las exploraciones locales y de las consultas por Internet proporcionadas por los servicios de File Reputation.

- **Exploración convencional**

  Los agentes que no utilizan Smart Scan se denominan **agentes exploración convencional**. Un agente de exploración convencional almacena todos los componentes de OfficeScan en el endpoint de agente y explora todos los archivos de manera local.

Método de exploración predeterminado

En esta versión de OfficeScan, el método de exploración predeterminado para las nuevas instalaciones es smart scan. Esto significa que si realiza una instalación nueva del servidor de OfficeScan y no ha cambiado el método de exploración en la consola Web, todos los agentes que gestiona el servidor utilizarán Smart Scan.

Si actualiza el servidor de OfficeScan desde una versión anterior y se activa una actualización automática de agentes, todos los agentes que el servidor administre utilizarán el método de exploración que estaba configurado antes de la actualización. Por ejemplo, si actualiza a partir de OfficeScan 11.0, que es compatible tanto con Smart Scan como con la exploración convencional, todos los agentes actualizados que utilicen Smart Scan continuarán utilizándolo, mientras que todos los agentes que utilicen la exploración convencional seguirán utilizando este tipo de exploración.

Comparación de métodos de exploración

La siguiente tabla ofrece una comparación entre los dos métodos de exploración:

TABLA 7-3. Comparación entre la exploración convencional y smart scan

REFERENCIAS DE LA COMPARACIÓN	EXPLORACIÓN CONVENCIONAL	SMART SCAN
Disponibilidad	Disponible en esta versión de OfficeScan, así como en todas las anteriores	Inicio en OfficeScan 10 disponible
Comportamiento de la exploración	El agente de exploración convencional explora en el endpoint local.	• El agente Smart Scan explora en el endpoint local. • Si el agente no puede determinar el riesgo del archivo durante la exploración, el agente envía una consulta de exploración a un origen de Smart Protection para comprobar el riesgo. • El agente "almacena en caché" el resultado de la consulta para mejorar el rendimiento de la exploración.
Componentes en uso y actualizados	Todos los componentes disponibles en la fuente de actualización, excepto el Smart Scan Agent Pattern	Todos los componentes disponibles en la fuente de actualización, excepto el Virus Pattern y Spyware Active-monitoring Pattern
Fuente de actualización tradicional	Servidor de OfficeScan	Servidor de OfficeScan

Cambio del método de exploración

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.

3. Haga clic en **Configuración** > **Configuración de la exploración** > **Métodos de exploración**.

4. Seleccione **Exploración convencional** o **Smart scan**.

5. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Cambiar de la exploración convencional a Smart Scan

Al cambiar los agentes a la exploración convencional, tenga en cuenta lo siguiente:

1. Número de agentes para cambiar

   Si se cambia un número relativamente reducido de agentes al mismo tiempo, se permite un uso más eficaz del servidor de OfficeScan y de los recursos del servidor de Smart Protection Server. Estos servidores puede llevar a cabo otras tareas críticas mientras los agentes cambian los métodos de exploración.

2. Tiempo

   Al volver a la exploración convencional, los agentes probablemente descargarán la versión completa del patrón de virus y del patrón de supervisión antispyware activa desde el servidor de OfficeScan. Estos archivos de patrón solo los utilizan los agentes de la exploración convencional.

   Considere la opción de realizar el cambio durante las horas de menor actividad para garantizar que el proceso de descarga se realiza en un corto período de tiempo. Considere cambiar si ningún agente tiene una actualización desde el servidor

programada. Además, desactive de forma temporal la opción "Actualizar ahora" de los agentes y vuelva a activarla una vez los agentes hayan cambiado a Smart Scan.

3. Configuración del árbol de agentes

   El método de exploración es una configuración granular que se puede establecer a nivel de raíz, dominio o agente. Al cambiar a la exploración convencional, puede:

   - Cree un nuevo dominio del árbol de agentes y asigne exploración convencional como su método de exploración. Cualquier agente que mueva a este dominio utilizará la exploración convencional. Cuando mueva el agente, active el parámetro **Aplicar la configuración del nuevo dominio a los agentes seleccionados**.
   - Seleccionar un dominio y configurarlo para que utilice la exploración convencional. Los agentes Smart Scan que pertenezcan al dominio cambiarán a la exploración convencional.
   - Seleccione uno o varios agentes Smart Scan de un dominio y cámbielos a la exploración convencional.

Nota

Los cambios que se realicen en el método de exploración del dominio sobrescribirán el método de exploración configurado para los agentes.

Cambiar de la exploración convencional a Smart Scan

Si va a cambiar agentes de la exploración convencional a Smart Scan, asegúrese de haber configurado Smart Protection Services.

Para conocer más detalles, consulte *Configuración de los Servicios de Smart Protection en la página 4-13*.

La siguiente tabla proporciona otras consideraciones para el cambio a Smart Scan.

TABLA 7-4. Consideraciones a la hora de cambiar a smart scan

CONSIDERACIÓN	DETALLES
Licencia del producto	Para utilizar smart scan, asegúrese de que están activadas las licencias de los siguientes servicios y que no están caducadas: • Antivirus • Reputación Web y antispyware
Servidor de OfficeScan	Asegúrese de que los agentes se pueden conectar al servidor de OfficeScan. Solo a los agentes en línea se les notificará el cambio a Smart Scan. Los que estén sin conexión recibirán la notificación en el momento en el que se conecten. A los agentes independientes se les notificará cuando estén en línea o, en caso de que cuenten con derechos de actualización programada, cuando se ejecute dicha actualización. Compruebe también que el servidor de OfficeScan cuenta con los componentes más actualizados, ya que los agentes Smart Scan tienen que descargar Smart Scan Agent Pattern del servidor. Para actualizar los componentes consulte *Actualizaciones del servidor de OfficeScan en la página 6-16*.
Número de agentes para cambiar	Si se cambia un número de agentes relativamente bajo al mismo tiempo, los recursos del servidor de OfficeScan se utilizan de una forma más eficaz. El servidor de OfficeScan puede llevar a cabo otras tareas esenciales mientras los agentes cambian los métodos de exploración.

Consideración	Detalles
Tiempo	Al cambiar a Smart Scan por primera vez, los agentes tienen que descargar la versión completa de Smart Scan Agent Pattern del servidor de OfficeScan. El Smart Scan Pattern solo lo utilizan los agentes Smart Scan. Considere la opción de realizar el cambio durante las horas de menor actividad para garantizar que el proceso de descarga se realiza en un corto período de tiempo. Hágalo también cuando ningún agente tenga programada una actualización desde el servidor. Además, desactive de forma temporal la opción "Actualizar ahora" de los agentes y vuelva a activarla una vez estos hayan cambiado a Smart Scan.
Configuración del árbol de agentes	El método de exploración es una configuración granular que se puede establecer en la raíz, en el dominio o en el agente. Al cambiar a smart scan, puede: • Crear un nuevo dominio del árbol de agentes y asignar Smart Scan como su método de exploración. Ningún agente que mueva a este dominio utilizará Smart Scan. Cuando mueva el agente, active el parámetro **Aplicar la configuración del nuevo dominio a los agentes seleccionados**. • Seleccionar un dominio y configurarlo para que utilice smart scan. Los agentes de la exploración convencional que pertenezcan al dominio cambiarán a Smart Scan. • Seleccionar uno o varios agentes de exploración convencional de un dominio y cambiarlos a Smart Scan. **Nota** Los cambios que se realicen en el método de exploración del dominio sobrescribirán el método de exploración configurado para cada agente.

CONSIDERACIÓN	DETALLES
Compatibilidad con IPv6	Los agentes Smart Scan envían consultas sobre la exploración a las fuentes de Smart Protection. Un agente Smart Scan que solo utilice IPv6 no puede enviar consultas directamente a fuentes que utilicen únicamente IPv4, como: • Smart Protection Server 2.0 (integrado o independiente) **Nota** La versión 2.5 del Smart Protection Server es la primera compatible con IPv6. • Red de Smart Protection de Trend Micro Del mismo modo, un agente Smart Scan que solo utilice IPv4 no puede enviar consultas a los servidores de Smart Protection Server que utilicen únicamente IPv6. Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir que los agentes Smart Scan se conecten a las fuentes.

Tipos de exploración

OfficeScan ofrece los siguientes tipos de exploración para proteger los equipos del Agente de OfficeScan de los riesgos de seguridad:

TABLA 7-5. Tipos de exploración

TIPO DE EXPLORACIÓN	DESCRIPCIÓN
Exploración en tiempo real	Explora automáticamente un archivo del endpoint en el momento de la recepción, la apertura, la descarga, la copia o la modificación Consulte *Exploración en tiempo real en la página 7-16* para obtener más información.

Tipo de exploración	Descripción
Exploración manual	Exploración iniciada por el usuario que explora un archivo o un conjunto de archivos solicitados por el usuario Consulte *Exploración manual en la página 7-19* para obtener más información.
Exploración programada	Explora automáticamente los archivos del endpoint en función de un programa que el administrador o el usuario final han configurado Consulte *Exploración programada en la página 7-21* para obtener más información.
Explorar ahora	Es una exploración iniciada por el administrador que explora los archivos de uno o varios equipos de destino. Consulte *Explorar ahora en la página 7-24* para obtener más información.

Exploración en tiempo real

La Exploración en tiempo real es una exploración continua y constante. Cada vez que se recibe, se abre, se descarga, se copia o se modifica un archivo, la Exploración en tiempo real escanea el archivo en busca de riesgos de seguridad. Si OfficeScan no detecta ningún riesgo de seguridad, el archivo permanece en su ubicación y los usuarios pueden acceder al archivo. En caso de detectar algún riesgo de seguridad o un posible virus o malware, OfficeScan mostrará un mensaje de notificación en el que indicará el nombre del archivo infectado y el riesgo de seguridad específico.

La exploración en tiempo real conserva una caché de exploración persistente que se recarga cada vez que se inicia el Agente de OfficeScan. El Agente de OfficeScan hace un seguimiento de todos los cambios en archivos o carpetas que se han hecho desde la descarga del Agente de OfficeScan y elimina dichos archivos de la caché.

Nota

Para modificar el mensaje de notificación, abra la consola Web y vaya a **Administración** > **Notificaciones** > **Agentes**.

Defina y aplique la configuración de la Exploración en tiempo real a uno o varios agentes y dominios, o bien a todos los agentes que el servidor administra.

Configurar la exploración en tiempo real

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la exploración** > **Configuración de la exploración en tiempo real**.
4. Seleccione las siguientes opciones:
   - **Activar la exploración de virus/malware**
   - **Activar la exploración de spyware/grayware**

   Nota

   Si desactiva la exploración de virus o malware, la de spyware o grayware también se desactiva. Durante una epidemia de virus, la exploración en tiempo real no se puede desactivar (o se activa automáticamente si no lo está) con el fin de evitar que los virus modifiquen o eliminen archivos y carpetas de los equipos del agente.
5. En la pestaña **Destino**, configure lo siguiente:
   - *Actividad del usuario en los archivos en la página 7-28*
   - *Archivos para explorar en la página 7-29*
   - *Configuración de la exploración en la página 7-29*
6. Haga clic en la pestaña **Acción** y, a continuación, configure lo siguiente:

TABLA 7-6. Acciones de exploración

ACCIÓN	REFERENCIA
Acción de virus/ malware	Acción principal (seleccione una): • *Utilizar ActiveAction en la página 7-39* • *Usar la misma acción para todos los tipos de virus/ malware en la página 7-41* • *Usar una acción específica para cada tipo de virus/ malware en la página 7-42* **Nota** Para obtener información detallada acerca de las distintas acciones, consulte *Acciones de exploración de virus y malware en la página 7-38*. Acciones de virus/malware adicionales: • *Directorio de cuarentena en la página 7-42* • *Crear copia de seguridad antes de limpiar los archivos en la página 7-44* • *Damage Cleanup Services en la página 7-45* • *Mostrar un mensaje de notificación cuando se detecte un virus/malware en la página 7-46* • *Mostrar un mensaje de notificación cuando se detecte un probable virus/malware en la página 7-46*
Acción de spyware/ grayware	Acción principal: • *Acciones de exploración de spyware y grayware en la página 7-52* Acción de spyware/grayware adicional: • *Mostrar un mensaje de notificación al detectar spyware o grayware. en la página 7-53*

7. En la pestaña **Exclusión de la exploración**, configure los directorios, los archivos y las extensiones para excluirlos de la exploración.

Para conocer más detalles, consulte *Exclusiones de la exploración en la página 7-33*.

8. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Exploración manual

La exploración manual es una exploración bajo petición que se inicia automáticamente cuando un usuario ejecuta la exploración en la consola del Agente de OfficeScan. El tiempo que lleva completar la exploración depende del número de archivos que se deben explorar y de los recursos de hardware del endpoint del Agente de OfficeScan.

Defina y aplique la configuración de la exploración manual a uno o varios agentes y dominios, o a todos los agentes que administra el servidor.

Configurar la exploración manual

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la exploración** > **Configuración de la exploración manual**.
4. En la pestaña **Destino**, configure lo siguiente:

- *Archivos para explorar en la página 7-29*
- *Configuración de la exploración en la página 7-29*
- *Uso de la CPU en la página 7-31*

5. Haga clic en la pestaña **Acción** y, a continuación, configure lo siguiente:

TABLA 7-7. Acciones de exploración

ACCIÓN	REFERENCIA
Acción de virus/ malware	Acción principal (seleccione una): • *Utilizar ActiveAction en la página 7-39* • *Usar la misma acción para todos los tipos de virus/ malware en la página 7-41* • *Usar una acción específica para cada tipo de virus/ malware en la página 7-42* **Nota** Para obtener información detallada acerca de las distintas acciones, consulte *Acciones de exploración de virus y malware en la página 7-38*. Acciones de virus/malware adicionales: • *Directorio de cuarentena en la página 7-42* • *Crear copia de seguridad antes de limpiar los archivos en la página 7-44* • *Damage Cleanup Services en la página 7-45*
Acción de spyware/ grayware	Acción principal: • *Acciones de exploración de spyware y grayware en la página 7-52*

6. En la pestaña **Exclusión de la exploración**, configure los directorios, los archivos y las extensiones para excluirlos de la exploración.

   Para conocer más detalles, consulte *Exclusiones de la exploración en la página 7-33*.

7. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Exploración programada

La Exploración programada se ejecuta automáticamente en la fecha y hora especificadas. Utilice la exploración programada para automatizar las exploraciones rutinarias en el agente y mejorar la eficacia de la administración de la exploración.

Defina y aplique la configuración de la exploración programada a uno o varios agentes y dominios, o bien a todos los agentes que administra el servidor.

Configurar la exploración programada

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la exploración** > **Configuración de la exploración programada**.
4. Seleccione las siguientes opciones:

   - **Activar la exploración de virus/malware**

- **Activar la exploración de spyware/grayware**

> **Nota**
>
> Si desactiva la exploración de virus o malware, la de spyware o grayware también se desactiva.

5. En la pestaña **Destino**, configure lo siguiente:
   - *Programa en la página 7-32*
   - *Archivos para explorar en la página 7-29*
   - *Configuración de la exploración en la página 7-29*
   - *Uso de la CPU en la página 7-31*
6. Haga clic en la pestaña **Acción** y, a continuación, configure lo siguiente:

TABLA 7-8. Acciones de exploración

ACCIÓN	REFERENCIA
Acción de virus/ malware	Acción principal (seleccione una): • *Utilizar ActiveAction en la página 7-39* • *Usar la misma acción para todos los tipos de virus/ malware en la página 7-41* • *Usar una acción específica para cada tipo de virus/ malware en la página 7-42* **Nota** Para obtener información detallada acerca de las distintas acciones, consulte *Acciones de exploración de virus y malware en la página 7-38*. Acciones de virus/malware adicionales: • *Directorio de cuarentena en la página 7-42* • *Crear copia de seguridad antes de limpiar los archivos en la página 7-44* • *Damage Cleanup Services en la página 7-45* • *Mostrar un mensaje de notificación cuando se detecte un virus/malware en la página 7-46* • *Mostrar un mensaje de notificación cuando se detecte un probable virus/malware en la página 7-46*
Acción de spyware/ grayware	Acción principal: • *Acciones de exploración de spyware y grayware en la página 7-52* Acción de spyware/grayware adicional: • *Mostrar un mensaje de notificación al detectar spyware o grayware. en la página 7-53*

7. En la pestaña **Exclusión de la exploración**, configure los directorios, los archivos y las extensiones para excluirlos de la exploración.

Para conocer más detalles, consulte *Exclusiones de la exploración en la página 7-33*.

8. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Explorar ahora

Los administradores de OfficeScan inician la opción Explorar ahora de forma remota mediante la consola Web y puede estar dirigida a uno o a varios equipos del agente.

Defina y aplique la configuración de Explorar ahora a uno o varios agentes y dominios, o bien a todos los agentes que administra el servidor.

Configurar Explorar ahora

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la exploración** > **Configuración de Explorar ahora**.
4. Seleccione las siguientes opciones:

   - **Activar la exploración de virus/malware**

- **Activar la exploración de spyware/grayware**

> **Nota**
>
> Si desactiva la exploración de virus o malware, la de spyware o grayware también se desactiva.

5. En la pestaña **Destino**, configure lo siguiente:

   - *Archivos para explorar en la página 7-29*
   - *Configuración de la exploración en la página 7-29*
   - *Uso de la CPU en la página 7-31*

6. Haga clic en la pestaña **Acción** y, a continuación, configure lo siguiente:

TABLA 7-9. Acciones de exploración

ACCIÓN	REFERENCIA
Acción de virus/ malware	Acción principal (seleccione una): • *Utilizar ActiveAction en la página 7-39* • *Usar la misma acción para todos los tipos de virus/ malware en la página 7-41* • *Usar una acción específica para cada tipo de virus/ malware en la página 7-42* **Nota** Para obtener información detallada acerca de las distintas acciones, consulte *Acciones de exploración de virus y malware en la página 7-38*. Acciones de virus/malware adicionales: • *Directorio de cuarentena en la página 7-42* • *Crear copia de seguridad antes de limpiar los archivos en la página 7-44* • *Damage Cleanup Services en la página 7-45*

Acción	Referencia
Acción de spyware/ grayware	Acción principal: • *Acciones de exploración de spyware y grayware en la página 7-52*

7. En la pestaña **Exclusión de la exploración**, configure los directorios, los archivos y las extensiones para excluirlos de la exploración.

   Para conocer más detalles, consulte *Exclusiones de la exploración en la página 7-33*.

8. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Iniciar Explorar ahora

Inicie la opción Explorar ahora en los equipos que sospeche puedan estar infectados.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Tareas** > **Explorar ahora**.
4. Para cambiar la configuración previa de **Explorar ahora** antes de iniciar la exploración, haga clic en **Configuración**.

Aparecerá la pantalla **Configuración de Explorar ahora**. Consulte *Explorar ahora en la página 7-24* para obtener más información.

5. En el árbol de agentes, seleccione los agentes que realizarán la exploración y, a continuación, haga clic en **Iniciar Explorar ahora**.

   El servidor envía una notificación a los agentes.

6. Compruebe el estado de la notificación para ver si hay agentes que no la recibieron.

7. Haga clic en **Seleccionar endpoints no notificados** y, a continuación, haga clic en **Iniciar Explorar ahora** para volver a enviar la notificación de inmediato a los agentes que no la recibieron.

   Ejemplo: número total de agentes: 50

   TABLA 7-10. Situaciones de agentes sin notificar

SELECCIÓN DEL ÁRBOL DE AGENTES	AGENTES NOTIFICADOS (TRAS HACER CLIC EN "INICIAR EXPLORAR AHORA")	AGENTES SIN NOTIFICAR
Ninguno (los 50 agentes seleccionados automáticamente)	35 de 50 agentes	15 agentes
Selección manual (45 de 50 agentes seleccionados)	40 de 45 agentes	5 agentes + otros 5 agentes no incluidos en la selección manual

8. Haga clic en **Detener notificación** para indicar a OfficeScan que deje de enviar la notificación a los agentes que ya la han recibido. Los agentes que ya hayan sido notificados y los que se encuentren en el proceso de la exploración ignorarán este comando.

9. En el caso de los agentes que ya se encuentran en el proceso de exploración, haga clic en **Detener Explorar ahora** para notificarles que detengan la exploración.

Configuración común para todos los tipos de exploración

Establezca tres tipos de configuración para cada tipo de exploración: criterios de exploración, exclusiones de exploración y acciones de exploración. Aplique esta configuración a uno o a varios agentes y dominios, o bien a todos los agentes que administra el servidor.

Criterios de exploración

Especifique qué archivos debería escanear un determinado tipo de exploración mediante los atributos de archivo, como el tipo y la extensión de archivo. Especifique también las condiciones que provocarán la exploración. Por ejemplo, configure la exploración en tiempo real para que realice una exploración de cada archivo una vez que se descargue en el endpoint.

Actividad del usuario en los archivos

Seleccione las actividades en los archivos que darán lugar al inicio de la Exploración en tiempo real. Seleccione una de las siguientes opciones:

- **Explorar archivos creados/modificados**: explora los nuevos archivos que se han introducido en el endpoint (por ejemplo, tras descargar un archivo), o bien archivos que se están modificando
- **Explorar archivos recuperados**: explora los archivos cuando se abren
- **Explorar archivos creados/modificados y recuperados**

Por ejemplo, si se selecciona la tercera opción, se realizará la exploración de un archivo nuevo que se haya descargado en el endpoint, el cual permanecerá en su ubicación actual si no se detecta ningún riesgo de seguridad. Se explorará el mismo archivo cuando el usuario lo abra y, en caso de que éste lo modifique, antes de que se guarden las modificaciones realizadas.

Archivos para explorar

Seleccione una de las siguientes opciones:

- **Todos los archivos explorables**: explora todos los archivos.
- **Tipos de archivo explorados por IntelliScan**: explora solo los archivos que se sabe que pueden albergar código malicioso, incluidos los que se ocultan en un nombre de extensión inofensivo.

  Consulte *IntelliScan en la página E-6* para obtener más información.
- **Archivos con las siguientes extensiones**: explora solo los archivos cuyas extensiones estén incluidas en la lista de extensiones de archivo. Agregue nuevas extensiones o elimine cualquiera de las ya existentes.

Configuración de la exploración

Seleccione una o varias de las opciones siguientes:

- **Explorar disquete durante el apagado del sistema**: la exploración en tiempo real explora cualquier disquete en busca de virus de sector de arranque antes de apagar el endpoint. De esta forma se impide que se ejecute cualquier virus/malware cuando algún usuario reinicie el endpoint a partir del disco.
- **Explorar carpetas ocultas**: permite a OfficeScan detectar y explorar las carpetas ocultas del endpoint durante la exploración manual.
- **Explorar unidad de red**: explora unidades o carpetas de red asignadas al endpoint del Agente de OfficeScan durante la exploración manual o en tiempo real.
- **Explorar el sector de arranque del dispositivo de almacenamiento USB tras conectarlo**: explora automáticamente solo el sector de arranque de un dispositivo de almacenamiento USB cada vez que el usuario lo conecta (Exploración en tiempo real).
- **Explorar todos los archivos de los dispositivos de almacenamiento extraíbles tras conectarlos**: explora automáticamente todos los archivos de un dispositivo de almacenamiento USB cada vez que el usuario lo conecta (Exploración en tiempo real).

- **Poner en cuarentena las variantes de malware detectadas en la memoria**: La supervisión de comportamiento explora la memoria del sistema en busca de procesos sospechosos, y la exploración en tiempo real asigna el proceso y lo explora en busca de amenazas de malware. Si existe una amenaza de malware, la exploración en tiempo real pone en cuarentena el proceso o el archivo.

  Nota

  Esta función requiere que los administradores activen el servicio de prevención de cambios no autorizados y el servicio de protección avanzada.

- **Explorar archivos comprimidos**: permite a OfficeScan explorar un número determinado de capas de compresión y omitir la exploración de las capas sobrantes. OfficeScan también limpia o elimina los archivos infectados que se encuentran en archivos comprimidos. Por ejemplo, si el máximo son dos capas y un archivo comprimido que va a explorarse tiene seis, OfficeScan explora dos capas y omite las cuatro restantes. Si un archivo comprimido contiene amenazas de seguridad, OfficeScan lo limpia o lo elimina.

  Nota

  OfficeScan trata los archivos de Microsoft Office 2007 con formato de Office Open XML como si fueran archivos comprimidos. Office Open XML, el formato de archivo de las aplicaciones de Office 2007, utiliza tecnologías de compresión ZIP. Si desea que los archivos creados mediante estas aplicaciones se exploren en busca de virus/malware, debe activar la exploración de archivos comprimidos.

- **Explorar objetos OLE**: Cuando un archivo contiene varias capas de incrustación y vinculación de objetos (OLE), OfficeScan explora el número de capas que se haya especificado y omite las demás.

  Todos los agentes que administra el servidor tienen activada esta configuración durante los procesos Exploración manual, Exploración en tiempo real, Exploración programada y Explorar ahora. Todas las capas se escanean en busca de virus o malware y spyware o grayware.

  Por ejemplo:

  Si se especifican dos capas, un documento de Microsoft Word está incrustado en el archivo (primera capa). En el documento de Word, se encuentra una hoja de

cálculo de Microsoft Excel (segunda capa), en la cual se encuentra un archivo `.exe` (tercera capa). OfficeScan explorará el documento de Word y la hoja de cálculo de Excel, pero omitirá el archivo `.exe`.

- **Detectar código de exploit en archivos OLE**: La detección de exploits OLE identifica malware de forma heurística buscando un código de exploit en los archivos de Microsoft Office.

Nota

El número de capas especificado se aplica a las opciones **Explorar objetos OLE** y a **Detectar código de exploit en archivos OLE**.

- **Activar IntelliTrap**: detecta y elimina virus o malware de archivos comprimidos ejecutables. Esta opción solo está disponible para la exploración en tiempo real.

  Consulte *IntelliTrap en la página E-7* para obtener más información.

- **Activar la exploración de explotación de CVE para archivos descargados mediante la Web y los canales de correo electrónico**: Bloquea los procesos que intentan aprovechar vulnerabilidades conocidas en productos disponibles comercialmente según el sistema de vulnerabilidades y exposiciones comunes (CVE). Esta opción solo está disponible para la exploración en tiempo real.

- **Explorar sector de arranque**: explora el sector de arranque del disco duro en busca de virus o malware durante los procesos Exploración manual, Exploración programada y Explorar ahora.

Uso de la CPU

OfficeScan puede realizar una pausa después de explorar un archivo y antes de explorar el siguiente. Esto se utiliza durante la Exploración manual, la Exploración programada y Explorar ahora.

Seleccione una de las siguientes opciones:

- **Alto**: sin pausas entre las exploraciones.
- **Medio**: realiza pausas entre exploraciones de archivos si el consumo de la CPU es superior al 50 %, y no realiza ninguna pausa si es del 50 % o inferior.

- **Bajo**: realiza pausas entre exploraciones de archivos si el consumo de la CPU es superior al 20 %, y no realiza ninguna pausa si es del 20 % o inferior.

Si selecciona Medio o Bajo, cuando se inicia la exploración y el consumo de CPU se encuentra dentro del umbral (50 % o 20 %), OfficeScan no realizará ninguna pausa entre las exploraciones, lo que permite que se realice una exploración más rápida en el tiempo. OfficeScan utiliza más recursos de la CPU durante el proceso, pero como el consumo de CPU es el óptimo, el rendimiento del endpoint no se ve drásticamente afectado. Cuando el consumo de la CPU comienza a superar el umbral, OfficeScan realiza una pausa para reducir el uso de la CPU, y se reanuda cuando el consumo vuelve a situarse dentro del umbral.

Si selecciona Alto, OfficeScan no comprobará el consumo de la CPU actual y explorará los archivos sin realizar ninguna pausa.

Programa

Configure con cuánta frecuencia (diaria, semanal o mensual) y a qué hora se ejecutará una exploración programada.

Para las exploraciones programadas mensuales, puede seleccionar un día concreto del mes o un día de la semana y el orden dentro del mes.

- **Día concreto del mes**: Selecciónelo entre el día 1 y el 31. Si selecciona los días 29, 30 o 31 y el mes no tiene esos días, OfficeScan ejecutará la exploración programada el último día del mes. Por lo tanto:
    - Si selecciona el día 29, la exploración programada se ejecutará el 28 de febrero (excepto en los años bisiestos) y el día 29 en el resto de los meses.
    - Si selecciona el día 30, la exploración programada se ejecutará el 28 o el 29 de febrero, y el día 30 en el resto de los meses.
    - Si selecciona el día 31, la exploración programada se ejecutará el 28 o el 29 de febrero, el día 30 de abril, de junio, de septiembre y de noviembre, y el día 31 en el resto de los meses.
- **Un día de la semana y su orden dentro del mes**: Un mismo día de la semana se repite cuatro o cinco veces dentro de un mes. Por ejemplo, en un mes normalmente hay cuatro lunes. Especifique un día de la semana y el orden dentro del mes. Por

ejemplo, seleccione ejecutar la exploración programada el segundo lunes de cada mes. Si selecciona el quinto día del día elegido y este día no existe en un determinado mes, la exploración se ejecutará el cuarto día.

Exclusiones de la exploración

Defina las exclusiones de la exploración para aumentar el rendimiento de ésta y omitir la exploración de archivos que provocan falsas alarmas. Cuando se ejecuta un tipo de exploración determinado, OfficeScan comprueba la lista de exclusión de la exploración y determina qué archivos del endpoint no se incluirán en la exploración de virus/malware y spyware/grayware.

Cuando active la exclusión de la exploración, OfficeScan no explorará ningún archivo que presente las siguientes condiciones:

- El archivo se encuentra en un directorio determinado (o en cualquiera de sus subdirectorios).
- El nombre del archivo coincide con alguno de los nombres incluidos en la Lista de Exclusiones.
- La extensión del archivo coincide con alguna de las extensiones incluidas en la Lista de Exclusiones.

Consejo

Para obtener una lista de productos que Trend Micro recomienda sin incluir exploraciones en tiempo real, vaya a:

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Excepciones comodín

Las listas de exclusión de la exploración para archivos y directorios son compatibles con el uso de caracteres comodines. Utilice el carácter "?" para sustituir un carácter y "*" para sustituir varios caracteres.

Utilice los caracteres comodín prudentemente. El uso de un caracter incorrecto puede excluir archivos o directorios incorrectos. Por ejemplo, añadir `C:\*` a la lista de exclusión de la exploración (archivos) excluiría el disco `C:\` al completo.

TABLA 7-11. Exclusiones de la exploración mediante el uso de caracteres comodín

VALOR	EXCLUIDO	NO EXCLUIDO

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Todos los archivos `.txt` del directorio `C:\`	El resto de tipos de archivos del directorio `C:\`
`[]`	Incompatible	Incompatible

Lista de exclusión de la exploración (directorios)

OfficeScan no explorará todos los archivos que se encuentren dentro de un determinado directorio del equipo. Puede especificar un máximo de 256 directorios.

Nota

Al excluir un directorio de las exploraciones, OfficeScan excluye de las exploraciones automáticamente todos los subdirectorios del directorio.

También puede seleccionar **Excluir directorios donde hay instalados productos de Trend Micro**. Si selecciona esta opción, OfficeScan excluye automáticamente de la exploración los directorios de los siguientes productos de Trend Micro:

- <*Carpeta de instalación del servidor*>

Nota

Durante una exploración manual, OfficeScan explora la carpeta de instalación del servidor.

- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

Si tiene un producto de Trend Micro que NO aparece en la lista, añada los directorios del producto a la Lista de Exclusiones de la exploración.

De igual forma, vaya a la sección **Configuración de la exploración** de **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad** para configurar OfficeScan de manera que se excluyan los directorios de Microsoft Exchange 2000/2003. Si utiliza Microsoft Exchange 2007 o una versión posterior, añada manualmente el directorio a la lista de exclusiones de la exploración. Acceda al sitio siguiente para obtener más detalles sobre la exclusión de la exploración:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Cuando configure la lista de archivos, seleccione una de las siguientes opciones:

- **Se retiene la lista actual** (default): OfficeScan proporciona esta opción para evitar la sobrescritura accidental de la lista de exclusión existente del agente. Para guardar e implementar los cambios de la lista de exclusión, seleccione cualquiera de las otras opciones.

- **Se sobrescribe**: esta opción quita la lista de exclusión completa del agente y la reemplaza con la lista actual. Tras hacer clic en **Aplicar a todos los agentes**, OfficeScan muestra un mensaje de confirmación de advertencia.
- **Se agregan rutas a esta**: esta opción agrega los elementos de la lista actual a la lista de exclusión del agente. Si ya existe un elemento en la lista de exclusión del agente, el agente lo omitirá.
- **Se eliminan rutas de esta**: esta opción elimina los elementos de la lista actual de la lista de exclusión del agente, si se encuentra.

Lista de exclusión de la exploración (archivos)

OfficeScan no explorará un archivo si su nombre coincide con alguno de los nombres incluidos en la lista de exclusión. Si desea excluir un archivo que se encuentra en una determinada ubicación del endpoint, incluya su ruta, por ejemplo `C:\Temp\sample.jpg`.

Puede especificar un máximo de 256 archivos.

Cuando configure la lista de archivos, seleccione una de las siguientes opciones:

- **Se retiene la lista actual** (default): OfficeScan proporciona esta opción para evitar la sobrescritura accidental de la lista de exclusión existente del agente. Para guardar e implementar los cambios de la lista de exclusión, seleccione cualquiera de las otras opciones.
- **Se sobrescribe**: esta opción quita la lista de exclusión completa del agente y la reemplaza con la lista actual. Tras hacer clic en **Aplicar a todos los agentes**, OfficeScan muestra un mensaje de confirmación de advertencia.
- **Se agregan rutas a esta**: esta opción agrega los elementos de la lista actual a la lista de exclusión del agente. Si ya existe un elemento en la lista de exclusión del agente, el agente lo omitirá.
- **Se eliminan rutas de esta**: esta opción elimina los elementos de la lista actual de la lista de exclusión del agente, si se encuentra.

Lista de exclusión de la exploración (extensiones de archivos)

OfficeScan no explorará un archivo si su extensión coincide con alguna de las extensiones que se incluyen en la lista de exclusión. Puede especificar un máximo de 256 extensiones de archivo. No es necesario incluir un punto (.) antes de la extensión.

Para la Exploración manual, la Exploración programada y Explorar ahora, utilice el interrogante (?) o el asterisco (*) como caracteres comodín. Por ejemplo, si no desea explorar todos los archivos cuyas extensiones empiecen por la letra D, como `DOC`, `DOT` o `DAT`, escriba `D*` o `D?`.

Nota

La exploración en tiempo real no admite el uso de caracteres comodín para especificar extensiones.

Aplicar la configuración para la exclusión de la exploración a todos los tipos de exploraciones

OfficeScan le permite definir la configuración de la exclusión de la exploración para un determinado tipo de exploración y aplicar la misma configuración al resto de tipos de exploración. Por ejemplo:

Luis, un administrador de OfficeScan, se dio cuenta el 1 de enero que en los equipos del agente hay un gran número de archivos `.JPG` que no suponen ninguna amenaza a la seguridad. Luis añadió `JPG` a la Lista de Exclusiones de archivos para la Exploración manual y aplicó esta configuración a todos los tipos de exploración. Así, la Exploración en tiempo real, Explorar ahora y la Exploración programada están configuradas para que omitan la exploración de los archivos `.jpg`.

Una semana después, Luis eliminó `JPG` de la lista de exclusión para la Exploración en tiempo real pero no aplicó la configuración a todos los tipos de exploraciones. En este caso, los archivos `JPG` se explorarán pero únicamente durante la Exploración en tiempo real.

Acciones de exploración

Especifique la acción que realizará OfficeScan cuando un tipo de exploración determinado detecte un riesgo de seguridad. OfficeScan presenta una serie de acciones de exploración diferentes para virus/malware y spyware/grayware.

Acciones de exploración de virus y malware

La acción de exploración que OfficeScan realiza depende del tipo de virus o malware y el tipo de exploración que ha detectado el virus o malware. Por ejemplo, cuando OfficeScan detecta un troyano (tipo de virus/malware) durante la Exploración manual (tipo de exploración), limpia (acción) el archivo infectado.

Para obtener información sobre los diferentes tipos de virus o malware, consulte *Virus y malware en la página 7-2*.

A continuación se describen las acciones que OfficeScan puede llevar a cabo para hacer frente a virus o malware.

TABLA 7-12. Acciones de exploración de virus y malware

ACCIÓN	DESCRIPCIÓN
Eliminar	OfficeScan elimina el archivo infectado.
Cuarentena	OfficeScan cambia el nombre del archivo infectado, lo cifra y lo mueve a un directorio de cuarentena temporal en el agente del endpoint, que se encuentra en <*Carpeta de instalación del agente*>`\Suspect`. A continuación, el Agente de OfficeScan envía los archivos en cuarentena al directorio de cuarentena especificado. Consulte *Directorio de cuarentena en la página 7-42* para obtener más información. El directorio de cuarentena predeterminado se encuentra en el servidor de OfficeScan, en <*Carpeta de instalación del servidor*>`\PCCSRV\Virus`. Si debe restaurar cualquiera de los archivos en cuarentena, utilice Central Quarantine Restore. Para conocer más detalles, consulte *Restauración de archivos en cuarentena en la página 7-46*.

Acción	Descripción
Limpiar	OfficeScan limpia el archivo infectado antes de permitir acceso completo al archivo. Si el archivo no se puede limpiar, OfficeScan realiza una segunda acción, la cual puede ser una de las acciones siguientes: poner en cuarentena, eliminar, cambiar nombre y omitir. Para configurar la segunda acción, haga clic en **Agentes** > **Administración de agentes**. Haga clic en **Configuración** > **Configuración de la exploración** > **{Tipo de exploración} pestaña** > **Acción**. Esta acción se puede realizar con todos los tipos de malware con excepción de virus/malware probables.
Cambiar nombre	OfficeScan cambia la extensión del archivo infectado por "`vir`". Los usuarios no pueden abrir el archivo inicialmente infectado pero sí pueden hacerlo si lo asocian a una determinada aplicación. un virus/malware podría ejecutarse al abrir el archivo infectado con el nombre cambiado.
Omitir	OfficeScan solo puede aplicar esta acción de exploración cuando detecta algún tipo de virus durante las acciones Exploración manual, Exploración programada y Explorar ahora. OfficeScan no puede utilizar esta acción durante la exploración en tiempo real porque, si no se realiza ninguna acción cuando se detecta un intento de abrir o ejecutar un archivo infectado, permitirá la ejecución de virus/malware. Todas las otras acciones de exploración se pueden utilizar durante la exploración en tiempo real.
Denegar acceso	Esta acción de exploración solo se puede realizar durante la exploración en tiempo real. Cuando OfficeScan detecta un intento de abrir o ejecutar un archivo infectado, inmediatamente bloquea la operación. Los usuarios pueden eliminar el archivo infectado manualmente.

Utilizar ActiveAction

Los distintos tipos de virus y malware requieren acciones de exploración diferentes. La personalización de las acciones de exploración requiere una serie de conocimientos

acerca de los virus/malware, y puede resultar una tarea tediosa. OfficeScan utiliza ActiveAction para hacer frente a estos problemas.

ActiveAction es un conjunto de acciones de exploración preconfiguradas para la defensa frente a los virus y el malware. Si no está familiarizado con las acciones de exploración o si no está seguro de cuál es la acción más adecuada para un determinado tipo de virus o malware, Trend Micro le recomienda utilizar ActiveAction.

Utilizar ActiveAction ofrece las siguientes ventajas:

- ActiveAction utiliza acciones de exploración recomendadas por Trend Micro. De este modo, no tendrá que perder tiempo configurando las acciones de exploración.
- Los programadores de virus modifican sin cesar el modo en que los virus y el malware atacan a los ordenadores. La configuración de ActiveAction se actualiza para proporcionar protección ante las últimas amenazas y métodos de ataque de los virus y el malware.

Nota

ActiveAction no está disponible para buscar spyware/grayware.

En la siguiente tabla se muestra el modo en que ActiveAction trata cada tipo de virus/malware:

TABLA 7-13. Acciones de exploración recomendadas por Trend Micro frente a virus y malware

TIPO DE VIRUS/ MALWARE	EXPLORACIÓN EN TIEMPO REAL		EXPLORACIÓN MANUAL/ EXPLORACIÓN PROGRAMADA/ EXPLORAR AHORA	
	PRIMERA ACCIÓN	SEGUNDA ACCIÓN	PRIMERA ACCIÓN	SEGUNDA ACCIÓN
Explotación de CVE	Denegar acceso	N/D	N/A	N/A
Broma	Cuarentena	N/D	Cuarentena	N/D
Troyanos	Cuarentena	N/D	Cuarentena	N/D

Tipo de virus/ malware	Exploración en tiempo real		Exploración manual/ Exploración programada/ Explorar ahora	
	Primera acción	Segunda acción	Primera acción	Segunda acción
Virus	Limpiar	Cuarentena	Limpiar	Cuarentena
Virus de prueba	Denegar acceso	N/D	Omitir	N/D
Packer	Cuarentena	N/D	Cuarentena	N/D
Malware probable	Denegar acceso o realizar una acción configurada por el usuario	N/A	Omitir o realizar una acción configurada por el usuario	N/A
Otro malware	Limpiar	Cuarentena	Limpiar	Cuarentena

Para el posible malware, la acción predeterminada es "Denegar acceso" durante la exploración en tiempo real y "Omitir" durante la exploración manual, la exploración programada y Explorar ahora. Si prefiere utilizar otras acciones, tiene a su disposición Poner en cuarentena, Eliminar o Cambiar nombre.

Usar la misma acción para todos los tipos de virus/malware

Seleccione esta opción si desea que se lleve a cabo la mismo acción para todos los tipos de virus o malware, excepto para los virus y malware probables. Si selecciona "Limpiar" como primera acción, seleccione una segunda acción que OfficeScan realiza por si la limpieza no se realiza correctamente. Si la primera acción no es "Limpiar" no se puede establecer una segunda acción.

Si elige "Limpiar" como primera acción, OfficeScan realiza la segunda acción cuando detecta virus o malware probables.

Usar una acción específica para cada tipo de virus/malware

seleccionar manualmente una acción de exploración para cada tipo de virus o malware.

Todas las acciones de exploración están disponibles para todos los tipos de virus y malware, excepto para los virus y malware probables. Si selecciona "Limpiar" como primera acción, seleccione una segunda acción que OfficeScan realiza por si la limpieza no se realiza correctamente. Si la primera acción no es "Limpiar" no se puede establecer una segunda acción.

Para los virus y malware probables están disponibles todas las acciones de exploración, excepto "Limpiar".

Directorio de cuarentena

Si la acción que se debe llevar a cabo sobre un archivo infectado es "Poner en cuarentena", el Agente de OfficeScan cifrará el archivo y lo moverá a una carpeta de cuarentena temporal ubicada en <*Carpeta de instalación del agente*>\SUSPECT y, a continuación, lo enviará al directorio de cuarentena especificado.

Nota

Puede restaurar archivos en cuarentena cifrados por si necesita acceder a ellos en el futuro.

Para conocer más detalles, consulte *Restaurar archivos cifrados en la página 7-48*.

Acepte el directorio de cuarentena predeterminado, ubicado en el equipo del servidor de OfficeScan. El directorio se encuentra en formato de URL y contiene el nombre de host del servidor o la dirección IP.

- Si el servidor administra agentes IPv4 e IPv6, utilice el nombre de host para que todos los agentes puedan enviar archivos en cuarentena al servidor.
- Si el servidor solo tiene una dirección IPv4 (o se identifica mediante esta), solo los agentes que utilizan IPv4 de manera exclusiva y los agentes de doble pila pueden enviar archivos en cuarentena al servidor.
- Si el servidor solo tiene una dirección IPv6 (o se identifica mediante esta), solo los agentes que utilizan IPv6 de manera exclusiva y los agentes de doble pila pueden enviar archivos en cuarentena al servidor.

También puede especificar un directorio de cuarentena alternativo si escribe la ubicación como una URL, una ruta UNC o una ruta de archivo absoluta. Los agentes deberían poder conectarse a este directorio alternativo. Por ejemplo, el directorio alternativo debe contar con una dirección IPv6 para recibir archivos en cuarentena de agentes de doble pila y que solo utilizan IPv6. Trend Micro recomienda designar un directorio alternativo de doble pila, identificar el directorio por su nombre de host y utilizar la ruta UNC al escribir el directorio.

Consulte la siguiente tabla para ver información sobre cuándo utilizar la URL, la ruta UNC o la ruta de archivos absoluta:

TABLA 7-14. Directorio de cuarentena

DIRECTORIO DE CUARENTENA	FORMATO ACEPTADO	EJEMPLO	NOTAS
Un directorio en el equipo del servidor de OfficeScan	URL	`http://<osceserver>`	Este es el directorio predeterminado. Defina la configuración de este directorio, como el tamaño de la carpeta de cuarentena. Para conocer más detalles, consulte *Administrador de cuarentena en la página 14-65*.
	Ruta UNC	`\\<osceserver>\ofcscan\Virus`	

Directorio de cuarentena	Formato aceptado	Ejemplo	Notas
Directorio de otro equipo del servidor de OfficeScan (en caso de disponer de otros servidores de OfficeScan en la red)	URL	`http://<osceserver2>`	Asegúrese de que los agentes se pueden conectar a este directorio. Si especifica un directorio incorrecto, el Agente de OfficeScan mantendrá los archivos en cuarentena en la carpeta SUSPECT hasta que especifique un directorio de cuarentena correcto. En los registros de virus/malware del servidor, el resultado de la exploración es "No se puede enviar el archivo en cuarentena a la carpeta de cuarentena indicada". Si utiliza una ruta UNC, asegúrese de que la carpeta del directorio de cuarentena está compartida con el grupo "Todos" y que este grupo tiene asignados derechos de escritura y lectura.
	Ruta UNC	`\\<osceserver2>\ofcscan\Virus`	
Otro endpoint en la red	Ruta UNC	`\\<nombre_equipo>\temp`	
Otro directorio en el Agente de OfficeScan	Ruta absoluta	`C:\temp`	

Crear copia de seguridad antes de limpiar los archivos

Si OfficeScan está configurado para limpiar un archivo infectado, antes es posible realizar una copia de seguridad de éste. Esto le permitirá restaurarlo en caso de que lo necesite en el futuro. OfficeScan cifra el archivo de copia de seguridad para evitar que se abra y, a continuación, lo guarda en la carpeta <*Carpeta de instalación del agente*>`\Backup`.

Para restaurar los archivos de copia de seguridad, consulte *Restaurar archivos cifrados en la página 7-48*.

Damage Cleanup Services

Damage Cleanup Services limpia los equipos de virus basados en archivos y de red, además de restos de virus y gusanos (troyanos, entradas del registro y archivos víricos).

El agente activa Damage Cleanup Services antes o después de la exploración de virus/malware en función del tipo de exploración.

- Cuando se ejecutan los procesos Exploración manual, la Exploración programada y Explorar ahora, el Agente de OfficeScan activa Damage Cleanup Services y, a continuación, inicia la exploración de virus/malware. El agente puede volver a activar Damage Cleanup Services durante la exploración de virus/malware si se requiere una limpieza.
- Durante la Exploración en tiempo real, el Agente de OfficeScan realiza la exploración de virus/malware en primer lugar y, a continuación, activa Damage Cleanup Services si se precisa una limpieza.

Puede seleccionar el tipo de limpieza que ejecuta Damage Cleanup Services:

- **Limpieza estándar**: el Agente de OfficeScan realiza una de las siguientes acciones durante la limpieza estándar:
  - Detecta y elimina troyanos activos.
  - Elimina los procesos creados por los troyanos.
  - Repara los archivos del sistema modificados por los troyanos.
  - Elimina los archivos y aplicaciones depositados por los troyanos.
- **Limpieza avanzada**: además de las acciones de la limpieza estándar, el Agente de OfficeScan detiene las actividades llevadas a cabo por software de seguridad no autorizado (también conocido como FakeAV) y ciertas variantes de rootkits. Además, el Agente de OfficeScan cuenta con reglas de limpieza avanzadas que permiten detectar y detener de forma proactiva las aplicaciones que presentan comportamientos propios de FakeAV y rootkits.

Nota

La limpieza avanzada proporciona una protección proactiva, pero al mismo tiempo devuelve un número elevado de falsos positivos.

Damage Cleanup Services no realiza la limpieza de virus y malware probables a menos que se seleccione la opción **Ejecutar la limpieza cuando se detecte una posible amenaza de virus/malware** Solo se puede seleccionar esta opción si la acción para los virus y el malware probables no es **Omitir** ni **Denegar acceso**. Por ejemplo, si el Agente de OfficeScan detecta virus/malware probables durante la Exploración en tiempo real y la acción establecida es la cuarentena, el Agente de OfficeScan pone en cuarentena el archivo infectado en primer lugar y, a continuación, ejecuta la limpieza si es necesario. El tipo de limpieza (estándar o avanzada) depende de la selección realizada.

Mostrar un mensaje de notificación cuando se detecte un virus/malware

Cuando OfficeScan detecta virus o malware durante la Exploración en tiempo real y la Exploración programada, puede mostrar un mensaje en el que se informa al usuario acerca de la detección.

Para modificar el mensaje de notificación, seleccione **Virus/Malware** en el menú desplegable **Tipo** de **Administración** > **Notificaciones** > **Agentes**.

Mostrar un mensaje de notificación cuando se detecte un probable virus/malware

Cuando OfficeScan detecta virus o malware probables durante la exploración en tiempo real y la exploración programada, puede mostrar un mensaje en el que se informa al usuario acerca de la detección.

Para modificar el mensaje de notificación, seleccione **Virus/Malware** en el menú desplegable **Tipo** de **Administración** > **Notificaciones** > **Agentes**.

Restauración de archivos en cuarentena

Puede restaurar archivos que OfficeScan haya puesto en cuarentena si cree que la detección no fue precisa. La característica Central Quarantine Restore le permite buscar archivos en el directorio de cuarentena y llevar a cabo comprobaciones de verificación SHA1 para asegurarse de que los archivos que quiere restaurar no se hayan modificado.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, seleccione un dominio o un agente.
3. Haga clic en **Tareas** > **Central Quarantine Restore**.

   Aparecerá la pantalla de **Criterios de Central Quarantine Restore Criteria**.
4. Escriba el nombre de los datos que quiere restaurar en el campo **Archivo/Objeto infectado**.
5. Si lo prefiere, puede especificar el período de tiempo, el nombre de la amenaza de seguridad y la ruta del archivo de datos.
6. Haga clic en **Buscar**.

   En la pantalla **Central Quarantine Restore** que aparece se muestran los resultados de la búsqueda.
7. Seleccione **Agregar el archivo restaurado a la lista de exclusión de nivel de dominio** para asegurar que todos los Agentes de OfficeScan de los dominios en los que se restauran los archivos los agreguen a la lista de exclusión de la exploración.

   Esto garantiza que OfficeScan no detecte los archivos como una amenaza en futuras exploraciones.
8. Si lo desea, puede escribir el valor SHA1 del archivo para poder verificarlo.
9. Seleccione los archivos de la lista que quiere restaurar y haga clic en **Restaurar**.

Consejo

Para ver los Agentes de OfficeScan individuales que restauran el archivo, haga clic en el enlace de la columna **Endpoints**.

10. Haga clic en **Cerrar** en el cuadro de diálogo de confirmación.

Para comprobar que OfficeScan ha restaurado los archivos en cuarentena de forma correcta, consulte *Visualización de los registros de Central Quarantine Restore en la página 7-106*.

Restaurar archivos cifrados

Para evitar que se abra un archivo infectado, OfficeScan lo cifra:

- Antes de ponerlo en cuarentena
- Al realizar una copia de seguridad de él anterior a su limpieza

OfficeScan proporciona una herramienta que descifra y, luego, restaura el archivo en caso de que necesite recuperar información de él. OfficeScan puede descifrar y restaurar los siguientes archivos:

TABLA 7-15. Archivos que OfficeScan puede descifrar y restaurar

ARCHIVO	DESCRIPCIÓN
Archivos en cuarentena en el endpoint del agente	Estos archivos se encuentran en la carpeta <*Carpeta de instalación del agente*>`\SUSPECT\Backup` y se purgan automáticamente después de siete días. Estos archivos también se cargan al directorio de cuarentena designado del servidor de OfficeScan.
Archivos en cuarentena del directorio de cuarentena designado	De forma predeterminada, este directorio está ubicado en el equipo del servidor de OfficeScan. Para conocer más detalles, consulte *Directorio de cuarentena en la página 7-42*.

ARCHIVO	DESCRIPCIÓN
Copias de seguridad de los archivos cifrados	Estas son las copias de seguridad de los archivos infectados que OfficeScan ha podido limpiar. Estos archivos se encuentran en la carpeta `<carpeta de instalación del agente>\Backup`. Para restaurar estos archivos, es necesario que los usuarios los muevan a la carpeta `<carpeta de instalación del agente>\SUSPECT\Backup`. OfficeScan solo realiza copias de seguridad y cifra los archivos antes de limpiarlos si selecciona la acción **Crear copia de seguridad del archivo antes de limpiarlo** en **Agentes** > **Administración de agentes** y hace clic en **Configuración** > **Configuración de la exploración** > **{Tipo de exploración} pestaña** > **Acción**.

¡ADVERTENCIA!

Si se recupera un archivo infectado, el virus o malware podría propagarse a otros archivos y equipos. Antes de restaurar el archivo, aísle el endpoint infectado y mueva archivos importantes de este endpoint a una ubicación de copia de seguridad.

Descifrado y restauración de archivos

Procedimiento

- Si el archivo se encuentra en el endpoint del Agente de OfficeScan:

  a. Abra el símbolo del sistema y vaya a <*carpeta de instalación del agente*>.

  b. Ejecute `VSEncode.exe` haciendo doble clic en el archivo o escribiendo lo siguiente en el símbolo del sistema:

  ```
  VSEncode.exe /u
  ```

  Este parámetro hace que se abra una pantalla en la que aparece una lista de los archivos que se encuentran en `<carpeta de instalación del agente>\SUSPECT\Backup`.

  c. Seleccione un archivo para restaurar y haga clic en **Restaurar**. La herramienta sólo puede restaurar los archivos de uno en uno.

d. En la pantalla que se abre, especifique la carpeta en la que desea restaurar el archivo.

e. Haga clic en **Aceptar**. El archivo se restaurará en la carpeta especificada.

Nota

Es posible que en cuanto el archivo se restaure, OfficeScan lo escanee de nuevo y lo trate como si estuviera infectado. Para evitar que esto ocurra, agréguelo a la Lista de Exclusiones de la exploración. Consulte *Exclusiones de la exploración en la página 7-33* para obtener más información.

f. Haga clic en **Cerrar** cuando haya terminado de restaurar los archivos.

- Si el archivo se encuentra en el servidor de OfficeScan en un directorio de cuarentena personalizado:

  a. Si el archivo se encuentra en el equipo del servidor de OfficeScan, abra el símbolo del sistema y vaya a <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\VSEncrypt`.

  Si el archivo se encuentra en un directorio de cuarentena personalizado, vaya a `<Carpeta de instalación del servidor>\PCCSRV\Admin\Utility` y copie la carpeta `VSEncrypt` en el endpoint en el que se encuentra el directorio de cuarentena personalizado.

  b. Cree un archivo de texto y escriba a continuación la ruta completa de los archivos que desee cifrar o descifrar.

  Por ejemplo, para restaurar los archivos de `C:\Mis documentos\Informes`, escriba `C:\Mis documentos\Informes\*.*` en el archivo de texto.

  Los archivos en cuarenta del equipo del servidor de OfficeScan se encuentran en `<carpeta de instalación del servidor>\PCCSRV\Virus`.

  c. Guarde el archivo de texto con una extensión `INI` o `TXT`. Por ejemplo, guárdelo con el nombre `ForEncryption.ini` en la unidad `C:`.

  d. Abra el símbolo del sistema y vaya al directorio en el que se encuentra la carpeta `VSEncrypt`.

e. Ejecute el archivo `VSEncode.exe` escribiendo lo siguiente:

```
VSEncode.exe /d /i <ubicación del archivo INI o TXT>
```

Donde:

`<ubicación del archivo INI o TXT>` es la ruta del archivo `INI` o `TXT` que ha creado (por ejemplo, `C:\ForEncryption.ini`).

f. Utilice los otros parámetros para emitir varios comandos.

TABLA 7-16. Restaurar parámetros

PARÁMETRO	DESCRIPCIÓN
Ninguno (sin parámetros)	Cifrar archivos
/d	Descifrar archivos
/debug	Cree un registro de depuración y guárdelo en el endpoint. En el endpoint del Agente de OfficeScan, el registro de depuración `VSEncrypt.log` se crea en `<Carpeta de instalación del agente>`.
/o	Sobrescribe un archivo cifrado o descifrado si ya existe.
/f <nombre del archivo>	Cifra o descifra un único archivo
/nr	No restaura el nombre del archivo original
/v	Muestra información acerca de la herramienta
/u	Inicia la interfaz de usuario de la herramienta
/r <Carpeta de destino>	La carpeta en la que se restaurará un archivo
/s <Nombre del archivo original>	El nombre del archivo cifrado original

Por ejemplo, escriba `VSEncode [/d] [/debug]` para descifrar los archivos de la carpeta `Suspect` y crear un registro de depuración. Cuando se descifra o cifra un archivo, OfficeScan crea el archivo descifrado o cifrado en la misma

carpeta. Antes de descifrar o cifrar un archivo, asegúrese de que no está bloqueado.

Acciones de exploración de spyware y grayware

La acción de exploración que OfficeScan realiza depende del tipo de exploración que ha detectado el spyware/grayware. Mientras que se pueden configurar determinadas acciones para cada tipo de virus/malware, solo se puede configurar una sola acción para los tipos de spyware/grayware. Por ejemplo, cuando OfficeScan detecta cualquier tipo de spyware/grayware durante la Exploración manual (tipo de exploración), limpia (acción) los recursos del sistema afectados.

Para obtener información sobre los diferentes tipos de spyware/grayware, consulte *Spyware y grayware en la página 7-5*.

Nota

Las acciones de exploración de spyware/grayware solo se pueden configurar a través de la consola Web. La consola del Agente de OfficeScan no otorga acceso a esta configuración.

En la siguiente tabla se describen las acciones que OfficeScan puede llevar a cabo proteger contra spyware/grayware.

TABLA 7-17. Acciones de exploración de spyware y grayware

ACCIÓN	DESCRIPCIÓN
Limpiar	OfficeScan finaliza los procesos o elimina los registros, archivos, cookies y accesos directos. Después de limpiar el spyware/grayware, los Agentes de OfficeScan realizan una copia de seguridad de los datos de spyware/grayware, los cuales puede restaurar si considera que el acceso a estos casos de spyware y grayware no representa un peligro. Consulte *Restaurar spyware/grayware en la página 7-56* para obtener más información.

Acción	Descripción
Omitir	OfficeScan no realiza ninguna acción sobre los componentes de spyware/grayware detectados pero registra la detección de spyware/grayware en los registros. Esta acción sólo se puede llevar a cabo durante la Exploración manual, la Exploración programada y Explorar ahora. Durante el Escaneo en tiempo real, la acción es "Denegar acceso". OfficeScan no llevará a cabo ninguna acción si el spywareo grayware detectado está incluido en la lista de permitidos. Consulte *Lista de spyware/grayware permitido en la página 7-53* para obtener más información.
Denegar acceso	OfficeScan deniega el acceso a los componentes de spyware/grayware detectados para copiarlos o abrirlos Esta acción sólo se puede llevar a cabo durante la Exploración en tiempo real. Durante el Escaneo manual, los Escaneos programados y Explorar ahora, la acción es "Omitir".

Mostrar un mensaje de notificación al detectar spyware o grayware.

Cuando OfficeScan detecta spyware o grayware durante la Exploración en tiempo real y la Exploración programada, puede mostrar un mensaje en el que se informa al usuario acerca de la detección.

Para modificar el mensaje de notificación, seleccione **Spyware/Grayware** en el menú desplegable **Tipo** de **Administración** > **Notificaciones** > **Agentes**.

Lista de spyware/grayware permitido

OfficeScan ofrece una lista de spyware y grayware "permitido" que contiene los archivos o las aplicaciones que no desea que se traten como spyware y grayware. Cuando se detecta un spyware y grayware determinado durante el proceso de exploración, OfficeScan revisa la lista de spyware y grayware permitido y no realiza ninguna acción si encuentra alguna coincidencia entre lo detectado y algún elemento de la lista.

Aplique la lista de permitidos a uno o varios agentes y dominios, o bien a todos los agentes que el servidor administra. La lista de spyware y grayware permitido se aplica a todos los tipos de exploraciones, lo que significa que se utilizará la misma lista para la

Exploración manual, la Exploración en tiempo real, la Exploración programada y Explorar ahora.

Adición del spyware/grayware ya detectado a la Lista de Permitidos.

Procedimiento

1. Vaya a una de las siguientes opciones:
   - **Agentes** > **Administración de agentes**
   - **Registros** > **Agentes** > **Riesgos de seguridad**
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de spyware y grayware** o **Ver registros** > **Registros de spyware y grayware**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Seleccione los registros y haga clic en **Agregar a lista de permitidos**.
6. Aplique el spyware/grayware permitido solo a los equipos del agente seleccionados o a determinados dominios.
7. Haga clic en **Guardar**. Los agentes seleccionados aplican la configuración y el servidor de OfficeScan agrega el spyware/grayware a la lista de spyware y grayware permitido que se encuentra en **Agentes** > **Administración de agentes** > **Configuración** > **Lista de spyware/grayware permitido**.

Nota

OfficeScan admite un máximo de 1.024 elementos de spyware/grayware en la lista de permitidos.

Administrar la lista de spyware/grayware permitido

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Lista de spyware/grayware permitido**.
4. En la tabla **Nombres de spyware y grayware**, seleccione un nombre de spyware y grayware. Para seleccionar varios nombres, mantenga pulsada la tecla Ctrl mientras realiza las selecciones individuales.
   - También puede escribir una palabra clave en el campo **Buscar** y hacer clic en **Buscar**. OfficeScan actualizará la tabla con los nombres que coincidan con la palabra clave.
5. Haga clic en **Agregar**.

   Los nombres se mueven a la tabla **Lista de permitidos**.
6. Para quitar nombres de la lista permitida, seleccione los nombre que desee y haga clic en **Quitar**. Para seleccionar varios nombres, mantenga pulsada la tecla Ctrl mientras realiza las selecciones individuales.
7. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Restaurar spyware/grayware

Tras limpiar el spyware/grayware, los Agentes de OfficeScan realizan una copia de seguridad de los datos de spyware/grayware. Notifique a un agente que esté conectado de manera que restaure los datos de los cuales se ha realizado una copia de seguridad si considera que estos son inofensivos. Seleccione los datos de spyware/grayware que se restaurarán según la hora de la copia de seguridad.

Nota

Los usuarios del Agente de OfficeScan no pueden iniciar la restauración de spyware/grayware y no reciben ninguna notificación sobre los datos guardados como copia de seguridad que el agente ha podido restaurar.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, abra un dominio y, a continuación, seleccione un agente.

   Nota

   Solo un agente a la vez puede realizar la restauración de spyware/grayware.

3. Haga clic en **Tareas** > **Restaurar spyware y grayware**.
4. Para ver los elementos que se restaurarán de cada segmento de datos, haga clic en **Ver**.

   Se abrirá una nueva pantalla. Haga clic en **Atrás** para volver a la pantalla anterior.
5. Seleccione los segmentos de datos que desea restaurar.
6. Haga clic en **Restaurar**.

   OfficeScan le notificará el estado de la restauración. Revise los registros de restauración de spyware y grayware si desea consultar un informe completo. Consulte *Visualización de los registros de restauración de spyware y grayware en la página 7-111* para obtener más información.

Lista de programas de confianza

Puede configurar OfficeScan de manera que omita la exploración de procesos de confianza durante las exploraciones en tiempo real y de supervisión de comportamiento. Tras agregar un programa a la lista de programas de confianza, OfficeScan no realizará una exploración en tiempo real en el programa ni en los programas que este ha iniciado. Agregue programas de confianza a la lista de programas de confianza para mejorar el rendimiento de la exploración en los endpoints.

Nota

Puede agregar archivos a la lista de programas de confianza si se cumplen los siguientes requisitos:

- El archivo no está ubicado en el directorio del sistema de Windows.
- El archivo tiene una firma digital válida.

Tras agregar un programa a la lista de programas de confianza, OfficeScan excluye el programa de las siguientes exploraciones de forma automática:

- Comprobación de archivos de la exploración en tiempo real
- Supervisión del comportamiento
- Exploración de procesos de la exploración en tiempo real

Configuración de la lista de programas de confianza

La lista de programas de confianza excluye los programas y los procesos secundarios a los que llama el programa desde las exploraciones de exploración en tiempo real y la supervisión del comportamiento.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.

3. Haga clic en **Configuración** > **Lista de programas de confianza**.
4. Escriba la ruta completa del programa que se excluirá de la lista.
5. Haga clic en **Agregar a la lista de programas de confianza**.
6. Para eliminar un programa de la lista, haga clic en el icono **Eliminar**.
7. Para exportar la lista de programas de confianza, haga clic en **Exportar** y seleccione una ubicación para el archivo.

   Nota

   OfficeScan guardará la lista con el formato `DAT`.

8. Para importar una lista de programas de confianza, haga clic en **Importar** y seleccione una ubicación para el archivo.

   a. Haga clic en **Examinar...** y seleccione la ubicación del archivo `DAT`.

   b. Haga clic en **Importar**.

9. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Derechos y otras configuraciones de la exploración

Los usuarios con derechos de exploración tienen mayor control sobre la forma de exploración de los archivos en sus equipos. Los derechos de exploración permiten a los usuarios o al Agente de OfficeScan llevar a cabo las siguientes tareas:

- Los usuarios pueden definir la configuración de la exploración manual, la exploración programada y la exploración en tiempo real. Para conocer más detalles, consulte *Derechos de tipo de exploración en la página 7-59*.
- Los usuarios pueden posponer, detener u omitir la exploración programada. Para conocer más detalles, consulte *Derechos y otras configuraciones de la exploración programada en la página 7-62*.
- Los usuarios activan la exploración de los mensajes de correo electrónico POP3 en busca de virus o malware. Para conocer más detalles, consulte *Derechos y otras configuraciones de la exploración del correo en la página 7-68*.
- El Agente de OfficeScan puede utilizar la configuración de la caché para mejorar el rendimiento de la exploración. Para conocer más detalles, consulte *Configuración de la caché para las exploraciones en la página 7-70*.
- Los usuarios pueden personalizar una lista de programas de confianza individual. Para conocer más detalles, consulte *Derechos de lista de programas de confianza en la página 7-74*.

Derechos de tipo de exploración

Permite a los clientes configurar su propia configuración de Exploración manual, Exploración en tiempo real y Exploración programada.

Concesión de derechos de tipo de exploración

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Privilegios**, vaya a la sección **Exploraciones**.
5. Seleccione los tipos de exploración que los usuarios tienen permiso para configurar.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Definir la configuración de la exploración para el agente de OfficeScan

Procedimiento

1. Haga clic con el botón derecho del ratón en el icono del Agente de OfficeScan de la bandeja del sistema y seleccione **Abrir la consola del agente de OfficeScan**.
2. Haga clic en **Configuración** > **{tipo de exploración}**.

FIGURA 7-1. Configuración de la exploración en la consola del Agente de OfficeScan

3. Defina los siguientes valores de configuración:

   - Configuración de la exploración en tiempo real: Actividad del usuario en los archivos, Archivos para explorar, Configuración de la exploración, Exclusiones de la exploración y Acciones de exploración.
   - Configuración de la exploración manual: Archivos para explorar, Configuración de la exploración, Uso de la CPU, Exclusiones de la exploración y Acciones de exploración.

- Configuración de la exploración programada: Programa, Archivos para explorar, Configuración de la exploración, Uso de la CPU, Exclusiones de la exploración y Acciones de exploración.

4. Haga clic en **Aceptar**.

Derechos y otras configuraciones de la exploración programada

Si la exploración programada se ha establecido para que se ejecute en el agente, los usuarios pueden posponer, omitir o detener la exploración programada.

Posponer la exploración programada

Los usuarios con el derecho "Posponer la exploración programada" pueden llevar a cabo las siguientes acciones:

- Posponer la exploración programada antes de que se ejecute y especificar la duración del aplazamiento. La exploración programada solo puede posponerse una vez.
- En caso de que la Exploración programada esté en curso, los usuarios pueden detener la exploración y reiniciarla más tarde. Los usuarios pueden especificar el tiempo que debe transcurrir para que se reinicie la exploración. Cuando se reinicie la exploración, se volverán a explorar todos los archivos anteriormente explorados. Puede detener la exploración programada y reiniciarla solo una vez.

Nota

La duración del aplazamiento y el tiempo transcurrido que los usuarios pueden especificar como mínimo es de 15 minutos. El máximo es 12 horas y 45 minutos.

Para modificar el período de aplazamiento, vaya a **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad**. En la sección **Configuración de la exploración programada**, modifique la opción **Posponer la exploración programada hasta __ horas y __ minutos**.

Omitir y detener la exploración programada

Este derecho permite a los usuarios llevar a cabo las opciones siguientes:

- Omitir la exploración programada antes de que se ejecute
- Detener la exploración programada si está en curso

Nota

Los usuarios no pueden omitir o detener una exploración programada más de una vez. Incluso tras reiniciar el sistema, la exploración programada continuará la exploración en función de la siguiente hora programada.

Notificación de derechos de exploración programada

Para que los usuarios puedan beneficiarse de los derechos de exploración programada, recuérdeles los derechos que les ha concedido mediante la configuración de OfficeScan para que muestre un mensaje de notificación antes de ejecutar la exploración programada.

Concesión de derechos de exploración programada y visualización de la notificación de los derechos

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Exploraciones programadas**.
5. Seleccione las siguientes opciones:
   - **Posponer la exploración programada**

- **Omitir y detener la exploración programada**

6. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Configuración de la exploración programada**.

7. Seleccione **Mostrar una notificación antes de que se produzca una exploración programada**

   Al activar esta opción, aparece un mensaje de notificación en el endpoint del agente minutos antes de que se ejecute la exploración programada. Los usuarios reciben la notificación de la exploración programada (fecha y hora) y sus derechos de exploración programada, tales como posponer, omitir o detener la exploración.

   Nota

   Puede configurar el número de minutos. Para configurar la cantidad de minutos, vaya a **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad**. En la sección **Configuración de la exploración programada**, modifique el parámetro de configuración **Recordar a los usuarios la exploración programada __ minutos antes de que se ejecute**.

8. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Aplazamiento/omisión e interrupción de la Exploración programada en el agente

Procedimiento

- Si no ha comenzado la exploración programada:

  a. Haga clic con el botón derecho en el icono del Agente de OfficeScan situado en la bandeja del sistema y seleccione **Configuración de la exploración programada avanzada**.

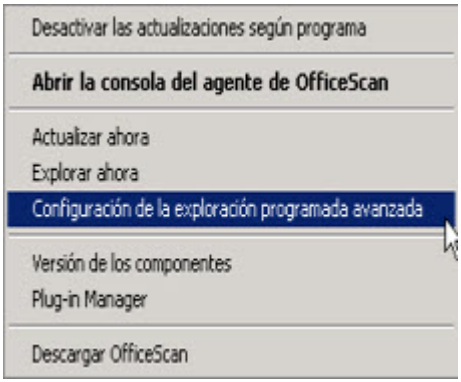


FIGURA 7-2. Opción Configuración avanzada de la exploración programada

Nota

Los usuarios no tienen que aplicar este paso si se activa el mensaje de notificación y se configura para que aparezcan minutos antes de que se ejecute la Exploración programada. Para obtener información detallada acerca del mensaje de notificación, consulte *Notificación de derechos de exploración programada en la página 7-63*.

  b. En la ventana de notificación que aparece, seleccione alguna de las opciones siguientes:

  - **Posponer la exploración __ horas y __ minutos.**

- **Omitir esta exploración programada. La siguiente exploración programada se ejecuta el <fecha> a las <hora>.**

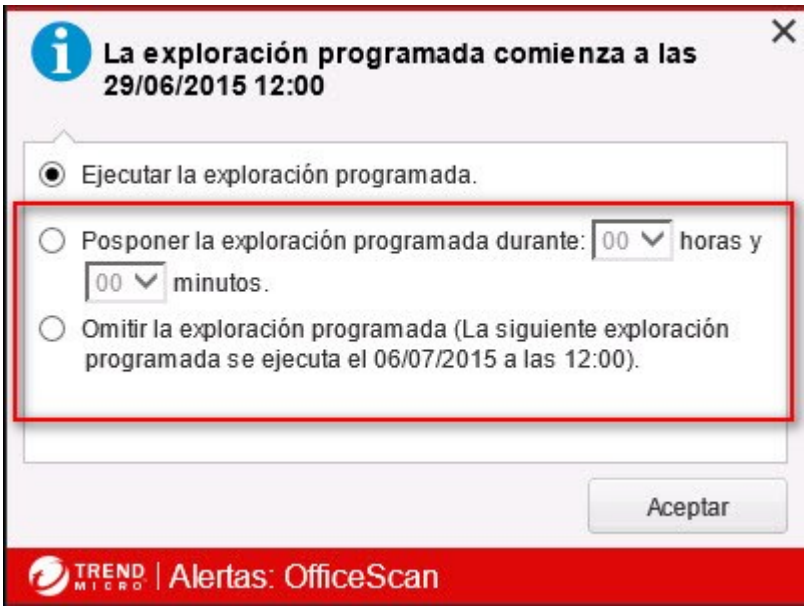


FIGURA 7-3. Derechos de exploración programada en el endpoint del Agente de OfficeScan

- Si la exploración programada está en curso:

  a. Haga clic con el botón derecho en el icono del Agente de OfficeScan situado en la bandeja del sistema y seleccione **Configuración avanzada de la exploración programada**.

  b. En la ventana de notificación que aparece, seleccione alguna de las opciones siguientes:

  - **Detener la exploración. Reiniciar la exploración tras __ horas y __ minutos.**
  - **Detener la exploración. La siguiente exploración programada se ejecuta el <fecha> a las <hora>.**

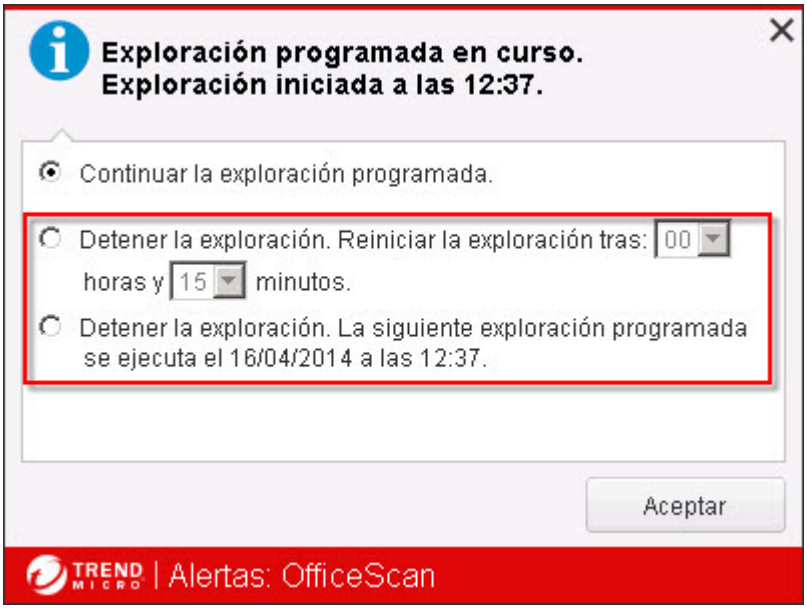


FIGURA 7-4. Derechos de exploración programada en el endpoint del Agente de OfficeScan

Derechos y otras configuraciones de la exploración del correo

Si los agentes disponen de los derechos de exploración del correo, la opción **Exploración de correo** se visualizará en la consola del Agente de OfficeScan. La opción **Exploración del correo** muestra la exploración de correo POP3.

FIGURA 7-5. Configuración de la exploración de correo en la consola del Agente de OfficeScan

La siguiente tabla describe el programa de exploración del correo POP3.

TABLA 7-18. Programas de exploración de correo

DETALLES	DESCRIPCIÓN
Objetivo	Explora los mensajes de correo electrónico de POP3 en busca de virus y malware.
Requisitos previos	• Los administradores deben habilitarlo desde la consola Web para que los usuarios puedan utilizarlo **Nota** Para habilitar POP3 Mail Scan, consulte *Concesión de derechos de exploración de correo y habilitación de la exploración del correo POP3 en la página 7-69*. • Acción frente a los virus y el malware configurable desde la consola del Agente de OfficeScan, pero no desde la consola Web.
Tipos de exploración compatibles	Exploración en tiempo real La exploración se realiza a medida que se recuperan los mensajes de correo electrónico del servidor de correo POP3.
Resultados de la exploración	• Información sobre los riesgos de seguridad detectados disponible tras la finalización de la exploración • Resultados de la exploración no registrados en la pantalla **Registros** de la consola del Agente de OfficeScan. • Resultados de la exploración no enviados al servidor
Otros detalles	Comparte el servicio proxy de OfficeScan NT (`TMProxy.exe`) con la función de reputación Web

Concesión de derechos de exploración de correo y habilitación de la exploración del correo POP3

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Exploración del correo**.
5. Seleccione **Mostrar la configuración de la exploración del correo en la consola del agente de OfficeScan**.
6. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Configuración de la exploración del correo electrónico POP3**.
7. Seleccione **Explorar el correo POP3**.
8. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración de la caché para las exploraciones

El Agente de OfficeScan puede generar los archivos de caché de la firma digital y de la exploración bajo petición para mejorar el rendimiento de su exploración. Cuando se ejecuta una exploración a petición, el Agente de OfficeScan comprueba en primer lugar el archivo de caché de la firma digital y, a continuación, el archivo de caché de la exploración bajo petición en busca de archivos que se deban excluir de la exploración. La duración de la exploración se reduce si se excluye un gran numero de archivos.

Caché de la firma digital

El archivo de caché de la firma digital se utiliza durante los procesos Exploración manual, Exploración programada y Explorar ahora. Los agentes no exploran los archivos cuyas firmas se hayan agregado al archivo de caché de la firma digital.

El Agente de OfficeScan utiliza el mismo patrón de firma digital utilizado en la función de la supervisión del comportamiento para generar el archivo de caché de la firma digital. Digital Signature Pattern contiene una lista de archivos que Trend Micro considera fiables y, por lo tanto, que se pueden excluir de las exploraciones.

Nota

La función Supervisión del comportamiento se desactiva de forma automática en las plataformas de servidor de Windows (la compatibilidad con las versiones de 64 bits para Windows XP, 2003 y Vista sin SP1 no se encuentra disponible). Si se activa la caché de la firma digital, los Agentes de OfficeScan de estas plataformas descargarán el patrón de firma digital para utilizarlo en la caché, y no descargarán el resto de componentes de la supervisión del comportamiento.

Los agentes generan el archivo de caché de la firma digital de acuerdo a un programa, que se puede configurar en la consola Web. Los agentes lo hacen para:

- Agregar las firmas de nuevos archivos que se han introducido en el sistema desde que se generó el último archivo de caché.
- Eliminar las firmas de los archivos que se han modificado o eliminado del sistema.

Durante el proceso de generación de la caché, los agentes comprueban las siguientes carpetas en busca de archivos fiables y, a continuación, agregan las firmas de estos archivos al archivo de caché de la firma digital:

- `%PROGRAMFILES%`
- `%WINDIR%`

El proceso de generación de la caché no afecta al rendimiento del endpoint, ya que los agentes utilizan una cantidad mínima de recursos del sistema durante el proceso. Los agentes también pueden reanudar una tarea de generación de caché que se haya

interrumpido por alguna razón (por ejemplo, cuando el equipo host está apagado o cuando el adaptador de CA de un endpoint inalámbrico está desenchufado).

Caché de la exploración bajo petición

El archivo de caché de la exploración bajo petición se utiliza durante los procesos de Exploración manual, Exploración programada y Explorar ahora. Los Agentes de OfficeScan no exploran los archivos cuyas cachés se hayan agregado al archivo de caché de la exploración bajo petición.

Cada vez que se ejecuta una exploración, el Agente de OfficeScan comprueba las propiedades de los archivos libres de amenazas. Si un archivo libre de amenazas no se ha modificado durante un periodo de tiempo determinado (que se puede configurar), el Agente de OfficeScan agrega la caché del archivo al archivo de caché de la exploración bajo petición. Cuando se produce la siguiente exploración, el archivo no se explora a menos que haya caducado su caché.

La caché de un archivo libre de amenazas caduca una vez transcurrido un número de días concreto (que también se puede configurar). Cuando la exploración se realiza durante o después de la fecha de caducidad de la caché, el Agente de OfficeScan elimina la caché caducada y explora el archivo en busca de amenazas. Si el archivo está libre de amenazas y sigue sin presentar modificaciones, la caché del archivo se vuelve a agregar al archivo de caché de la exploración a petición. Si el archivo está libre de amenazas, pero se ha modificado recientemente, la caché no se agrega y el archivo se incluye en la siguiente exploración que se realice.

La caché de un archivo libre de amenazas caduca con el fin de prevenir la exclusión de archivos infectados de las exploraciones, como se ilustra en los siguientes ejemplos:

- Es posible que un archivo de patrones muy desactualizado haya considerado un archivo infectado y no modificado como libre de amenazas. Si la caché no caduca, el archivo infectado permanece en el sistema hasta que se modifique y lo detecte una exploración en tiempo real.
- Si un archivo de caché se ha modificado y la exploración en tiempo real no se encuentra operativa durante la modificación, la caché ha de caducar para que dicho archivo se explore en busca de amenazas.

El número de cachés agregadas al archivo de caché de la exploración a petición depende del tipo y el objetivo de la exploración. Por ejemplo, el número de cachés puede ser

menor si el Agente de OfficeScan explora solo 200 de los 1000 archivos de un endpoint durante la exploración manual.

Si se realizan exploraciones a petición con frecuencia, el archivo de caché de este tipo de exploración reduce la duración de la exploración significativamente. En una tarea de exploración en la que ninguna de las cachés haya caducado, una exploración que normalmente tarda 12 minutos se puede reducir a 1 minuto. Normalmente, reducir el número de días que un archivo debe permanecer sin modificar y ampliar la caducidad de la caché mejoran el rendimiento. Ya que los archivos deben permanecer sin modificar durante un periodo de tiempo relativamente corto, se pueden agregar más cachés al archivo de caché. El periodo de caducidad de las cachés también es más largo, por lo que son más los archivos que se omiten en la exploración.

Si rara vez ejecuta exploraciones a petición, puede desactivar la caché de la exploración a petición, ya que caducaría antes de que la siguiente exploración se ejecute.

Configuración de la caché para las exploraciones

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Configuración de la caché para las exploraciones**.
5. Configure la caché de la firma digital.
   a. Seleccione **Activar caché de la firma digital**.
   b. En **Generar la caché cada __ días**, especifique la frecuencia con la que el agente genera la caché.
6. Configure la caché para la exploración a petición.
   a. Seleccione **Activar caché de la exploración bajo petición**.

b. En **Agregar caché para guardar los archivos que no han sufrido cambios durante __ días**, especifique el número de días que un archivo debe permanecer sin modificaciones para que se incluya en la caché.

c. En **La caché de cada archivo seguro caduca en __ días**, especifique el número de días máximo que una caché permanece en el archivo de caché.

> **Nota**
>
> Para evitar que todas las cachés agregadas durante una exploración caduquen el mismo día, las expiraciones se producen de forma aleatoria dentro del número de días máximo especificado. Por ejemplo, si se han agregado 500 cachés a la caché hoy y el número máximo de días especificado es 10, una parte de las cachés caducará al día siguiente y la mayoría de ellas en los días posteriores. Al décimo día, caducarán todas las cachés restantes.

7. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Derechos de lista de programas de confianza

Puede otorgar el derecho de configurar OfficeScan a los usuarios finales, de manera que omita la exploración de procesos de confianza durante las exploraciones en tiempo real y de supervisión de comportamiento. Tras agregar un programa a la lista de programas de confianza, OfficeScan no realizará una exploración en tiempo real en el programa ni en los programas que este ha iniciado. Agregue programas de confianza a la lista de programas de confianza para mejorar el rendimiento de la exploración en los endpoints.

Asignación de la configuración de la lista de programas de confianza

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Lista de programas de confianza**.
5. Seleccione **Mostrar la lista de programas de confianza en la consola del agente de OfficeScan**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración general de la exploración

La configuración general de la exploración se aplica a los agentes de varias formas.

- Una configuración concreta de la exploración se puede aplicar a todos los agentes que administra el servidor o solo a los agentes que tengan ciertos derechos de exploración. Por ejemplo, si define la duración de la Exploración programada

pospuesta, solo los agentes con derecho a posponer la exploración programada utilizarán la configuración.

- Una configuración de exploración determinada se puede aplicar a todos los tipos de exploración o sólo a uno en concreto. Por ejemplo, en los endpoints que tienen instalados el servidor de OfficeScan y el Agente de OfficeScan, puede excluir de la exploración la base de datos del servidor de OfficeScan. Sin embargo, esta configuración se aplica sólo durante la exploración en tiempo real.
- Una configuración de la exploración determinada se puede aplicar a la exploración de viruso malware, de spyware o grayware, o a ambas. Por ejemplo, el modo de valoración sólo se aplica durante la exploración de spyware o grayware.

Configuración general de la exploración

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Configuración de seguridad** y defina la configuración general de la exploración en cada una de las secciones disponibles.
   - *Sección Configuración de la exploración en la página 7-78*
   - *Sección Configuración de la exploración programada en la página 7-84*
3. Haga clic en la pestaña **Sistema**.
4. En la sección **Configuración del servicio de software seguro certificado**, configure el ajuste **Activar el servicio de software seguro certificado para la supervisión de comportamiento, el cortafuegos y las exploraciones antivirus**.

   El servicio de software seguro certificado realiza consultas a los centros de datos de Trend Micro para comprobar la seguridad de un programa detectado por el bloqueador de comportamientos malintencionados, la supervisión de eventos, el cortafuegos o las exploraciones antivirus. Active el Servicio de software seguro certificado para reducir la probabilidad de detecciones de falsos positivos.

Nota

Asegúrese de que los Agentes de OfficeScan tengan la configuración del proxy correcta (para obtener más información, consulte *Configuración del proxy del agente de OfficeScan en la página 15-54*) antes de activar el servicio de software seguro certificado. Una configuración incorrecta del proxy, junto con una conexión intermitente a Internet, puede acarrear atrasos o fallos en la respuesta de los centros de datos de Trend Micro, lo que puede hacer que los programas que se supervisen no respondan.

Además, los Agentes de OfficeScan que solo utilizan IPv6 no podrán realizar consultas directas a los centros de datos de Trend Micro. Con el fin de permitir que los Agentes de OfficeScan se conecten a los centros de datos de Trend Micro, se necesita un servidor proxy de doble pila que pueda convertir direcciones IP, como puede ser DeleGate.

5. Haga clic en la pestaña **Red**.

6. En la sección **Configuración del ancho de banda del registro de virus/malware**, configure el ajuste **Activar el agente de OfficeScan para que cree una entrada de registro de virus/malware única para las detecciones reincidentes del mismo virus/malware al cabo de una hora**.

   OfficeScan consolida las entradas de los registros de virus cuando detecta varias infecciones del mismo virus/malware durante un breve periodo de tiempo. OfficeScan detecta el mismo virus/malware varias veces, se llena el registro de virus/malware en poco tiempo y se consume ancho de banda de la red cada vez que el Agente de OfficeScan envía la información del registro al servidor. Si se activa esta función, se reducirá tanto el número de entradas del registro de virus/malware como la cantidad de ancho de banda de la red consumido por los Agentes de OfficeScan cuando envían la información del registro de virus al servidor.

7. Haga clic en la pestaña **Control de agentes**.

8. En la sección **Configuración general**, configure el ajuste **Agregar la exploración manual al menú de acceso directo de Windows en los endpoints**.

   Cuando esta configuración está activada, todos los Agentes de OfficeScan gestionados por el servidor agregan la opción **Explorar con OfficeScan** al menú del Explorador de Windows que se activa al hacer clic con el botón derecho. Cuando los usuarios hacen clic con el botón derecho en un archivo o carpeta en el escritorio de Windows o en el Explorador de Windows y seleccionan esta opción,

la exploración manual explora el archivo o la carpeta para comprobar si existen virus, malware, spyware y grayware.

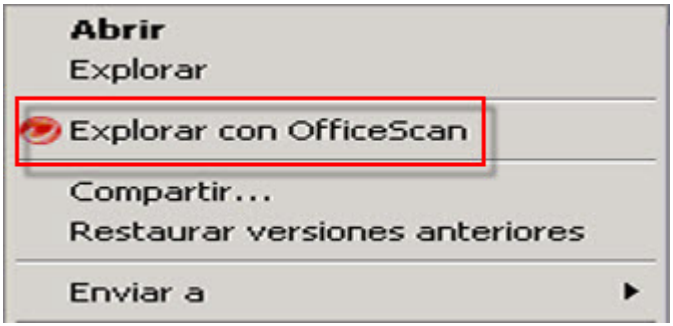


FIGURA 7-6. Opción Explorar con OfficeScan

9. Haga clic en **Guardar**.

Sección Configuración de la exploración

La sección **Configuración de la exploración** de la pestaña **Configuración de seguridad** en la pantalla **Configuración global para los agentes** permite a los administradores configurar lo siguiente:

- *Excluir la carpeta de la base de datos del servidor de OfficeScan de la exploración en tiempo real en la página 7-79*
- *Excluir los archivos y las carpetas del servidor de Microsoft Exchange de las exploraciones en la página 7-79*
- *Activar la exploración retardada en operaciones de archivos en la página 7-80*
- *Activar la protección antimalware de inicio temprano en los endpoints en la página 7-80*
- *Limpiar y eliminar archivos infectados dentro de archivos comprimidos en la página 7-80*
- *Activar el modo de valoración en la página 7-83*
- *Buscar cookies en la página 7-84*

Excluir la carpeta de la base de datos del servidor de OfficeScan de la exploración en tiempo real

En caso de que el Agente de OfficeScan y el servidor de OfficeScan se encuentren en el mismo endpoint, el Agente de OfficeScan no explorará la base de datos del servidor en busca de virus/malware y spyware/grayware durante la exploración en tiempo real.

Consejo

Active esta configuración para impedir que la base de datos sufra los daños que pueden provocarse durante la exploración.

Excluir los archivos y las carpetas del servidor de Microsoft Exchange de las exploraciones

En caso de que el Agente de OfficeScan y un servidor de Microsoft Exchange 2000 o 2003 se encuentren en el mismo endpoint, OfficeScan no explorará las siguientes carpetas y los siguientes archivos del servidor de Microsoft Exchange para comprobar si hay virus/malware o spyware/grayware durante los procesos de Exploración manual, Exploración en tiempo real, Exploración programada y Explorar ahora:

- Las siguientes carpetas ubicadas en `\Exchsrvr\Mailroot\vsi 1`: `Queue`, `PickUp` y `BadMail`.
- `.\Exchsrvr\mdbdata`, incluidos estos archivos: `priv1.stm`, `priv1.edb`, `pub1.stm` y `pub1.edb`.
- `.\Exchsrvr\Storage Group`

En Microsoft Exchange 2007 o versiones posteriores, es necesario añadir manualmente las carpetas a la lista de exclusión de la exploración. Para consultar información detallada sobre las exclusiones de la exploración, consulte el siguiente sitio Web:

http://technet.microsoft.com/en-us/library/bb332342.aspx

Consulte *Exclusiones de la exploración en la página 7-33* para conocer los pasos que hay que seguir a la hora de configurar la lista de exclusión de la exploración.

Activar la exploración retardada en operaciones de archivos

Los administradores pueden configurar OfficeScan para retardar la exploración de archivos. OfficeScan permite al usuario copiar archivos y, a continuación, explora los archivos una vez que ha finalizado el proceso de copia. Esta exploración retardada mejora el rendimiento de los procesos de copia y exploración.

Nota

La exploración retardada requiere que el motor de exploración antivirus (VSAPI) sea la versión 9.713 o posterior. Para obtener más información sobre la actualización de este servidor, consulte *Actualizar el servidor de OfficeScan de forma manual en la página 6-27*

Activar la protección antimalware de inicio temprano en los endpoints

OfficeScan es compatible con la característica Antimalware de inicio temprano (ELAM, por sus siglas en inglés) como parte del estándar de arranque seguro con el fin de proporcionar protección durante el tiempo de arranque en los endpoints. Cuando se inicien los endpoints, los administradores pueden activar esta característica para iniciar los agentes de OfficeScan antes que los controladores de software de terceros. Esta característica permite a los agentes de OfficeScan detectar malware durante el proceso de arranque del sistema operativo.

Después de explorar todos los controladores de software de terceros, el agente de OfficeScan notifica la información de clasificación de los controladores al kernel del sistema. Los administradores podrán definir acciones basadas en las clasificaciones en la política de grupo en Windows y ver los resultados de la exploración a través del Visualizador de sucesos de los endpoints.

Nota

ELAM es compatible solo con Windows 8, Windows Server 2012 o versiones posteriores.

Limpiar y eliminar archivos infectados dentro de archivos comprimidos

Cuando todos los agentes gestionados por el servidor detectan virus/malware en archivos comprimidos durante los procesos Exploración manual, Exploración en tiempo

real, Exploración programada y Explorar ahora y, además, se cumplen las siguientes condiciones, los agentes limpian o eliminan los archivos infectados.

- "Limpiar" o "Eliminar" es la acción definida para OfficeScan. Compruebe la acción que OfficeScan lleva a cabo en los archivos infectados en **Agentes** > **Administración de agentes > Configuración** > **Configuración de la exploración** > **{Tipo de exploración} pestaña** > **Acción**.
- Puede activar esta configuración. Al activar esta configuración, puede aumentar el uso de los recursos del endpoint durante la exploración y, además, la exploración puede tardar más tiempo en completarse. Esto se debe a que OfficeScan tiene que descomprimir el archivo, limpiar o eliminar los archivos infectados que se encuentran en el archivo comprimido y, a continuación, volver a comprimir el archivo.
- El formato de archivo comprimido es compatible. OfficeScan solo admite ciertos formatos de archivo comprimido, incluidos ZIP y Office Open XML, que utiliza las tecnologías de compresión ZIP. Office Open XML es el formato predeterminado para las aplicaciones de Microsoft Office 2007 tales como Excel, PowerPoint y Word.

Nota

póngase en contacto con su proveedor de asistencia para obtener una lista completa de formatos de archivo comprimidos.

Por ejemplo, la exploración en tiempo real está definida para que elimine los archivos infectados por virus. Después de que la exploración en tiempo real descomprime un archivo comprimido denominado `abc.zip` y detecta un archivo infectado llamado `123.doc` dentro del archivo comprimido, OfficeScan elimina `123.doc` y, a continuación, vuelve a comprimir `abc.zip`, al que ahora se puede acceder con seguridad.

En la siguiente tabla se describe lo que sucede si no se cumple ninguna de las condiciones.

TABLA 7-19. Situaciones y resultados de los archivos comprimidos

ESTADO DE "LIMPIAR/ ELIMINAR ARCHIVOS INFECTADOS DENTRO DE ARCHIVOS COMPRIMIDOS"	ACCIÓN QUE DEBE REALIZAR OFFICESCAN	FORMATO DE ARCHIVO COMPRIMIDO	RESULTADO
Activada	Limpiar o eliminar	Incompatible Ejemplo: `def.rar` contiene el archivo infectado `123.doc`.	OfficeScan cifra `def.rar` pero no lo limpia, elimina ni realiza ninguna otra acción en `123.doc`.
Desactivado	Limpiar o eliminar	Compatible/No compatible Ejemplo: `abc.zip` contiene el archivo infectado `123.doc`.	OfficeScan no limpia, elimina ni realiza ninguna otra acción sobre `abc.zip` y `123.doc`.

ESTADO DE "LIMPIAR/ ELIMINAR ARCHIVOS INFECTADOS DENTRO DE ARCHIVOS COMPRIMIDOS"	ACCIÓN QUE DEBE REALIZAR OFFICESCAN	FORMATO DE ARCHIVO COMPRIMIDO	RESULTADO
Activado/ Desactivado	Ni Limpiar ni Eliminar (en otras palabras, cualquiera de las siguientes acciones: Cambiar nombre, Poner en cuarentena, Denegar acceso u Omitir)	Compatible/No compatible Ejemplo: `abc.zip` contiene el archivo infectado `123.doc`.	OfficeScan lleva a cabo la acción configurada (Cambiar nombre, Poner en cuarentena, Denegar acceso u Omitir) en `abc.zip`, no en `123.doc`. Si la acción es: **Cambiar nombre**: OfficeScan cambia el nombre de `abc.zip` a `abc.vir`, pero no cambia el nombre de `123.doc`. **Poner en cuarentena**: OfficeScan pone en cuarentena `abc.zip` (`123.doc` y todos los archivos no infectados se ponen en cuarentena). **Omitir**: OfficeScan no realiza ninguna acción en `abc.zip` ni `123.doc`, pero registra la detección del virus. **Denegar acceso**: OfficeScan deniega el acceso a `abc.zip` cuando se abre (no se puede abrir `123.doc` ni ningún archivo no infectado).

Activar el modo de valoración

Cuando está activado el modo de valoración, todos los agentes gestionados por el servidor registrarán el spyware/grayware detectado durante los procesos Exploración

manual, Exploración programada, Exploración en tiempo real y Explorar ahora, pero no limpiará los componentes de spyware y grayware. La limpieza finaliza los procesos o elimina los registros, los archivos, las cookies y los accesos directos.

Trend Micro ofrece un modo de valoración que le permite evaluar los elementos que Trend Micro detecta como spyware y grayware y emprender entonces las acciones pertinentes. Por ejemplo, el spyware/grayware detectado que no considere un riesgo de seguridad se puede añadir a la lista de spyware/grayware permitido.

Cuando este modo se encuentra activado, OfficeScan lleva a cabo las siguientes acciones de exploración:

- **Omitir**: durante los procesos Exploración manual, Exploración programada y Explorar ahora.
- **Denegar acceso**: durante el proceso Exploración en tiempo real.

Nota

El modo de valoración anula cualquier acción de exploración definida por el usuario. Por ejemplo, incluso si selecciona "Limpiar" como la acción de exploración para la exploración manual, "Omitir" seguirá siendo la acción de exploración cuando el agente esté en el modo de valoración.

Buscar cookies

Seleccione esta opción si considera las cookies como posibles riesgos de seguridad. Cuando esté seleccionada, todos los agentes que el servidor gestiona explorarán las cookies para comprobar si contienen spyware/grayware durante los procesos Exploración manual, Exploración programada, Exploración en tiempo real y Explorar ahora.

Sección Configuración de la exploración programada

Solo los agentes configurados para ejecutar la exploración programada podrán usar los siguientes valores de configuración. La Exploración programada puede buscar virus, malware, spyware y grayware.

La sección Configuración de la exploración programada de la Configuración general de la exploración permite a los administradores configurar lo siguiente:

- *Recordar a los usuarios la Exploración programada __ minutos antes de que se ejecute en la página 7-85*
- *Posponer la exploración programada hasta __ horas y __ minutos en la página 7-85*
- *Detener la exploración programada automáticamente si la exploración dura más de __ horas y __ minutos en la página 7-86*
- *Omitir la exploración programada si la duración de la batería del endpoint inalámbrico es inferior al __ % y el adaptador de CA está desenchufado en la página 7-86*
- *Reanudar Escaneos programados omitidos en la página 7-86*

Recordar a los usuarios la Exploración programada __ minutos antes de que se ejecute

OfficeScan muestra un mensaje de notificación minutos antes de que se inicie la exploración para recordar a los usuarios la fecha y hora a la que se realizará la exploración programada y cualquier derecho que les haya concedido.

Puede activar o desactivar el mensaje de notificación en **Agentes** > **Administración de agentes > Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones (pestaña)** > **Configuración de la exploración programada**. En caso de que esté desactivada esta opción, no aparecerá ningún recordatorio.

Posponer la exploración programada hasta __ horas y __ minutos

Solo los usuarios con el derecho "Posponer la exploración programada" pueden llevar a cabo las siguientes acciones:

- Posponer la exploración programada antes de que se ejecute y especificar la duración del aplazamiento.
- En caso de que la Exploración programada esté en curso, los usuarios pueden detener la exploración y reiniciarla más tarde. Los usuarios pueden especificar el tiempo que debe transcurrir para que se reinicie la exploración. Cuando se reinicie la exploración, se volverán a explorar todos los archivos anteriormente explorados.

La duración del aplazamiento/el tiempo transcurrido máximos que los usuarios pueden especificar es de 12 horas y 45 minutos, periodo que pueden reducir especificando el número de hora(s) y/o minuto(s) en los campos indicados.

Detener la exploración programada automáticamente si la exploración dura más de __ horas y __ minutos

OfficeScan detiene la exploración cuando se supera el tiempo especificado y aún no ha finalizado la exploración. OfficeScan notifica inmediatamente a los usuarios de cualquier riesgo de seguridad detectado durante la exploración.

Omitir la exploración programada si la duración de la batería del endpoint inalámbrico es inferior al __ % y el adaptador de CA está desenchufado

OfficeScan omite la exploración tan pronto como se ejecuta la exploración programada si detecta que el endpoint inalámbrico tiene poca batería y el adaptador de CA no está conectado a ninguna fuente de alimentación. Si queda poca batería pero el adaptador de CA está conectado a una fuente de alimentación, la exploración continuará.

Reanudar Escaneos programados omitidos

Si la exploración programada no se ha iniciado debido a que OfficeScan no se ha ejecutado en el día y la hora programados o si el usuario la interrumpe (p. ej. el usuario desactiva el endpoint después de que la exploración se inicia), puede especificar cuándo desea que OfficeScan la reanude.

Especifique la exploración programada que se debe reiniciar:

- **Reanudar una exploración programada interrumpida**: reanuda las exploraciones programadas que los usuarios han interrumpido al apagar el endpoint.
- **Reanudar una exploración programada omitida**: reanuda las exploraciones programadas que se han omitido debido a que el endpoint no se estaba ejecutando.

Especifique cuándo reanudar la exploración:

- **A la misma hora el día siguiente**: si OfficeScan se ejecuta a la misma hora del siguiente día, la exploración se reanuda.
- **__ minutos tras el inicio del endpoint**: OfficeScan reanuda la exploración tras una cantidad de minutos determinada después de que el usuario enciende el endpoint. El número de minutos está comprendido entre 10 y 120.

Nota

Los usuarios pueden posponer u omitir una exploración reanudada si el administrador ha activado este derecho. Para conocer más detalles, consulte *Derechos y otras configuraciones de la exploración programada en la página 7-62*.

Notificaciones de riesgos de seguridad

OfficeScan incluye un conjunto de mensajes de notificación predeterminados para informarle a usted, a otros administradores de OfficeScan y a los usuarios del Agente de OfficeScan acerca de los riesgos de seguridad que se han detectado.

Para obtener más información sobre las notificaciones que se envían a los administradores, consulte *Notificaciones de riesgos de seguridad para los administradores en la página 7-87*.

Para obtener más información sobre las notificaciones que se envían a los usuarios del Agente de OfficeScan, consulte *Notificaciones de riesgos de seguridad para los usuarios del agente de OfficeScan en la página 7-94*.

Notificaciones de riesgos de seguridad para los administradores

Configure OfficeScan para que le envíe a usted y a otros administradores de OfficeScan una notificación cuando detecte un riesgo de seguridad, o únicamente cuando la acción realizada para hacer frente al riesgo de seguridad no haya tenido éxito y, por lo tanto, se requiera la intervención del administrador.

OfficeScan incluye un conjunto de mensajes de notificación predeterminados para informarle a usted y a los administradores de OfficeScan de las detecciones de riesgos de

seguridad. Puede modificar las notificaciones y definir la configuración de notificaciones adicionales según sus necesidades.

TABLA 7-20. Tipos de notificaciones de sobre los riesgos de seguridad

TIPO	REFERENCIA
Virus/Malware	*Configuración de las notificaciones de riesgos de seguridad para los administradores en la página 7-88*
Spyware/Grayware	*Configuración de las notificaciones de riesgos de seguridad para los administradores en la página 7-88*
Transmisiones de activos digitales	*Configurar las notificaciones de prevención de pérdida de datos para los administradores en la página 11-57*
Rellamadas de C&C	*Configuración de notificaciones de rellamadas de C&C para administradores en la página 12-16*

Nota

OfficeScan puede enviar notificaciones mediante correo electrónico, captura SNMP y registros de sucesos de Windows NT. Defina la configuración cuando OfficeScan envíe notificaciones mediante estos canales. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

Configuración de las notificaciones de riesgos de seguridad para los administradores

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Administrador**.
2. En la pestaña **Criterios**:
   a. Vaya a las secciones **Virus/Malware** y **Spyware/Grayware**.
   b. Especifique si las notificaciones se enviarán cuando OfficeScan detecte virus o malware y spyware o grayware o solo cuando la acción con estos riesgos de seguridad no se realice correctamente.

3. En la pestaña **Correo electrónico**:

   a. Vaya a las secciones **Detecciones de virus/malware** y **Detecciones de spyware/grayware**.

   b. Seleccione **Activar la notificación por correo electrónico**.

   c. Seleccione **Enviar notificaciones a los usuarios con permisos de dominio del árbol de agentes**.

   Puede utilizar Role-based Administration para conceder a los usuarios permisos de dominio del árbol de agentes. Si se produce una detección en un Agente de OfficeScan que pertenece a un dominio específico, el correo electrónico se enviará a las direcciones de correo electrónico de los usuarios con permisos de dominio. Consulte los ejemplos de la siguiente tabla:

TABLA 7-21. Dominios y permisos del árbol de agentes

DOMINIO DEL ÁRBOL DE AGENTES	FUNCIONES CON PERMISOS DE DOMINIO	CUENTA DE USUARIO CON LA FUNCIÓN	DIRECCIÓN DE CORREO ELECTRÓNICO PARA LA CUENTA DE USUARIO
Dominio A	Administrador (integrado)	raíz	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Dominio B	Administrador (integrado)	raíz	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un Agente de OfficeScan que pertenece al dominio A detecta un virus, el correo electrónico se enviará a mary@xyz.com, john@xyz.com y chris@xyz.com.

Si un Agente de OfficeScan que pertenece al dominio B detecta spyware, el correo electrónico se enviará a mary@xyz.com y jane@xyz.com.

Nota

Si activa esta opción, todos los usuarios con permisos de dominio deben tener una dirección de correo electrónico correspondiente. El correo electrónico de notificación no se enviará a los usuarios sin dirección de correo electrónico. Los usuarios y las direcciones de correo electrónico se configuran en **Administración** > **Administración de cuentas** > **Cuentas de usuario**.

d. Seleccione **Enviar notificaciones a la(s) siguiente(s) dirección(es) de correo electrónico** y, después, escriba las direcciones de correo electrónico.

e. Acepte o modifique el asunto y el mensaje predeterminados. Puede utilizar variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 7-22. Variables de símbolo para notificaciones de riesgos de seguridad

VARIABLE	DESCRIPCIÓN
Detecciones de virus/malware	
%v	Nombre del virus/malware
%s	Endpoint con virus/malware
%i	Dirección IP del endpoint
%c	Dirección MAC del endpoint
%m	El dominio del endpoint.
%p	Ubicación del virus/malware
%y	Fecha y hora de la detección del virus/malware
%e	Versión del Motor de Escaneo antivirus
%r	Versión del patrón de virus
%a	Acción realizada frente al riesgo de seguridad
%n	Nombre del usuario conectado al endpoint infectado
Detecciones de spyware/grayware	

Variable	Descripción
%s	Endpoint con spyware/grayware
%i	Dirección IP del endpoint
%m	El dominio del endpoint.
%y	Fecha y hora de la detección del spyware/grayware
%n	Nombre del usuario conectado al endpoint en el momento de la detección
%T	Spyware/Grayware y resultado de la exploración

4. En la pestaña **Captura SNMP**:

   a. Vaya a las secciones **Detecciones de virus/malware** y **Detecciones de spyware/grayware**.

   b. Seleccione **Activar la notificación por captura SNMP**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo en la siguiente tabla para representar los datos en el campo **Mensaje**.

Tabla 7-23. Variables de símbolo para notificaciones de riesgos de seguridad

Variable	Descripción
Detecciones de virus/malware	
%v	Nombre del virus/malware
%s	Endpoint con virus/malware
%i	Dirección IP del endpoint
%c	Dirección MAC del endpoint
%m	El dominio del endpoint.
%p	Ubicación del virus/malware
%y	Fecha y hora de la detección del virus/malware

Variable	Descripción
%e	Versión del Motor de Escaneo antivirus
%r	Versión del patrón de virus
%a	Acción realizada frente al riesgo de seguridad
%n	Nombre del usuario conectado al endpoint infectado
Detecciones de spyware/grayware	
%s	Endpoint con spyware/grayware
%i	Dirección IP del endpoint
%m	El dominio del endpoint.
%y	Fecha y hora de la detección del spyware/grayware
%n	Nombre del usuario conectado al endpoint en el momento de la detección
%T	Spyware/Grayware y resultado de la exploración
%v	Nombre del spyware/grayware
%a	Acción realizada frente al riesgo de seguridad

5. En la pestaña **Registro de sucesos de NT**:

   a. Vaya a las secciones **Detecciones de virus/malware** y **Detecciones de spyware/grayware**.

   b. Seleccione **Activar la notificación por el registro de sucesos de NT**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo en la siguiente tabla para representar los datos en el campo **Mensaje**.

Tabla 7-24. Variables de símbolo para notificaciones de riesgos de seguridad

Variable	Descripción
Detecciones de virus/malware	

Variable	Descripción
%v	Nombre del virus/malware
%s	Endpoint con virus/malware
%i	Dirección IP del endpoint
%c	Dirección MAC del endpoint
%m	El dominio del endpoint.
%p	Ubicación del virus/malware
%y	Fecha y hora de la detección del virus/malware
%e	Versión del Motor de Escaneo antivirus
%r	Versión del patrón de virus
%a	Acción realizada frente al riesgo de seguridad
%n	Nombre del usuario conectado al endpoint infectado
Detecciones de spyware/grayware	
%s	Endpoint con spyware/grayware
%i	Dirección IP del endpoint
%m	El dominio del endpoint.
%y	Fecha y hora de la detección del spyware/grayware
%n	Nombre del usuario conectado al endpoint en el momento de la detección
%T	Spyware/Grayware y resultado de la exploración
%v	Nombre del spyware/grayware
%a	Acción realizada frente al riesgo de seguridad

6. Haga clic en **Guardar**.

Notificaciones de riesgos de seguridad para los usuarios del agente de OfficeScan

OfficeScan puede mostrar mensajes de notificación en el endpoint del Agente de OfficeScan:

- Inmediatamente después de que la exploración en tiempo real y la exploración programada detecten virus/malware y spyware/grayware. Active el mensaje de notificación y modifique de forma opcional su contenido.
- Si es preciso reiniciar el endpoint del agente para finalizar la limpieza de archivos infectados. Para la exploración en tiempo real, el mensaje aparece después de haber explorado un riesgo de seguridad determinado. En el caso de que se utilicen las opciones de exploración manual, exploración programada y Explorar ahora, el mensaje aparece una vez y sólo después de que OfficeScan termina de explorar todos los destinos de exploración.

TABLA 7-25. Tipos de notificaciones del agente sobre los riesgos de seguridad

TIPO	REFERENCIA
Virus/Malware	*Configuración de las notificaciones de virus/malware en la página 7-96*
Spyware/Grayware	*Configuración de las notificaciones de spyware/grayware en la página 7-96*
Infracciones del cortafuegos	*Modificar el contenido del mensaje de notificación del cortafuegos en la página 13-30*
Infracciones de la reputación Web	*Modificar las notificaciones de amenazas Web en la página 12-15*
Infracciones del control de dispositivos	*Modificación de las notificaciones de Control de dispositivos en la página 10-19*
Infracciones de la política de supervisión de comportamiento	*Modificación del contenido del mensaje de notificación en la página 9-17*
Transmisiones de activos digitales	*Configuración de las notificaciones de prevención de pérdida de datos para los agentes en la página 11-60*

Tipo	Referencia
Rellamadas de C&C	*Modificar las notificaciones de amenazas Web en la página 12-15*

Notificación a los usuarios de detecciones de virus/malware y spyware/grayware

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la exploración** > **Configuración de la exploración en tiempo real** o **Configuración** > **Configuración de la exploración** > **Configuración de la exploración programada**.
4. Haga clic en la pestaña **Acción**.
5. Seleccione las siguientes opciones:
   - **Mostrar un mensaje de notificación en el endpoint del agente cuando se detecte una amenaza de virus/malware**
   - **Mostrar un mensaje de notificación en el endpoint del agente cuando se detecte una amenaza de virus/malware probable**
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración de las notificaciones de virus/malware

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. Seleccione **Virus/Malware** en el menú desplegable **Tipo**.
3. Defina la configuración de la detección.
   a. Seleccione la opción de mostrar una notificación para todos los sucesos relacionados con virus/malware o notificaciones independientes en función de los siguientes niveles de gravedad:
      - **Alto**: el Agente de OfficeScan no ha podido actuar contra el malware crítico.
      - **Medio**: el Agente de OfficeScan no ha podido actuar contra el malware.
      - **Bajo**: el Agente de OfficeScan ha podido resolver todas las amenazas.

   b. Acepte o modifique los mensajes predeterminados.
4. Haga clic en **Guardar**.

Configuración de las notificaciones de spyware/grayware

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. Seleccione **Spyware/Grayware** en el menú desplegable **Tipo**.
3. Acepte o modifique el mensaje predeterminado.

4. Haga clic en **Guardar**.

Notificación a los agentes sobre un reinicio necesario para finalizar la limpieza de los archivos infectados

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Notificación de reinicialización**.
5. Seleccione **Mostrar un mensaje de notificación si el endpoint necesita reiniciarse para finalizar la limpieza de los archivos infectados**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Registros de riesgos de seguridad

OfficeScan crea registros cuando detecta virus y malware o spyware y grayware, así como cuando restaura spyware y grayware.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de los registros de virus/malware

El Agente de OfficeScan genera registros cuando detecta virus y malware, y los envía al servidor.

Procedimiento

1. Vaya a una de las siguientes opciones:
   - **Registros** > **Agentes** > **Riesgos de seguridad**
   - **Agentes** > **Administración de agentes**
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de virus/malware** o **Ver registros** > **Registros de virus/malware**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora de la detección del virus/malware
   - Endpoint
   - Amenaza de seguridad
   - Origen de la infección

- Archivo u objeto infectado
- Ruta del archivo
- Canal de infección
- Tipo de exploración que detectó la presencia de virus/malware
- Resultados de la exploración

> **Nota**
>
> Para obtener más información sobre los resultados de la exploración, consulte *Resultados de la exploración de virus y malware en la página 7-99*.

- Dirección IP
- Dirección MAC
- Detalles del registro (haga clic en **Ver** para ver los detalles).

6. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

   El archivo CSV contiene la siguiente información:

   - Toda la información de los registros
   - Nombre del usuario conectado con endpoint en el momento de la detección

Resultados de la exploración de virus y malware

Los siguientes resultados de la exploración se muestran en los registros de virus/malware:

TABLA 7-26. Resultados de la exploración

RESULTADO	DESCRIPCIÓN
Eliminado	• La primera acción es «Eliminar» y el archivo infectado se ha eliminado.

Resultado	Descripción
	• La primera acción es «Limpiar», pero la limpieza no se realizó correctamente. La segunda acción es «Eliminar» y el archivo infectado se ha eliminado.
En cuarentena	• La primera acción es «Poner en cuarentena» y el archivo infectado se ha puesto en cuarentena. • La primera acción es «Limpiar», pero la limpieza no se realizó correctamente. La segunda acción es «Poner en cuarentena» y el archivo infectado se ha puesto en cuarentena.
Limpiado	Se limpió un archivo infectado.
Nombre modificado	• La primera acción es «Cambiar nombre» y se ha cambiado el nombre del archivo infectado. • La primera acción es «Limpiar», pero la limpieza no se realizó correctamente. La segunda acción es «Cambiar nombre» y se ha cambiado el nombre del archivo infectado.
Acceso denegado	• La primera acción es «Denegar acceso» y se ha denegado el acceso al archivo infectado cuando el usuario intentó abrir el archivo. • La primera acción es «Limpiar», pero la limpieza no se realizó correctamente. La segunda acción es «Denegar acceso» y se ha denegado el acceso al archivo infectado cuando el usuario intentó abrir el archivo. • Se han detectado posibles virus o malware durante la Exploración en tiempo real. • Es posible que la exploración en tiempo real haya denegado el acceso a los archivos infectados con un virus de arranque aunque la acción de exploración sea «Limpiar» (primera acción) y «Poner en cuarentena» (segunda acción). Esto es debido a que, al intentar limpiar un virus de arranque, se puede dañar el registro de arranque maestro (MBR) o el endpoint infectado. Ejecute la exploración manual para que OfficeScan pueda limpiar o poner en cuarentena el archivo.
Omitido	• La primera acción que se realiza es «Omitir». OfficeScan no ha realizado ninguna acción con respecto al archivo infectado.

Resultado	Descripción
	• La primera acción es «Limpiar», pero la limpieza no se realizó correctamente. La segunda acción es «Omitir» y OfficeScan no realizó ninguna acción sobre el archivo infectado.
Posible riesgo de seguridad omitido	Este resultado de exploración sólo aparecerá cuando OfficeScan detecte "posibles virus o malware" durante el Escaneo manual, los Escaneos programados o Explorar ahora. Consulte la siguiente página de la enciclopedia de virus en línea de Trend Micro para obtener información acerca de virus o malware probables, y descubrir cómo enviar archivos sospechosos a Trend Micro para su análisis. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
No se puede limpiar o poner en cuarentena el archivo	«Limpiar» es la primera acción. «Poner en cuarentena» es la segunda acción y ninguna de las acciones se realizaron correctamente. Solución: See *No se puede poner en cuarentena el archivo/No se puede cambiar el nombre del archivo en la página 7-101*.
No se puede limpiar o eliminar el archivo.	«Limpiar» es la primera acción. «Eliminar» es la segunda acción y ninguna de las dos acciones se realizaron correctamente. Solución: Consulte *No se puede eliminar el archivo en la página 7-102*.
No se puede limpiar o cambiar el nombre del archivo	«Limpiar» es la primera acción. «Cambiar el nombre» es la segunda acción y ninguna de las acciones se realizaron correctamente. Solución: See *No se puede poner en cuarentena el archivo/No se puede cambiar el nombre del archivo en la página 7-101*.
No se puede poner en cuarentena el archivo/No se puede cambiar el nombre del archivo	Explicación 1 El archivo infectado puede estar bloqueado por otra aplicación, estar ejecutándose o encontrarse en un CD. OfficeScan pondrá en cuarentena/cambiará el nombre del archivo cuando la aplicación libere el archivo o después de que este se ejecute. Solución

Resultado	Descripción
	En lo que respecta a los archivos infectados en un CD, absténgase de utilizar el CD debido a que el virus puede infectar otros endpoints de la red.
	Explicación 2 El archivo infectado se encuentra en la carpeta de archivos temporales de Internet del endpoint del agente. Puesto que el endpoint descarga archivos mientras navega, el explorador puede haber bloqueado el archivo infectado. Cuando el explorador Web libere el archivo, OfficeScan podrá poner en cuarentena/cambiar el nombre del archivo. Solución: Ninguna
No se puede eliminar el archivo	Explicación 1 Es posible que el archivo infectado se encuentre en un archivo comprimido y que se haya desactivado la opción **Limpiar/eliminar archivos infectados dentro de archivos comprimidos** de **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad**. Solución Active la opción **Limpiar/eliminar archivos infectados dentro de archivos comprimidos**. Cuando se activa, OfficeScan descomprime un archivo comprimido, limpia/elimina los archivos infectados del archivo comprimido y, a continuación, vuelve a comprimir el archivo. **Nota** Al activar esta configuración, puede aumentar el uso de los recursos del endpoint durante la exploración y, además, la exploración puede tardar más tiempo en completarse.
	Explicación 2 El archivo infectado puede estar bloqueado por otra aplicación, estar ejecutándose o encontrarse en un CD. OfficeScan eliminará el archivo cuando la aplicación libere el archivo o cuando este se haya ejecutado. Solución

Resultado	Descripción
	En lo que respecta a los archivos infectados en un CD, absténgase de utilizar el CD debido a que el virus puede infectar otros endpoints de la red.
	Explicación 3 El archivo infectado se encuentra en la carpeta de archivos temporales de Internet del endpoint del Agente de OfficeScan. Puesto que el endpoint descarga archivos mientras navega, el explorador puede haber bloqueado el archivo infectado. Cuando el explorador Web libere el archivo, OfficeScan podrá eliminar el archivo. Solución: Ninguna
No se puede enviar el archivo en cuarentena a la carpeta de cuarentena indicada	Aunque OfficeScan haya puesto en cuarentena correctamente un archivo en la carpeta `\Suspect` del endpoint del Agente de OfficeScan, no podrá enviar el archivo al directorio de cuarentena designado. Solución Determine el tipo de exploración (Exploración manual, Exploración en tiempo real, Exploración programada o Explorar ahora) que ha detectado el virus o el malware; a continuación, compruebe el directorio de cuarentena que se especifica en **Agentes** > **Administración de agentes > Configuración** > **{Tipo de exploración}** > **Acción (pestaña)**. Si el directorio de cuarentena se encuentra en el Equipo del servidor de OfficeScan o en otro Equipo del servidor de OfficeScan: 1. Compruebe si el agente se puede conectar con el servidor. 2. Si utiliza una URL como el formato del directorio de cuarentena: a. Asegúrese de que el nombre del endpoint que especifica después de `http://` es correcto. b. Compruebe el tamaño del archivo infectado. Si este supera el tamaño de archivo máximo que se especifica en **Administración** > **Configuración** > **Administrador de cuarentena**, ajuste la configuración para que se

Resultado	Descripción
	adecue al archivo. También puede realizar otras acciones como, por ejemplo, eliminar el archivo. c. Compruebe el tamaño de la carpeta del directorio de cuarentena y determine si ha superado la capacidad de la carpeta, la cual se especifica en **Administración** > **Configuración** > **Administrador de cuarentena**. Ajuste la capacidad de la carpeta o de eliminar manualmente archivos del directorio de cuarentena. 3. Si utiliza una ruta UNC, asegúrese de que la carpeta del directorio de cuarentena está compartida con el grupo «Todos» y que este grupo tiene asignados derechos de escritura y lectura. Compruebe también que la carpeta del directorio de cuarentena existe y que la ruta UNC es correcta. Si el directorio de cuarentena se encuentra en otro endpoint de la red (solo puede utilizar la ruta UNC en esta situación): 1. Compruebe si el Agente de OfficeScan se puede conectar con el endpoint. 2. Asegúrese de que la carpeta del directorio de cuarentena está compartida con el grupo «Todos» y que este grupo tiene asignados derechos de escritura y lectura. 3. Compruebe que la carpeta del directorio de cuarentena existe. 4. Compruebe que la ruta UNC es correcta. Si el directorio de cuarentena se encuentra en otro directorio del endpoint del Agente de OfficeScan (solo se puede utilizar la ruta absoluta en este caso), determine si existe la carpeta del directorio de cuarentena.
No se puede limpiar el archivo	Explicación 1 Es posible que el archivo infectado se encuentre en un archivo comprimido y que se haya desactivado la opción «Limpiar/eliminar» archivos infectados dentro de archivos comprimidos de **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad**. Solución

Resultado	Descripción
	Active la opción **Limpiar/eliminar archivos infectados dentro de archivos comprimidos**. Cuando se activa, OfficeScan descomprime un archivo comprimido, limpia/elimina los archivos infectados del archivo comprimido y, a continuación, vuelve a comprimir el archivo. **Nota** Al activar esta configuración, puede aumentar el uso de los recursos del endpoint durante la exploración y, además, la exploración puede tardar más tiempo en completarse.
	Explicación 2 El archivo infectado se encuentra en la carpeta de `archivos temporales de Internet` del endpoint del Agente de OfficeScan. Puesto que el endpoint descarga archivos mientras navega, el explorador puede haber bloqueado el archivo infectado. Cuando el explorador Web libere el archivo, OfficeScan podrá limpiar el archivo. Solución: Ninguna
	Explicación 3 Es posible que el archivo no se pueda limpiar. Consulte *Archivos que no se pueden limpiar en la página E-16* para obtener más información.
Acción necesaria	OfficeScan no puede completar la acción configurada en el archivo infectado sin la intervención del usuario. Sitúe el puntero del ratón sobre la columna **Acción necesaria** para ver la siguiente información: • «Acción necesaria: ponerse en contacto con el servicio de asistencia para obtener información sobre cómo quitar esta amenaza con la herramienta Anti-Threat Tool Kit "Arranque limpio" que se encuentra en OfficeScan ToolBox.» • «Acción necesaria: ponerse en contacto con el servicio de asistencia para obtener información sobre cómo quitar esta amenaza con la herramienta Anti-Threat Tool Kit "Disco de recuperación" que se encuentra en OfficeScan ToolBox.»

RESULTADO	DESCRIPCIÓN
	• «Acción necesaria: ponerse en contacto con el servicio de asistencia para obtener información sobre cómo quitar esta amenaza con la herramienta Anti-Threat Tool Kit "Rootkit Buster" que se encuentra en OfficeScan ToolBox.» • «Acción necesaria: OfficeScan detectó una amenaza en un agente infectado. Reinicie el endpoint para terminar de limpiar la amenaza de seguridad.» • «Acción necesaria: se requiere una exploración completa del sistema para eliminar completamente la amenaza de rootkit detectada en el endpoint.»

Visualización de los registros de Central Quarantine Restore

Después de limpiar el malware, los Agentes de OfficeScan hacen una copia de seguridad de los datos de malware. Notifique a un agente que esté conectado de manera que restaure los datos de los cuales se ha realizado una copia de seguridad si considera que estos son inofensivos. En los registros se puede encontrar la información sobre los datos de la copia de seguridad de malware que se han recuperado, el endpoint afectado y el resultado de la restauración.

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Central Quarantine Restore**.
2. Compruebe las columnas **Correcta**, **Incorrecta** y **Pendiente** para ver si OfficeScan ha restaurado de manera correcta los datos en cuarentena.
3. Haga clic en los enlaces de recuento de cada columna para obtener más información sobre cada endpoint afectado.

Nota

Si hay restauraciones **incorrectas**, puede intentar restaurar el archivo de nuevo en la pantalla **Detalles de Central Quarantine Restore Details** haciendo clic en **Restaurar todo**.

4. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Visualización de los registros de spyware/grayware

El Agente de OfficeScan genera registros cuando detecta spyware y grayware, y los envía al servidor.

Procedimiento

1. Vaya a una de las siguientes opciones:
   - **Registros** > **Agentes** > **Riesgos de seguridad**
   - **Agentes** > **Administración de agentes**
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de spyware y grayware** o **Ver registros** > **Registros de spyware y grayware**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora de la detección del spyware/grayware
   - Endpoint afectado
   - Nombre del spyware/grayware
   - Canal de infección
   - Tipo de exploración que detectó la presencia de spyware/grayware
   - Detalles sobre los resultados de la exploración de spyware o grayware (si la acción de exploración se ha realizado correctamente o no).

Consulte *Resultados de la exploración antispyware y grayware en la página 7-108* para obtener más información.

- Dirección IP
- Dirección MAC
- Detalles del registro (haga clic en **Ver** para ver los detalles).

6. Agregue spyware o grayware que considere inofensivo a la lista de spyware/grayware permitido.

7. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

   El archivo CSV contiene la siguiente información:

   - Toda la información de los registros
   - Nombre del usuario conectado al endpoint en el momento de la detección

Resultados de la exploración antispyware y grayware

Los siguientes resultados de la exploración se muestran en los registros de spyware/grayware:

TABLA 7-27. Resultados de la exploración de spyware/grayware de primer nivel

RESULTADO	DESCRIPCIÓN
Acción realizada correctamente. No se requiere ninguna otra.	Este es el resultado de primer nivel si la acción de exploración se ha realizado correctamente. El resultado de segundo nivel puede ser cualquiera de los siguientes: • *Limpiado* • *Acceso denegado*

RESULTADO	DESCRIPCIÓN
Se requieren más acciones	Este es el resultado de primer nivel si la acción de exploración no se ha realizado correctamente. Los resultados de segundo nivel deben contener como mínimo uno de los mensajes siguientes: • *Omitido* • *No es seguro limpiar el spyware/grayware.* • *Exploración de spyware/grayware detenida manualmente. Lleve a cabo una exploración completa* • *Spyware/Grayware limpiado, es necesario reiniciar. Reinicie el equipo* • *No se puede limpiar el spyware/grayware* • *Resultado de la exploración de spyware/grayware sin identificar. Póngase en contacto con el equipo de asistencia técnica de Trend Micro*

TABLA 7-28. Resultados de la exploración de spyware/grayware de segundo nivel

RESULTADO	DESCRIPCIÓN	SOLUCIÓN
Limpiado	OfficeScan ha finalizado los procesos o ha eliminado los registros, archivos, cookies y accesos directos.	N/D
Acceso denegado	OfficeScan ha denegado el acceso a los componentes de spyware y grayware detectados para copiarlos o abrirlos	N/D
Omitido	OfficeScan no ha realizado ninguna acción pero ha registrado la detección de spyware y grayware para su valoración.	agregue spyware/grayware que considere seguro a la lista de spyware/grayware permitido.

Resultado	Descripción	Solución
No es seguro limpiar el spyware/ grayware.	: este mensaje aparece si el motor de exploración antispyware intenta limpiar una carpeta y se reúnen los siguientes criterios. • Los elementos que se deben limpiar superan los 250 MB. • El sistema operativo utiliza los archivos de la carpeta. La carpeta también puede ser necesaria para un funcionamiento normal del sistema. • La carpeta es un directorio raíz (por ejemplo, `C:` o `F:`)	Póngase en contacto con su proveedor de asistencia para recibir ayuda.
Exploración de spyware/grayware detenida manualmente. Lleve a cabo una exploración completa	un usuario detuvo la exploración antes de que se completara.	ejecute una exploración manual y espere a que finalice.
Spyware/Grayware limpiado, es necesario reiniciar. Reinicie el equipo	OfficeScan ha limpiado componentes de spyware/grayware, pero el endpoint se debe reiniciar para completar la tarea.	Reinicie el endpoint de forma inmediata.
No se puede limpiar el spyware/ grayware	Se han detectado spyware y grayware en un CD-ROM o en una unidad de red. OfficeScan no puede limpiar los spyware/ grayware que se han detectado en estas ubicaciones.	Elimine manualmente el archivo infectado.

Resultado	Descripción	Solución
Resultado de la exploración de spyware/grayware sin identificar. Póngase en contacto con el equipo de asistencia técnica de Trend Micro	Una nueva versión del Motor de Escaneo de Spyware proporciona un nuevo resultado de exploración para el cual no se ha configurado OfficeScan.	Póngase en contacto con su proveedor de asistencia para obtener ayuda para determinar el nuevo resultado de la exploración.

Visualización de los registros de restauración de spyware y grayware

Tras limpiar el spyware/grayware, los Agentes de OfficeScan realizan una copia de seguridad de los datos de spyware/grayware. Notifique a un agente que esté conectado de manera que restaure los datos de los cuales se ha realizado una copia de seguridad si considera que estos son inofensivos. En los registros está disponible la información sobre qué datos de la copia de seguridad de spyware/grayware se han recuperado, el endpoint afectado y el resultado de la restauración.

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Restauración de spyware/grayware**.
2. Consulte la columna **Resultado** para comprobar si OfficeScan ha restaurado los datos de spyware y grayware correctamente.
3. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Ver los registros de archivos sospechosos

El Agente de OfficeScan genera registros cuando detecta archivos de la lista Archivos sospechosos y los envía al servidor.

Procedimiento

1. Vaya a una de las siguientes opciones:
   - **Registros** > **Agentes** > **Riesgos de seguridad**
   - **Agentes** > **Administración de agentes**
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de archivos sospechosos** o **Ver registros** > **Registro de archivos sospechosos**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora de la detección del archivos sospechosos
   - Endpoint
   - Dominio
   - Valor hash SHA-1 del origen de la infección del archivos
   - Ruta del archivo
   - Tipo de exploración que detectó la presencia de archivo sospechoso
   - Resultados de la exploración

     Nota

     Para obtener más información sobre los resultados de la exploración, consulte *Resultados de la exploración de virus y malware en la página 7-99*.

   - Dirección IP

Visualización de los registros de operaciones de exploración

Cuando se ejecutan las opciones Exploración manual, Exploración programada o Explorar ahora, el Agente de OfficeScan crea un registro de exploración que contiene información sobre dicha exploración. Puede consultar el registro de exploración en el servidor de OfficeScan o el Agente de OfficeScan.

Para consultar los registros de operaciones de exploración en el servidor de OfficeScan, vaya a una de las siguientes ubicaciones:

- **Registros** > **Agentes** > **Riesgos de seguridad** y haga clic en **Ver registros** > **Registros de operaciones de exploración**
- **Agentes** > **Administración de agentes** y haga clic en **Registros** > **Registros de operaciones de exploración**

Los registros de operaciones de exploración muestran la siguiente información:

- Fecha y hora en que OfficeScan inició la exploración
- Fecha y hora en que OfficeScan detuvo la exploración
- Estado de la exploración
    - **Completado**: la exploración se ha completado con normalidad.
    - **Interrumpida**: el usuario ha detenido la exploración antes de que se pudiese completar.
    - **Detenida de forma inesperada**: el usuario, el sistema o un suceso inesperado ha interrumpido la exploración. Por ejemplo, el servicio Exploración en tiempo real de OfficeScan puede haber finalizado de forma inesperada o el usuario puede haber forzado el reinicio del agente.
- Tipo de exploración
- Número de objetos explorados
- Número de detecciones de infecciones de virus/malware
- Número detecciones de spyware/grayware

- Versión del Smart Scan Agent Pattern
- Versión del patrón de virus
- Versión del patrón de spyware/grayware

Epidemias de riesgos de seguridad

Una epidemia de riesgos de seguridad se produce cuando las detecciones de virus/malware, spyware/grayware y sesiones de carpetas compartidas superan, en un periodo concreto de tiempo, un umbral específico. Hay varias formas de responder y de contener las epidemias de la red. Algunas de ellas son:

- Activar OfficeScan para que supervise la red en busca de actividades sospechosas
- Bloquear puertos y carpetas de endpoints del agente críticos
- Enviar mensajes de alerta de epidemias a los agentes
- Limpiar endpoints infectados

Criterios y notificaciones de las epidemias de riesgos de seguridad

Configure OfficeScan para que envíe a los administradores de OfficeScan una notificación cuando se produzcan los siguientes eventos:

TABLA 7-29. Tipos de notificaciones de epidemias sobre los riesgos de seguridad

TIPO	REFERENCIA
• Virus/Malware • Spyware/Grayware • Sesión de carpetas compartidas	*Configuración de los criterios y las notificaciones de las epidemias de riesgos de seguridad en la página 7-115*

TIPO	REFERENCIA
Infracciones del cortafuegos	*Configurar los criterios de epidemias de infracciones del cortafuegos y las notificaciones en la página 13-32*
Rellamadas de C&C	*Configuración de los criterios y las notificaciones de las epidemias de rellamadas de C&C en la página 12-21*

- Epidemia de virus/malware
- Epidemia de spyware/grayware
- Epidemias de infracciones del cortafuegos
- Epidemia de sesiones de carpetas compartidas

Defina una epidemia en función del número de detecciones y del periodo de detección. Las epidemias se activan cuando se supera el número de detecciones durante el periodo de detección.

OfficeScan incluye un conjunto de mensajes de notificación predeterminados para informarle a usted y a los administradores de OfficeScan de una epidemia. Puede modificar las notificaciones y definir la configuración de notificaciones adicionales según sus necesidades.

Nota

OfficeScan puede enviar notificaciones de las epidemias de riesgos de seguridad por correo electrónico, captura SNMP y registros de sucesos de Windows NT. En el caso de las epidemias en sesiones con carpetas compartidas, OfficeScan envía la notificación por correo electrónico. Defina la configuración cuando OfficeScan envíe notificaciones mediante estos canales. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

Configuración de los criterios y las notificaciones de las epidemias de riesgos de seguridad

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Epidemia**.

2. En la pestaña **Criterios**:

   a. Vaya a las secciones **Virus/Malware** y **Spyware/Grayware**:

   b. Especifique el número de fuentes de detección exclusivas.

   c. Especifique el número de detecciones y el periodo de detección de cada riesgo de seguridad.

Consejo

Trend Micro recomienda aceptar los valores predeterminados de esta pantalla.

OfficeScan envía la notificación cuando 10 tipos distintos de detecciones de virus/malware informan de un total de 101 riesgos de seguridad en un periodo de 5 horas. Si un agente tiene 101 detecciones de virus/malware de cualquier tipo en un periodo de 5 horas, OfficeScan también envía una notificación de epidemia.

3. En la pestaña **Criterios**:

   a. Vaya a la sección **Sesiones de carpetas compartidas**.

   b. Seleccione **Supervisar las sesiones de carpetas compartidas en la red**.

   c. En **Sesiones de carpetas compartidas registradas**, haga clic en el enlace de número para ver los endpoints con carpetas compartidas y los endpoints que pueden acceder a ellas.

   d. Especifique el número de sesiones de carpetas compartidas y el periodo de detección.

   OfficeScan envía un mensaje de notificación cuando se supera el número de sesiones de carpetas compartidas especificado.

4. En la pestaña **Correo electrónico**:

   a. Vaya a las secciones **Epidemias de virus/malware**, **Epidemias de spyware/grayware** y **Epidemias de sesiones de carpetas compartidas**.

   b. Seleccione **Activar la notificación por correo electrónico**.

   c. Especifique los destinatarios del correo electrónico.

d. Acepte o modifique el asunto y el mensaje predeterminados del correo electrónico. Puede utilizar variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 7-30. Variables de símbolo para notificaciones de epidemias de riesgos de seguridad

VARIABLE	DESCRIPCIÓN
Epidemias de virus/malware	
%CV	Número total de virus/malware detectados
%CC	Número total de endpoints con virus/malware
Epidemias de spyware/grayware	
%CV	Número total de spyware/grayware detectados
%CC	Número total de endpoints con spyware/grayware
Epidemias de sesiones de carpetas compartidas	
%S	Número de sesiones de carpetas compartidas
%T	Periodo de tiempo durante el cual se acumulan sesiones de carpetas compartidas
%M	Periodo de tiempo: en minutos

e. Seleccione información de virus o malware y de spyware o grayware para incluirla en el correo electrónico. Puede incluir el nombre del agente o del dominio, el nombre del riesgo de seguridad, la fecha y hora de la detección, la ruta y el archivo infectado y el resultado de la exploración.

f. Acepte o modifique los mensajes de notificación predeterminados.

5. En la pestaña **Captura SNMP**:

a. Vaya a las secciones **Epidemias de virus/malware** y **Epidemias de spyware/grayware**.

b. Seleccione **Activar la notificación por captura SNMP**.

c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 7-30: Variables de símbolo para notificaciones de epidemias de riesgos de seguridad en la página 7-117* para obtener más información.

6. En la pestaña **Registro de sucesos de NT**:

   a. Vaya a las secciones **Epidemias de virus/malware** y **Epidemias de spyware/grayware**.

   b. Seleccione **Activar la notificación por el registro de sucesos de NT**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 7-30: Variables de símbolo para notificaciones de epidemias de riesgos de seguridad en la página 7-117* para obtener más información.

7. Haga clic en **Guardar**.

Configuración de la prevención de epidemias de riesgos de seguridad

Cuando se produzca una epidemia, refuerce las medidas de prevención de epidemias para responder a ésta y contenerla. Defina la configuración de la prevención con detenimiento, ya que una configuración incorrecta puede causar problemas imprevistos en la red.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.
4. Haga clic en una de las siguientes políticas de prevención de epidemias y, a continuación, configúrela:

- *Limitar/Denegar el acceso a las carpetas compartidas en la página 7-120*
- *Bloqueo de puertos desprotegidos en la página 7-121*
- *Denegar el acceso de escritura a archivos y carpetas en la página 7-123*
- *Denegar el acceso a los archivos ejecutables comprimidos en la página 7-125*
- *Crear la gestión de exclusión mutua en procesos/archivos de malware en la página 7-124*

5. Seleccione las políticas que desea aplicar.

6. Seleccione el número de horas en que estará en vigor la prevención de epidemias. De forma predeterminada, son 48 horas. Puede restaurar manualmente la configuración de la red antes de que se cumpla el periodo de la prevención de epidemias.

¡ADVERTENCIA!

No permita que la prevención de epidemias permanezca activa indefinidamente. Para bloquear o denegar el acceso a archivos, carpetas o puertos de forma indefinida, modifique directamente la configuración del endpoint y la red en vez de utilizar OfficeScan.

7. Acepte o modifique los mensajes de notificación predeterminados del agente.

Nota

Si desea configurar OfficeScan para que le informe durante una epidemia, vaya a **Administración** > **Notificaciones** > **Epidemia**.

8. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

9. De nuevo, en el árbol de agentes de prevención de epidemias, compruebe la columna **Prevención de epidemias**.

   Aparecerá una marca de verificación en los endpoints que están aplicando medidas de prevención de epidemias.

OfficeScan graba los siguientes sucesos en los registros de sucesos del sistema:

- Sucesos del servidor (inicio de la prevención de epidemias y notificación a los agentes para activar la prevención de epidemias)
- Suceso del Agente de OfficeScan (activación de la prevención de epidemias)

Políticas de prevención de epidemias

Cuando se produzca una epidemia, aplique cualquiera de las siguientes políticas:

- *Limitar/Denegar el acceso a las carpetas compartidas en la página 7-120*
- *Bloqueo de puertos desprotegidos en la página 7-121*
- *Denegar el acceso de escritura a archivos y carpetas en la página 7-123*
- *Denegar el acceso a los archivos ejecutables comprimidos en la página 7-125*
- *Crear la gestión de exclusión mutua en procesos/archivos de malware en la página 7-124*

Limitar/Denegar el acceso a las carpetas compartidas

Durante las epidemias, limite o deniegue el acceso a las carpetas compartidas de la red para evitar que los riesgos de seguridad se propaguen por ellas.

Cuando esta política surte efecto, los usuarios pueden seguir compartiendo carpetas, pero la política no se aplicará a éstas. Además, informe a los usuarios que no compartan carpetas durante una epidemia y que no implementen la política de nuevo con el fin de aplicarla a las nuevas carpetas.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.

4. Haga clic en **Limitar/Denegar el acceso a las carpetas compartidas**.

5. Seleccione una de las siguientes opciones:

   - **Permitir el acceso de solo lectura**: limita el acceso a las carpetas compartidas.
   - **Denegar acceso**

   Nota

   La configuración de acceso de solo lectura no se aplica a las carpetas compartidas que ya están configuradas para denegar el acceso completo.

6. Haga clic en **Guardar**.

   Aparecerá de nuevo la pantalla **Configuración de la prevención de epidemias**.

7. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

Bloqueo de puertos desprotegidos

Durante las epidemias, bloquee los puertos vulnerables que los virus o el malware podrían utilizar para acceder a los endpoints del Agente de OfficeScan.

¡ADVERTENCIA!

Configure los parámetros de la prevención de epidemias con detenimiento. Tenga en cuenta que bloquear puertos activos puede hacer que los servicios de red que dependen de ellos dejen de estar disponibles. Por ejemplo, si bloquea el puerto de confianza, OfficeScan no podrá comunicarse con el agente durante la epidemia.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.
4. Haga clic en **Bloquear puertos**.
5. Seleccione si desea **bloquear el puerto de confianza**.
6. Seleccione los puertos que desea bloquear en la columna **Puertos bloqueados**.

    a. Si no hay ningún puerto en la tabla, haga clic en **Agregar**. En la pantalla que se abre, seleccione los puertos que desea bloquear y haga clic en **Guardar**.

    - **Todos los puertos (ICMP incluidos)**: esta opción bloquea todos los puertos excepto el puerto de confianza. Si también desea bloquear el puerto de confianza, active la casilla de verificación Bloquear puerto de confianza de la pantalla anterior.
    - **Puertos especificados**
        - **Puertos utilizados habitualmente**: seleccione al menos un número de puerto para que OfficeScan pueda guardar la configuración del bloqueo de puertos.
        - **Puertos utilizados habitualmente por troyanos**: bloquea los puertos que normalmente utilizan los troyanos. Consulte *Puerto de troyano en la página E-13* para obtener más información.
        - **Un número de puerto o intervalo de puertos entre 1 y 65535**: también puede especificar la dirección del tráfico que se bloqueará y algunos comentarios, tales como el motivo del bloqueo de los puertos especificados.
        - **Protocolo Ping (rechazar ICMP)**: haga clic en esta opción si desea bloquear solamente paquetes ICMP, por ejemplo, solicitudes ping.

    b. Para editar la configuración de los puertos bloqueados, haga clic en el número de puerto.

    c. En la pantalla que se abre, modifique la configuración y haga clic en **Guardar**.

d. Para quitar un puerto de la lista, selecciona la casilla de verificación que aparece junto al puerto deseado y haga clic en **Eliminar**.

7. Haga clic en **Guardar**.

   Aparecerá de nuevo la pantalla **Configuración de la prevención de epidemias**.

8. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

Denegar el acceso de escritura a archivos y carpetas

Los virus/malware pueden modificar o eliminar archivos y carpetas de los endpoints host. Durante una epidemia, configure OfficeScan para que los virus o malware no modifiquen ni eliminen los archivos y las carpetas de los endpoints del Agente de OfficeScan.

¡ADVERTENCIA!

OfficeScan no permite denegar el acceso de escritura a las unidades de red asignadas.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.
4. Haga clic en **Denegar el acceso de escritura a archivos y carpetas**.
5. Escriba la ruta de acceso de directorio. Cuando acabe de escribir la ruta de acceso de los directorios que desee proteger, haga clic en **Agregar**.

Nota

Escriba la ruta de acceso absoluta del directorio en vez de la ruta virtual.

6. Especifique los archivos que desea proteger en los directorios protegidos. Seleccione todos los archivos o archivos según sus extensiones. En el caso de las extensiones de archivos, si desea especificar una extensión que no figure en la lista, escríbala en el cuadro de texto y, a continuación, haga clic en **Añadir**.

7. Para proteger archivos específicos, en **Archivos para proteger**, escriba el nombre completo del archivo y haga clic en **Agregar**.

8. Haga clic en **Guardar**.

   Aparecerá de nuevo la pantalla **Configuración de la prevención de epidemias**.

9. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

Crear la gestión de exclusión mutua en procesos/archivos de malware

Puede configurar la prevención de epidemias para protegerse frente a amenazas de seguridad que utilicen procesos de mutex si sobrescribe los recursos que la amenaza necesita para infectar el sistema y extenderse por el mismo. La prevención de epidemias crea extensiones mutuas en archivos y procesos relacionados con malware conocido e impide que el malware acceda a estos recursos.

Consejo

Trend Micro recomienda mantener estas exclusiones hasta que se pueda implementar una solución para la amenaza de malware. Póngase en contacto con el servicio de asistencia para obtener los nombres de mutex correctos frente a los que hay que estar protegidos durante una epidemia.

Nota

La gestión de exclusión mutua requiere el servicio de prevención de cambios no autorizados y solo es compatible con plataformas de 32 bits.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.
4. Haga clic en **Crear gestión de exclusión mutua (mutex) en procesos/archivos de malware**.
5. Escriba el nombre del mutex del que desea protegerse en el campo correspondiente.

   Agregue o quite nombres de mutex de la lista mediante utilizando los botones **+** y **-**.

   Nota

   La prevención de epidemias es compatible con la gestión de exclusión mutua para un máximo de seis amenazas de mutex.

6. Haga clic en **Guardar**.

   Aparecerá de nuevo la pantalla **Configuración de la prevención de epidemias**.

7. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

Denegar el acceso a los archivos ejecutables comprimidos

Durante una epidemia, denegar el acceso a los archivos ejecutables comprimidos puede evitar que los riesgos de seguridad que contengan se extiendan por la red. Puede elegir permitir el acceso a archivos de confianza creados por programas Packer ejecutables compatibles.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Iniciar Prevención de epidemias**.
4. Haga clic en **Denegar el acceso a los archivos ejecutables comprimidos**.
5. Haga su selección en la lista de programas Packer ejecutables compatibles y, a continuación, haga clic en **Agregar** para permitir el acceso a archivos ejecutables comprimidos creados por programas Packer.

   Nota

   Solo puede aprobar el uso de archivos empaquetados creados por los programas Packer de la lista de Packers ejecutables. La prevención de epidemias denegará el acceso a los demás formatos de archivos empaquetados ejecutables.

6. Haga clic en **Guardar**.

   Aparecerá de nuevo la pantalla **Configuración de la prevención de epidemias**.

7. Haga clic en **Iniciar Prevención de epidemias**.

   Las medidas de prevención de epidemias que ha seleccionado se mostrarán en una ventana nueva.

Desactivar la prevención de epidemias

Restaure la configuración de red normal mediante la desactivación de la prevención de epidemias sólo cuando esté seguro de que una epidemia se ha contenido y de que OfficeScan ha limpiado o puesto en cuarentena todos los archivos infectados.

Procedimiento

1. Vaya a **Agentes** > **Prevención de epidemias**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Restaurar configuración**.
4. Para informar a los usuarios de que la epidemia ha finalizado, seleccione **Notificar a los usuarios después de restaurar la configuración original**.
5. Acepte o modifique los mensajes de notificación predeterminados del agente.
6. Haga clic en **Restaurar configuración**.

Nota

Si no restablece la configuración de la red manualmente, OfficeScan la restablecerá de forma automática una vez transcurrido el número de horas especificado en **Restaurar automáticamente la configuración de la red a su estado normal tras __ horas** de la pantalla **Configuración de la prevención frente a epidemias**. La configuración predeterminada es 48 horas.

OfficeScan graba los siguientes sucesos en los registros de sucesos del sistema:

- Sucesos del servidor (inicio de la prevención de epidemias y notificación a los Agentes de OfficeScan para activar la prevención de epidemias)
- Suceso del Agente de OfficeScan (activación de la prevención de epidemias)

7. Después de desactivar la prevención de epidemias, explore los endpoints conectados en red en busca de riesgos de seguridad para garantizar que la epidemia se ha contenido.

Capítulo 8

Protección frente a amenazas desconocidas

En este capítulo se describe cómo proteger los endpoints de amenazas desconocidas que intenten infiltrarse en la red.

Los temas que se incluyen son:

- *Aprendizaje automático predictivo en la página 8-2*
- *Servicio de conexión sospechosa en la página 8-5*
- *Envío de muestras en la página 8-9*
- *Registros de amenazas desconocidas en la página 8-11*

Aprendizaje automático predictivo

El aprendizaje automático predictivo de Trend Micro usa una tecnología de aprendizaje automático avanzada para comparar información de amenazas y analizar archivos a fondo a fin de detectar riesgos de seguridad desconocidos emergentes mediante huellas de ADN digital, asignaciones de API y otras características de los archivos. El aprendizaje automático predictivo también realiza un análisis del comportamiento en procesos desconocidos o de baja incidencia para determinar si una amenaza emergente o desconocida intenta infectar la red.

El aprendizaje automático predictivo es una herramienta potente que le ayuda a proteger su entorno frente a amenazas no identificadas y ataques de día cero.

Tipo de detección	Descripción
Archivo	Tras detectar un archivo desconocido o de baja incidencia, OfficeScan lo explora mediante el motor de exploración de amenazas avanzadas (ATSE) para extraer las características de archivo y, a continuación, envía el informe al motor de aprendizaje automático predictivo, el cual se aloja en Trend Micro Smart Protection Network. Mediante el uso de modelos de malware, el aprendizaje automático predictivo compara la muestra con el modelo de malware, le asigna una puntuación de probabilidad y determina el tipo de malware probable que el archivo contiene. En función de cómo haya configurado el aprendizaje automático predictivo, OfficeScan intentará «poner en cuarentena» el archivo afectado para evitar que la amenaza se propague por la red.

Tipo de detección	Descripción
Proceso	Tras detectar un proceso desconocido o de baja incidencia, OfficeScan supervisa el proceso mediante el motor de inteligencia contextual y envía el informe del comportamiento al motor de aprendizaje automático predictivo. Mediante el uso de modelos de malware de comportamiento, el aprendizaje automático predictivo compara el comportamiento del proceso con el modelo, le asigna una puntuación de probabilidad y determina el tipo de malware probable que ejecuta el proceso. Según cómo haya configurado el aprendizaje automático predictivo, OfficeScan podrá «terminar» el proceso afectado e intentar limpiar el archivo que ejecutó el proceso.

Configuración de las opciones del aprendizaje automático predictivo

Nota

El aprendizaje automático predictivo requiere que se activen los siguientes servicios:

- Prevención de cambios no autorizados
- Servicio de protección avanzada

Para obtener más información, consulte *Activar o desactivar los servicios del agente desde la consola Web en la página 15-9*.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración del aprendizaje automático predictivo**.

   Aparecerá la pantalla **Configuración del aprendizaje automático predictivo**.

4. Seleccione **Activar el aprendizaje automático predictivo**.

5. En **Configuración de detección**, seleccione el tipo de detecciones y la acción relacionada que llevará a cabo el aprendizaje automático predictivo.

Tipo de detección	Acciones
Archivo	• **Poner en cuarentena**: seleccione esta opción para poner en cuarentena automáticamente los archivos que presenten características relacionadas con malware según el análisis del aprendizaje automático predictivo. • **Solo registrar**: seleccione esta opción para explorar archivos desconocidos y registrar el análisis del aprendizaje automático predictivo para realizar una investigación interna a fondo de la amenaza.
Proceso	• **Terminar**: seleccione esta opción para terminar los procesos que presenten características relacionadas con malware según el análisis del aprendizaje automático predictivo. **Importante** El aprendizaje automático predictivo intentará limpiar los archivos que hayan ejecutado los procesos maliciosos. Si la acción de limpieza no se realiza correctamente, OfficeScan pondrá en cuarentena los archivos afectados. • **Solo registrar**: seleccione esta opción para explorar procesos desconocidos y registrar el análisis del aprendizaje automático predictivo para realizar una investigación interna a fondo de la amenaza.

6. En **Excepciones**, configure las excepciones de archivos del aprendizaje automático predictivo globales para evitar que todos los agentes detecten un archivo como malicioso.

   a. Haga clic en **Agregar hash de archivo**.

      Aparecerá la pantalla **Agregar archivo a la lista de excepciones**.

b. Especifique el valor hash SHA-1 del archivo para excluirlo de la exploración.

c. También puede añadir una nota para explicar el motivo de la excepción, o bien para indicar los nombres de archivo asociados con el valor hash.

d. Haga clic en **Agregar**.

OfficeScan añadirá el hash de archivo a la lista de excepciones.

7. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Servicio de conexión sospechosa

El servicio de conexión sospechosa gestiona las listas IP de C&C globales y definidas por el usuario, y supervisa el comportamiento de las conexiones que los endpoints establecen con los servidores C&C.

- Las listas de IP bloqueadas y permitidas definidas por el usuario permiten controlar mejor el acceso de los Endpoints a determinadas direcciones IP. Configure estas listas si quiere permitir el acceso a una dirección bloqueada por la lista IP de C&C global o bloquear el acceso a una dirección que pueda constituir un riesgo de seguridad.

  Para conocer más detalles, consulte *Configurar los ajustes de las listas de IP generales definidas por el usuario en la página 8-6*.

- La lista IP de C&C global se utiliza junto con el Motor de inspección del contenido de red (NCIE) para detectar conexiones de red con servidores de C&C

confirmados de Trend Micro. NCIE detecta el contacto del servidor C&C a través de cualquier canal de red. El servicio de conexión sospechosa registra toda la información de conexión en los servidores de la lista IP de C&C global para su evaluación.

Para obtener más información sobre cómo activar la lista IP de C&C global, consulte *Definir la configuración de conexión sospechosa en la página 8-7*.

- Después de detectar malware en un endpoint mediante la coincidencia con el patrón de reglas de relevancia de los paquetes de red, el servicio de conexión sospechosa puede investigar el comportamiento de la conexión para determinar si se ha producido una rellamada de C&C. Después de detectar una rellamada de C&C, el servicio de conexión sospechosa puede intentar bloquear y limpiar el origen de la conexión mediante la tecnología GeneriClean.

  Para obtener más información sobre cómo configurar el servicio de conexión sospechosa, consulte *Definir la configuración de conexión sospechosa en la página 8-7*.

  Para obtener más información sobre GeneriClean, consulte *GeneriClean en la página E-4*.

Active el servicio de conexión sospechosa en la pantalla **Configuración de servicios adicionales** para proteger a los agentes frente a rellamadas del servidor C&C. Para conocer más detalles, consulte *Activar o desactivar los servicios del agente desde la consola Web en la página 15-9*.

Configurar los ajustes de las listas de IP generales definidas por el usuario

Los administradores pueden configurar OfficeScan para permitir, bloquear o registrar todas las conexiones entre los agentes y las listas de direcciones IP de C&C definidas por el usuario.

Nota

Las listas de IP definidas por el usuario solo son compatibles con direcciones IPv4.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Configuración de seguridad**.
3. Vaya a la sección **Configuración de conexión sospechosa**.
4. Haga clic en **Editar lista de IP definida por el usuario**.
5. En la pestaña **Lista de permitidas** o **Lista de bloqueadas**, agregue las direcciones IP que quiera supervisar.

   Consejo

   Puede configurar OfficeScan para registrar solo las conexiones establecidas con direcciones de la lista de IP definida por el usuario. Para registrar solo conexiones establecidas con direcciones de la lista de IP definida por el usuario, consulte *Definir la configuración de conexión sospechosa en la página 8-7*.

   a. Haga clic en **Agregar**.

   b. En la pantalla que aparecerá, escriba la dirección IP, el intervalo de direcciones IP, o la dirección IPv4 y la máscara de subred que desea que supervise OfficeScan.

   c. Haga clic en **Guardar**.

6. Para quitar una dirección IP de la lista, seleccione la casilla de verificación que aparece junto a la dirección deseada y haga clic en **Eliminar**.
7. Una vez configuradas las listas, haga clic en **Cerrar** para volver a la pantalla **Configuración general del agente**.
8. Haga clic en **Guardar** para implementar las listas actualizadas en todos los agentes.

Definir la configuración de conexión sospechosa

OfficeScan puede registrar y bloquear todas las conexiones que se hayan establecido entre los agentes y las direcciones de la lista IP de C&C global. La pantalla

Configuración de conexión sospechosa también le permite registrar, pero continúa permitiéndole acceder a direcciones IP configuradas en la lista de IP bloqueadas definida por el usuario.

OfficeScan también puede supervisar aquellas conexiones que sean resultado de una botnet o cualquier otra amenaza de malware. Tras detectar una amenaza de malware, OfficeScan puede intentar limpiar la infección.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de conexión sospechosa**.

   Aparecerá la pantalla **Configuración de conexión sospechosa**.
4. Active la opción **Detectar las conexiones de red realizadas a las direcciones de la lista IP de C&C global** para supervisar las conexiones que se hayan establecido con servidores C&C confirmados por Trend Micro y decida si, para dichas conexiones, desea **Solo registrar** o **Bloquear**.

   - Para permitir a los agentes conectarse a las direcciones de la lista de IP bloqueadas definida por el usuario, active la configuración **Registrar y permitir el acceso a las direcciones de la lista de IP bloqueadas definida por el usuario**.

   Nota

   Debe activar el registro de conexiones a la red para que OfficeScan permita el acceso a las direcciones de la lista de IP bloqueadas definida por el usuario.

   Para obtener información acerca de la lista IP de C&C global, consulte *Servicio de conexión sospechosa en la página 8-5*.
5. Habilite la opción **Detectar las conexiones mediante huellas de red de malware** y decida si desea **Solo registrar** o **Bloquear** las conexiones.

Las huellas de red de malware llevan a cabo coincidencias de patrones de los encabezados de paquete. OfficeScan registra todas las conexiones establecidas por paquetes que tienen encabezados que coinciden con amenazas de malware conocidas utilizando el patrón de reglas de relevancia.

- Para que OfficeScan intente limpiar las conexiones que se han establecido con servidores C&C, active la opción **Limpiar conexiones sospechosas cuando se detecte una rellamada de C&C**. OfficeScan usa GeneriClean para limpiar amenazas de malware y finalizar la conexión con el servidor C&C.

Nota

Debe activar la opción **Registrar conexiones usando huellas de red de malware** para que OfficeScan pueda limpiar las conexiones que se han establecido con servidores C&C detectadas mediante la coincidencia de estructuras de paquetes.

6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Envío de muestras

Puede configurar los Agentes de OfficeScan para que envíen objetos de archivo que puedan contener amenazas que no se hayan identificado con anterioridad a una instancia de Analizador virtual para su análisis. Tras valorar los objetos, Analizador virtual añadirá los objetos que contengan amenazas desconocidas a las listas de objetos sospechosos de Analizador virtual y las distribuirá a los demás Agentes de OfficeScan de la red.

Para obtener más información, consulte *Configuración de la lista de objetos sospechosos en la página 14-34*.

El envío de muestras requiere lo siguiente:

- Debe registrar el servidor de OfficeScan con un servidor de Trend Micro Control Manager (6.0 SP3 con revisión 2 o posterior).
- El servidor de Trend Micro Control Manager debe tener una conexión activa con un servidor de Trend Micro Deep Discovery Analyzer (5.1 o posterior).

Estos son algunos archivos sospechosos:

- Programas que Trend Micro no conoce (descargados a través de exploradores Web compatibles o canales de correo electrónico).
- Detecciones heurísticas de procesos (descargadas a través de exploradores Web compatibles o canales de correo electrónico).
- Programas de ejecución automática de baja incidencia en almacenamiento extraíble.

Importante

Los Agentes de OfficeScan pueden enviar archivos de muestra de hasta 50 MB a Analizador virtual para su análisis.

Configuración del envío de muestras

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de envío de muestras**.

   Aparecerá la pantalla **Configuración de envío de muestras**.
4. Seleccione **Activar el envío de archivos sospechosos a Analizador virtual**.

5. Haga clic en **Guardar**.

Registros de amenazas desconocidas

Los Agentes de OfficeScan registran la actividad de amenazas desconocidas y envían los registros al servidor. De forma predeterminada, un Agente de OfficeScan que se ejecuta de forma continua agrega registros continuamente y los envía cada 60 minutos.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de los registros del aprendizaje automático predictivo

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Ver Registros** > **Registros del aprendizaje automático predictivo** o en **Registros** > **Registros del aprendizaje automático predictivo**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:

EVENTO	DESCRIPCIÓN
Fecha/hora	La hora a la que se produjo la detección
Endpoint	El endpoint en el que tuvo lugar la detección

EVENTO	DESCRIPCIÓN
Dirección IP	La dirección IP y el número del puerto del endpoint de origen
Amenaza a la seguridad	El nombre de la amenaza de seguridad determinada por el motor del aprendizaje automático predictivo
Resultado	El resultado de la acción ejecutada
Nombre de archivo	El nombre del objeto de archivo o del programa que ejecutó el proceso
Tipo	El tipo del objeto que activó la detección («Archivo» o «Proceso»)
Ruta del archivo	La ruta del objeto de archivo o del programa que ejecutó el proceso
Canal de infección	El canal en el que se originó la amenaza
Detalles	Un enlace que muestra el análisis detallado de esa detección concreta Para obtener más información, consulte *Detalles de registro del aprendizaje automático predictivo en la página 8-12*.

6. Para guardar registros como archivos de valores separados por comas (CSV), haga clic en **Exportar todo a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Detalles de registro del aprendizaje automático predictivo

Puede ver un informe completo de cada detección del registro del aprendizaje automático predictivo haciendo clic en el enlace **Ver** de la columna **Detalles**.

La pantalla **Detalles del registro** consta de dos secciones:

- Banner superior: incluye los detalles específicos relacionados con esa detección del registro determinada.

- Controles de la pestaña inferior: incluye detalles relacionados con la amenaza de aprendizaje automático predictivo, como puntuaciones de probabilidad de amenaza, información de archivo y otros endpoints de la red en los que se haya detectado lo mismo.

En la siguiente tabla se expone la información que se proporciona en el banner superior.

TABLA 8-1. Detalles del registro: banner superior

SECCIÓN	DESCRIPCIÓN
Hora de la detección/Acción	Indica la hora en que se produjo esa detección del registro concreta y la acción que el agente realizó acerca de la amenaza.
Nombre de archivo	Indica el nombre del archivo que activó la detección en el endpoint especificado. **Consejo** Haga clic en **Agregar a la lista de excepciones** para agregar el valor hash de archivo afectado a la lista global de excepciones del aprendizaje automático predictivo. Podrá ver la lista de excepciones completa en la pantalla **Configuración del aprendizaje automático predictivo**. Para obtener más información, consulte *Configuración de las opciones del aprendizaje automático predictivo en la página 8-3*. **Importante** Puede que el nombre del archivo detectado en esta ocasión no sea el mismo que el nombre del archivo detectado en otros agentes. El aprendizaje automático predictivo asocia las detecciones según los valores hash de archivo, no en función de nombres de archivo específicos. Consulte la pestaña **Endpoints afectados** para comprobar el nombre del archivo en otros endpoints.
Información del endpoint	Muestra el usuario que había iniciado sesión en el momento de la detección, el nombre del endpoint y la dirección IP del endpoint.

Sección	Descripción
Información del canal	Muestra el canal donde se originó la amenaza y la ubicación de la carpeta del endpoint a la que se transfirió la amenaza.

En la siguiente tabla se expone la información que se proporciona en las pestañas inferiores.

Tabla 8-2. Detalles del registro: información de las pestañas

Pestaña	Descripción
Indicadores de amenaza	Ofrece los resultados del análisis del aprendizaje automático predictivo. • **Probabilidad de amenaza**: indica la similitud del archivo o el proceso con el modelo de malware. • **Tipo de amenaza probable**: indica cuál es el tipo de amenaza más probable que contiene el archivo después de que el aprendizaje automático predictivo compare el análisis con otras amenazas conocidas. • **Identificadores de amenazas**: ofrece una lista de las funciones de API que usa el archivo o el proceso, las cuales pueden indicar el tipo de amenaza detectado. **Importante** La identificación de las funciones de API es uno de los factores para determinar el tipo de amenaza. El aprendizaje automático predictivo usa otras características de archivo y otros métodos de análisis para calcular la probabilidad de amenaza y el tipo de amenaza más probable. • **Amenazas conocidas similares**: ofrece una lista de tipos de amenaza conocidos que presentan características de archivo o proceso similares a las de la detección.
Detalles del archivo	Ofrece detalles generales relacionados con las propiedades del archivo y la información del certificado de ese registro de detección concreto.

Pestaña	Descripción
Endpoints afectados	Muestra una lista de los demás agentes de la red con la misma detección de aprendizaje automático predictivo y ofrece detalles específicos sobre las detecciones en los otros agentes.

Ver los registros de conexión sospechosa

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Ver registros** > **Registros de conexión sospechosa** o **Registros** > **Registros de conexión sospechosa**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:

Evento	Descripción
Fecha/hora	La hora a la que se produjo la detección
Endpoint	El endpoint en el que tuvo lugar la detección
Dominio	El dominio del endpoint en el que tuvo lugar la detección
Proceso	El proceso que inició la transmisión (path \application_name)
IP y puerto locales	La dirección IP y el número del puerto del endpoint de origen
IP y puerto remotos	La dirección IP y el número del puerto del endpoint de destino

EVENTO	DESCRIPCIÓN
Resultado	El resultado de la acción ejecutada
Detectado por	Origen de lista de C&C que identificó el servidor C&C
Dirección del tráfico	La dirección de la transmisión

6. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar todo a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Visualización de los registros de envío de muestras

OfficeScan almacena los datos de envío de muestras en los registros de sucesos del sistema. Para obtener un resumen más detallado de los datos de envío de muestras, Trend Micro recomienda utilizar la consola de Control Manager para consultar los registros. Control Manager ofrece un análisis detallado del proceso de administración de los archivos de objetos sospechosos y le proporciona una visión más completa del modo en que los objetos sospechosos pueden afectar a la red.

Procedimiento

1. Vaya a **Registros** > **Sucesos del sistema**.
2. En **Suceso**, busque los siguientes tipos de registro:
   - «Muestra enviada a Analizador virtual [file[<file_name], SHA1[<file_SHA1_value>]»
   - «Análisis de muestras del Analizador virtual completado [<date_time_analysis_completed>, file[<file_name], SHA1[<file_SHA1_value>], virus[<detection_type], rule[<virtual_analyzer_rule_type]]»

Capítulo 9

Uso de Supervisión del comportamiento

En este capítulo se describe cómo proteger los ordenadores frente a riesgos de seguridad mediante la función Supervisión de comportamiento.

Los temas que se incluyen son:

- *Supervisión del comportamiento en la página 9-2*
- *Configuración de las opciones de supervisión de comportamiento global en la página 9-13*
- *Privilegios de supervisión de comportamiento en la página 9-15*
- *Notificaciones de la supervisión del comportamiento para usuarios del agente de OfficeScan en la página 9-16*
- *Registros de supervisión del comportamiento en la página 9-18*

Supervisión del comportamiento

El componente Supervisión del comportamiento supervisa constantemente los Endpoints en busca de modificaciones inusuales en el sistema operativo o en el software instalado. El componente Supervisión del comportamiento protege los Endpoints mediante las funciones **Bloqueador de comportamientos malintencionados** y **Supervisión de eventos**. Como complemento a dichas funciones, dispone de una **lista de excepciones** configurada por el usuario y del **Servicio de software seguro certificado**.

Importante

- El componente Supervisión del comportamiento no es compatible con las plataformas Windows XP o Windows 2003 de 64 bits.
- El componente Supervisión del comportamiento no es compatible con las plataformas Windows Vista de 64 bits con SP1 o posterior.
- De forma predeterminada, la supervisión de comportamiento está desactivada en todas las versiones de las plataformas de Windows Server. Antes de activar la supervisión de comportamiento en estas plataformas del servidor, lea las directrices y las prácticas recomendadas descritas en *Servicios del agente de OfficeScan en la página 15-7*.

Bloqueador de comportamientos malintencionados

El Bloqueador de comportamientos malintencionados proporciona una capa adicional para la protección frente a amenazas procedentes de programas que muestren un comportamiento malicioso. Observa eventos del sistema durante un periodo de tiempo. Si los programas ejecutan combinaciones o secuencias de acciones diferentes, el Bloqueador de comportamientos malintencionados detecta el comportamiento malicioso conocido y bloquea los programas a los que esté asociado. Utilice esta función para garantizar un alto nivel de protección frente a las amenazas nuevas, las desconocidas y las emergentes.

La supervisión del comportamiento de malware proporciona las siguientes opciones de exploración de nivel de amenaza:

- **Amenazas conocidas**: bloquea comportamientos asociados a las amenazas conocidas.

- **Amenazas conocidas y potenciales**: bloquea el comportamiento asociado a las amenazas conocidas y realiza acciones contra el comportamiento potencialmente malicioso.

Cuando se bloquea un programa y las notificaciones están activadas, OfficeScan muestra una notificación en el Agente de OfficeScan endpoint. Para obtener información detallada acerca de las notificaciones, consulte *Notificaciones de la supervisión del comportamiento para usuarios del agente de OfficeScan en la página 9-16*.

Protección frente al ransomware

La protección frente al ransomware impide que las amenazas de «ransomware» modifiquen o cifren archivos sin autorización en los agentes. Ransomware es un tipo de malware que limita el acceso a los archivos y exige un pago para restaurar los archivos afectados.

OfficeScan ofrece los siguientes métodos para proteger su entorno frente a amenazas de ransomware.

Nota

Para disminuir el riesgo de que OfficeScan detecte un proceso seguro como malicioso, asegúrese de que el agente tiene acceso a Internet para realizar procesos de verificación adicionales mediante los servidores de Trend Micro.

Opción	Descripción
Proteger documentos frente a modificaciones o cifrados no autorizados	Puede configurar la supervisión de comportamiento para que detecte una determinada secuencia de sucesos que podrían indicar un ataque de ransomware. Cuando la supervisión del comportamiento haya comprobado los siguientes criterios, OfficeScan finalizará y pondrá en cuarentena los programas maliciosos: 1. Un proceso no reconocido como seguro intenta modificar, eliminar o cambiar el nombre de tres archivos dentro de un determinado intervalo de tiempo. 2. El proceso intentó modificar un tipo de extensión de archivo protegido. Active también **Crear automáticamente una copia de seguridad de los archivos modificados por programas sospechosos** para crear copias de los archivos que se cifran en los endpoints. Cuando finalice el proceso de cifrado y OfficeScan detecte una amenaza de ransomware, OfficeScan pedirá a los usuarios finales que restauren los archivos afectados sin haber perdido datos. **Nota** La copia de seguridad de archivos automática requiere al menos 100 MB de espacio en disco en el endpoint del agente, y solo realizará copias de seguridad de los archivos que tengan menos de 10 MB. La ubicación de la carpeta de copias de seguridad en el endpoint del agente es: <carpeta de instalación del agente>`\CCSF\module\DRE\data`. **¡ADVERTENCIA!** Si no se activa **Crear automáticamente una copia de seguridad de los archivos modificados por programas sospechosos**, OfficeScan no podrá recuperar los primeros archivos afectados por una amenaza de ransomware.

Opción	Descripción
Bloquear procesos que habitualmente se asocian con ransomware	El ransomware suele distribuir archivos ejecutables en ubicaciones concretas de los endpoints antes de intentar secuestrar archivos. Si se bloquean los procesos iniciados desde estas ubicaciones, se puede evitar que el ransomware secuestre archivos.
Activar la inspección de programas para detectar y bloquear archivos ejecutables comprometidos	La inspección de programas supervisa los procesos y lleva a cabo enlace de API para determinar si un programa se comporta de forma inesperada. Aunque este proceso aumenta la tasa general de detecciones de archivos ejecutables comprometidos, puede afectar negativamente al rendimiento del sistema. **Consejo** La inspección de programas ofrece una mayor seguridad si selecciona **Amenazas conocidas y potenciales** en el menú desplegable **Amenazas que se bloquearán**. **Importante** No es compatible con plataformas Windows Server 2003 sin SP2 (o posterior) ni Windows XP de 64 bits.

Protección frente a explotación

La protección frente a explotación funciona junto con la inspección de programas para supervisar el comportamiento de los programas y para detectar comportamientos anómalos que pueden indicar que un atacante ha aprovechado una vulnerabilidad de programa. Una vez detectado, la supervisión del comportamiento finaliza los procesos del programa.

Importante

La protección frente a explotación requiere la selección de la opción **Activar la inspección de programas para detectar y bloquear archivos ejecutables comprometidos**.

Proteger frente a programas recién encontrados

La supervisión del comportamiento funciona junto con los servicios de Web Reputation y la exploración en tiempo real para comprobar la incidencia de archivos descargados a través de canales HTTP, aplicaciones de correo electrónico o scripts de macros de Microsoft Office. Tras detectar un archivo "recién encontrado", los administradores pueden elegir preguntar a los usuarios antes de ejecutar el archivo. Trend Micro clasifica un programa como recién encontrado en función del número de detecciones de archivos o de la edad histórica del archivo según lo determina Smart Protection Network.

La supervisión de comportamiento explora los siguientes tipos de archivo de cada canal:

- HTTP/HTTPS: explora archivos `.exe`.
- Aplicaciones de correo electrónico: explora archivos `.exe`, archivos `.exe` comprimidos en paquetes `.zip` no cifrados y archivos `.rar`.

Nota

- Los administradores deben activar los servicios de Web Reputation en el agente para permitir que OfficeScan explore el tráfico HTTP o HTTPS antes de mostrar esta solicitud.
- OfficeScan compara los nombres de los archivos descargados a través de aplicaciones de correo electrónico durante el proceso de ejecución. Si el nombre de archivo ha sido cambiado, el usuario no recibe una notificación.

Supervisión de eventos

La función Supervisión de eventos proporciona un enfoque más general en la protección frente a software no autorizado o ataques de malware. Supervisa determinados sucesos en áreas del sistema, lo que permite que los administradores regulen aquellos programas que den lugar a dichos eventos. Utilice la función Supervisión de eventos si cuenta con unos requisitos de protección del sistema específicos que se hallen más allá de la protección que proporciona el Bloqueador de comportamientos malintencionados.

En la siguiente tabla se muestra una lista de los sucesos del sistema supervisado.

TABLA 9-1. Sucesos del sistema supervisado

SUCESOS	DESCRIPCIÓN
Archivos de sistema duplicados	Muchos programas maliciosos crean copias de sí mismos o de otros programas maliciosos utilizando los mismos nombres de archivo que el sistema Windows. Esto se hace generalmente para sobrescribir o sustituir archivos del sistema, evitar la detección o disuadir a los usuarios de que no eliminen los archivos maliciosos.
Modificar el archivo Hosts	El archivo Hosts asocia nombres de dominio con direcciones IP. Muchos programas maliciosos modifican el archivo Hosts para que el explorador Web entre en sitios Web infectados, falsos o que no existen.
Comportamiento sospechoso	El comportamiento sospechoso puede ser una acción específica o una serie de acciones que no suelen realizar los programas legítimos. Los programas con un comportamiento sospechoso se deben usar con precaución.
Nuevo complemento de Internet Explorer	Los programas de spyware/grayware a menudo instalan complementos de Internet Explorer no deseados, incluidas barras de herramientas y objetos de ayuda del explorador.
Modificar la configuración de Internet Explorer	Muchos virus o malware cambian elementos de la configuración de Internet Explorer, incluidos la página de inicio, sitios Web de confianza, configuración del servidor proxy y extensiones de menú.
Modificar las políticas de seguridad	Las modificaciones de las políticas de seguridad de Windows pueden permitir que aplicaciones no deseadas se ejecuten y cambien la configuración del sistema.
Inyección de biblioteca de programas	Muchos programas maliciosos configuran Windows de forma que todas las aplicaciones carguen automáticamente una biblioteca de programas (DLL). Esto permite que las rutinas maliciosas de la DLL se ejecuten cada vez que se inicia una aplicación.

Sucesos	Descripción
Modificar el shell	Muchos programas maliciosos modifican la configuración del shell de Windows para asociarse a determinados tipos de archivo. Esta rutina permite que los programas maliciosos se inicien automáticamente si los usuarios abren los archivos asociados en el Explorador de Windows. Los cambios en la configuración del shell de Windows también permiten que los programas maliciosos hagan un seguimiento de los programas utilizados y se inicien junto con aplicaciones legítimas.
Nuevo servicio	Los servicios de Windows son procesos que tienen funciones especiales y generalmente se ejecutan continuamente en segundo plano con acceso administrativo completo. Los programas maliciosos a veces se instalan como servicios para permanecer ocultos.
Modificar los archivos del sistema	Algunos archivos del sistema de Windows determinan el comportamiento del sistema, incluidos los programas de inicio y la configuración del salvapantallas. Muchos programas maliciosos modifican los archivos del sistema para iniciarse automáticamente durante el inicio y controlar el comportamiento del sistema.
Modificar la política de cortafuegos	La política de cortafuegos de Windows determina las aplicaciones que tienen acceso a la red, los puertos abiertos para la comunicación y las direcciones IP que pueden comunicarse con el equipo. Muchos programas maliciosos modifican la política para poder acceder a la red y a Internet.
Modificar los procesos del sistema	Numerosos programas maliciosos llevan a cabo acciones en procesos integrados de Windows. Entre estas acciones se pueden incluir terminar o modificar procesos en ejecución.
Nuevo programa de inicio	Las aplicaciones maliciosas suelen añadir o modificar entradas de inicio automático en el registro de Windows para iniciarse automáticamente cada vez que el ordenador arranca.

Cuando la función Supervisión de eventos detecta un suceso del sistema que se esté supervisando, efectúa la acción configurada para dicho suceso.

En la siguiente tabla se muestran posibles acciones que los administradores pueden realizar en los sucesos del sistema supervisado.

TABLA 9-2. Acciones en los sucesos del sistema supervisado

ACCIÓN	DESCRIPCIÓN
Valorar	OfficeScan permite siempre los programas asociados a un suceso, pero registra la acción en los registros para su valoración. Esta es la acción predeterminada para los sucesos del sistema supervisado. **Nota** Esta opción no es compatible con la Inyección en la biblioteca del programa en sistemas de 64 bits.
Permitir	OfficeScan permite siempre los programas asociados a un suceso.
Preguntar en caso necesario	OfficeScan solicita a los usuarios que permitan o denieguen programas asociados a un suceso y que añadan dichos programas a la lista de excepciones. Si el usuario no responde una vez transcurrido un determinado periodo de tiempo, OfficeScan permite de forma automática que el programa se ejecute. El periodo de tiempo predeterminado es de 30 segundos. Para modificar el periodo de tiempo, consulte *Configuración de las opciones de supervisión de comportamiento global en la página 9-13*. **Nota** Esta opción no es compatible con la Inyección en la biblioteca del programa en sistemas de 64 bits.
Denegar	OfficeScan bloquea siempre los programas asociados a un suceso e incluye la acción en los registros. Cuando se bloquea un programa y las notificaciones están activadas, OfficeScan muestra una notificación en el equipo OfficeScan. Para obtener información detallada acerca de las notificaciones, consulte *Notificaciones de la supervisión del comportamiento para usuarios del agente de OfficeScan en la página 9-16*.

Lista de excepción de supervisión del comportamiento

La lista de excepciones de Supervisión del comportamiento contiene programas que esta función no supervisa.

- **Programas permitidos**: los programas de esta lista pueden ejecutarse. Otras funciones de OfficeScan (como la exploración basada en archivos) seguirán comprobando los programas permitidos antes de que finalmente se les permita ejecutarse.
- **Programas bloqueados**: los programas de esta lista no se pueden iniciar jamás. La función Supervisión de eventos debe estar activada para que se pueda configurar esta lista.

Configure la lista de excepciones desde la consola Web. También puede conceder a los usuarios el derecho a configurar su propia lista de excepciones desde la consola del Agente de OfficeScan. Para conocer más detalles, consulte *Privilegios de supervisión de comportamiento en la página 9-15*.

Configuración del Bloqueador de comportamientos malintencionados, la función Supervisión de eventos y la Lista de excepciones

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de la supervisión del comportamiento**.
4. Haga clic en la pestaña **Reglas**.
5. Para activar el Bloqueador de comportamientos malintencionados:
   a. Seleccione **Activar bloqueador de comportamientos malintencionados** y especifique los tipos de amenaza que se bloquearán:

- **Amenazas conocidas**: bloquea comportamientos asociados a amenazas de malware conocidas.
- **Amenazas conocidas y potenciales**: bloquea comportamientos asociados a amenazas conocidas y lleva a cabo acciones en respuesta a comportamientos potencialmente maliciosos.

b. Seleccione las funciones de protección frente al ransomware que desea activar para protegerse de las amenazas de ransomware.

- **Proteger documentos frente a modificaciones o cifrados no autorizados**: detiene posibles amenazas de ransomware y evita, de este modo, que cifren o modifiquen el contenido de los documentos.
  - **Crear automáticamente una copia de seguridad de los archivos modificados por programas sospechosos y restaurarlos**: crea copias de seguridad de los archivos que se cifran en los endpoints para evitar la pérdida de datos en caso de que OfficeScan detecte una amenaza de ransomware.

Nota

La copia de seguridad de archivos automática requiere al menos 100 MB de espacio en disco en el endpoint del agente, y solo realizará copias de seguridad de los archivos que tengan menos de 10 MB.

- **Bloquear procesos que habitualmente se asocian con ransomware**: bloquea procesos asociados con amenazas de ransomware conocidas antes de que logren cifrar o modificar documentos.
- **Activar la inspección de programas para detectar y bloquear archivos ejecutables comprometidos**: La inspección de programas supervisa los procesos y lleva a cabo enlace de API para determinar si un programa se comporta de forma inesperada. Aunque este proceso aumenta la tasa general de detecciones de archivos ejecutables comprometidos, puede afectar negativamente al rendimiento del sistema.

Consejo

La inspección de programas ofrece una mayor seguridad si selecciona **Amenazas conocidas y potenciales** en el menú desplegable **Amenazas que se bloquearán**.

Para conocer más detalles, consulte *Protección frente al ransomware en la página 9-3*.

c. En **Protección frente a explotación**, active **Finalizar programas que presenten un comportamiento anómalo asociado con ataques de explotación** para protegerse frente a programas que puedan ser explotados.

Nota

La protección frente a explotación requiere la selección de la opción **Activar la inspección de programas para detectar y bloquear archivos ejecutables comprometidos**.

Para conocer más detalles, consulte *Protección frente a explotación en la página 9-5*.

6. En la sección **Programas recién encontrados**, active **Supervisar programas recién encontrados que se han descargado a través de HTTP o aplicaciones de correo electrónico** y decida si se debe **Preguntar al usuario** antes de ejecutar el programa descargado, o bien si OfficeScan solo registrará las detecciones.

7. Defina la configuración de la función Supervisión de eventos.

   a. Seleccione **Activar Supervisión de eventos**.

   b. Elija los sucesos del sistema que desee supervisar y seleccione una acción para cada uno de los eventos seleccionados.

      Para obtener más información acerca de los sucesos y acciones del sistema supervisado, consulte *Supervisión de eventos en la página 9-6*.

8. Haga clic en la pestaña **Excepciones** para configurar las listas de excepciones.

   a. En **Escriba la ruta de archivo completa del programa**, introduzca la ruta completa del programa para aprobarlo o bloquearlo. Separe las entradas múltiples mediante punto y coma (;).

   b. Haga clic en **Agregar a la lista de permitidos** o **Agregar a lista de bloqueados**.

c. Para eliminar un programa bloqueado o permitido de la lista, haga clic en el icono de la papelera ( ) situado junto al programa.

Nota

OfficeScan acepta un máximo de 1024 programas permitidos y 1024 programas bloqueados.

9. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración de las opciones de supervisión de comportamiento global

OfficeScan aplica la configuración global del agente a todos los agentes, o bien solo a los agentes con ciertos derechos.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Configuración de seguridad**.
3. Vaya a la sección **Configuración de la supervisión del comportamiento**.
4. Configure la opción **Realizar la acción automáticamente si el usuario no responde al cabo de __ segundo(s)** como corresponda.

Esta configuración solo funciona si está activa la función Supervisión de eventos y se ha seleccionado la acción "Preguntar en caso necesario" para un suceso del sistema que se supervisa. Esta acción solicita al usuario que permita o deniegue programas asociados al suceso. Si el usuario no responde una vez transcurrido un determinado periodo de tiempo, OfficeScan permite de forma automática que el programa se ejecute.

Para conocer más detalles, consulte *Supervisión de eventos en la página 9-6*.

5. Haga clic en la pestaña **Sistema**.

6. Vaya a la sección **Configuración del servicio de software seguro certificado** y active el servicio de software seguro certificado cuando se le solicite.

   El servicio de software seguro certificado realiza consultas a los centros de datos de Trend Micro para comprobar la seguridad de un programa detectado por el bloqueador de comportamientos malintencionados, la supervisión de eventos, el cortafuegos o las exploraciones antivirus. Active el Servicio de software seguro certificado para reducir la probabilidad de detecciones de falsos positivos.

   Nota

   Asegúrese de que los Agentes de OfficeScan tengan la configuración del proxy correcta (para obtener más información, consulte *Configuración del proxy del agente de OfficeScan en la página 15-54*) antes de activar el servicio de software seguro certificado. Una configuración incorrecta del proxy, junto con una conexión intermitente a Internet, puede acarrear atrasos o fallos en la respuesta de los centros de datos de Trend Micro, lo que puede hacer que los programas que se supervisen no respondan.

   Además, los Agentes de OfficeScan que solo utilizan IPv6 no podrán realizar consultas directas a los centros de datos de Trend Micro. Con el fin de permitir que los Agentes de OfficeScan se conecten a los centros de datos de Trend Micro, se necesita un servidor proxy de doble pila que pueda convertir direcciones IP, como puede ser DeleGate.

7. Haga clic en **Guardar**.

Privilegios de supervisión de comportamiento

Si los agentes tienen derechos de supervisión del comportamiento, la opción de supervisión del comportamiento será visible en la pantalla **Configuración** de la consola del Agente de OfficeScan. Los usuarios pueden administrar su propia lista de excepciones.

FIGURA 9-1. La opción de supervisión del comportamiento de la consola del Agente de OfficeScan.

Concesión de privilegios de supervisión de comportamiento

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Derechos de supervisión del comportamiento**.
5. Seleccione **Mostrar la configuración de la supervisión de comportamiento en la consola del agente de OfficeScan**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Notificaciones de la supervisión del comportamiento para usuarios del agente de OfficeScan

OfficeScan puede mostrar un mensaje de notificación en un equipo del Agente de OfficeScan inmediatamente después de que la supervisión del comportamiento bloquee

un programa. Active el envío de mensajes de notificación y, de forma opcional, modifique el contenido del mensaje.

Habilitación del envío de mensajes de notificación

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Configuración de la supervisión del comportamiento**.
5. Seleccione **Mostrar una notificación cuando se bloquee un programa**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Modificación del contenido del mensaje de notificación

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.

2. En el menú desplegable **Tipo**, seleccione **Infracciones de la política de supervisión de comportamiento**.

3. Modifique los mensajes predeterminados en el cuadro de texto habilitado para ello.

   - Infracciones de la política de supervisión de comportamiento: escriba el mensaje que recibirán los usuarios finales cuando el Bloqueador de comportamientos malintencionados detecte una infracción de la política.
   - Programas recién encontrados: escriba el mensaje que recibirán los usuarios finales cuando el Bloqueador de comportamientos detecte un programa que no reconozca descargado mediante canales HTTP/HTTPS o de aplicaciones de correo electrónico.

4. Haga clic en **Guardar**.

Registros de supervisión del comportamiento

Los Agentes de OfficeScan registran los intentos de acceso no autorizado por parte de los programas y envían los registros al servidor. De forma predeterminada, un Agente de OfficeScan que se ejecuta de forma continua agrega registros continuamente y los envía cada 60 minutos.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de registros de supervisión del comportamiento

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de supervisión del comportamiento** o **Ver registros** > **Registros de supervisión del comportamiento**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora en la que se ha detectado el proceso no autorizado
   - Endpoint en el que se ha detectado el proceso no autorizado
   - El dominio del endpoint
   - Infracción, que es la regla de supervisión de eventos que ha infringido el proceso
   - Acción que se estaba llevando a cabo cuando se ha producido la infracción
   - Suceso, que es el tipo de objeto al que ha accedido el programa
   - Nivel de riesgo del programa no autorizado
   - Programa, que es el programa no autorizado
   - Operación, que es la acción que ha llevado a cabo el programa no autorizado
   - Objetivo, que es el proceso al que se ha accedido
   - El canal de infección en el que se originó la amenaza
6. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Configuración del programa de envío del registro de supervisión del comportamiento

Procedimiento

1. Acceda a <*carpeta de instalación del servidor*>\PCCSRV.
2. Utilice un editor de textos (p. ej. el Bloc de notas) para abrir el archivo `ofcscan.ini`.
3. Busque la cadena "`SendBMLogPeriod`" y marque el valor que aparece junto a ésta.

   El valor predeterminado es 3.600 segundos y la cadena aparece como `SendBMLogPeriod=3600`.
4. Especifique el valor en segundos.

   Por ejemplo, para cambiar el período de registro a 2 horas, cambie el valor a 7.200.
5. Guarde el archivo.
6. Vaya a **Agentes** > **Configuración global para los agentes**.
7. Haga clic en **Guardar** sin realizar ningún cambio en la configuración.
8. Reinicie el agente.

Capítulo 10

Uso del Control de dispositivos

En este capítulo se describe cómo proteger los ordenadores frente a riesgos de seguridad mediante la función Control de dispositivos.

Los temas que se incluyen son:

- *Control de dispositivos en la página 10-2*
- *Permisos para dispositivos de almacenamiento en la página 10-4*
- *Permisos para dispositivos sin almacenamiento en la página 10-11*
- *Modificación de las notificaciones de Control de dispositivos en la página 10-19*
- *Registros de control de dispositivos en la página 10-19*

Control de dispositivos

Control de dispositivos regula el acceso a los dispositivos de almacenamiento externo y a los recursos de red conectados a los equipos. El control de dispositivos ayuda a evitar la pérdida y la fuga de datos y, junto con la exploración de archivos, ayuda a protegerse frente a los riesgos de seguridad.

Puede configurar las políticas del control de dispositivos para agentes internos y externos. Los administradores de OfficeScan suelen aplicar políticas más restrictivas a los agentes externos.

Las políticas constituyen una configuración granular en el árbol de agentes de OfficeScan. Puede aplicar determinadas políticas a grupos de agentes o a agentes individuales. También puede aplicar una única política a todos los agentes.

Después de implementar las políticas, los agentes utilizan los criterios de ubicación que haya definido en la pantalla **Ubicación del Endpoint** (consulte *Ubicación del Endpoint en la página 15-2*) para determinar sus ubicaciones y la política que se va a aplicar. Los agentes cambian de política cada vez que cambia la ubicación.

Importante

- De forma predeterminada, el control de dispositivos está desactivado en todas las versiones de Windows Server 2003, Windows Server 2008, Windows Server 2012 y Windows Server 2016. Antes de activar el control de dispositivos en estas plataformas del servidor, lea las directrices y prácticas recomendadas que se describen en *Servicios del agente de OfficeScan en la página 15-7*.
- Para obtener una lista de los modelos de dispositivos compatibles, consulte el documento *Listas de protección de datos* en:

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Los tipos de dispositivos que OfficeScan puede supervisar dependen de que esté activada la licencia de protección de datos. La protección de datos es un módulo con licencia individual y se ha de activar antes de poder utilizarse. Para obtener información detallada acerca de la licencia de protección de datos, consulte *Licencia de protección de datos en la página 3-4*.

TABLA 10-1. Dispositivos que supervisa el Servicio de prevención de cambios no autorizados

TIPO DE DISPOSITIVO	DESCRIPCIÓN DEL DISPOSITIVO
Dispositivos de almacenamiento	CD/DVD **Importante** El control de dispositivos solo puede limitar el acceso de dispositivos de grabación de CD/DVD que usan el formato del sistema de archivos LFS. Algunas aplicaciones de otros fabricantes que usan Master Format pueden realizar operaciones de lectura o escritura incluso cuando el control de dispositivos está activado. Utilice la prevención de pérdida de datos para limitar el acceso de dispositivos de grabación de CD/DVD que usan cualquier tipo de formato. Para conocer más detalles, consulte *Bloqueo de acceso a grabadores de datos (CD/DVD) en la página 11-36*.
	Disquetes
	Unidades de red
	Dispositivos de almacenamiento USB

TABLA 10-2. Dispositivos que supervisa la prevención de pérdida de datos

TIPO DE DISPOSITIVO	DESCRIPCIÓN DEL DISPOSITIVO
Dispositivos móviles	Dispositivos móviles
Dispositivos de almacenamiento	CD/DVD
	Disquetes
	Unidades de red
	Dispositivos de almacenamiento USB

Tipo de dispositivo	Descripción del dispositivo
Dispositivos sin almacenamiento	Adaptadores Bluetooth
	Puertos COM y LPT
	Interfaz IEEE 1394
	Dispositivos de imagen
	Dispositivos infrarrojo
	Módems
	Tarjeta PCMCIA
	Llave de impresión de pantalla
	NIC inalámbricas

Permisos para dispositivos de almacenamiento

Los permisos de Control de dispositivos para dispositivos de almacenamiento se utilizan cuando:

- Permite el acceso a dispositivos USB de almacenamiento, CD/DVD, disquetes y unidades de red. Puede conceder el acceso total a estos dispositivos o limitar el nivel de acceso.
- Configure la lista de dispositivos USB de almacenamiento permitidos. La función Control de dispositivos le permite bloquear el acceso a todos los dispositivos USB de almacenamiento, excepto a aquellos que se hayan agregado a lista de dispositivos permitidos. Puede conceder el acceso total a los dispositivos permitidos o limitar el nivel de acceso.

En la siguiente tabla se muestran los permisos para los dispositivos de almacenamiento.

TABLA 10-3. Permisos de Control de dispositivos para dispositivos de almacenamiento

PERMISOS	ARCHIVOS DEL DISPOSITIVO	ARCHIVOS ENTRANTES
Acceso completo	Operaciones permitidas: copiar, mover, abrir, guardar, eliminar y ejecutar	Operaciones permitidas: guardar, mover y copiar Esto significa que un archivo se puede guardar, mover y copiar en el dispositivo.
Modificar	Operaciones permitidas: copiar, mover, abrir, guardar y eliminar Operaciones prohibidas: ejecutar	Operaciones permitidas: guardar, mover y copiar
Leer y ejecutar	Operaciones permitidas: copiar, abrir y ejecutar Operaciones prohibidas: guardar, mover y eliminar	Operaciones prohibidas: guardar, mover y copiar
Leer	Operaciones permitidas: copiar y abrir Operaciones prohibidas: guardar, mover, eliminar y ejecutar	Operaciones prohibidas: guardar, mover y copiar
Enumerar solo contenido del dispositivo	Operaciones prohibidas: todas El dispositivo y los archivos que este contiene están visibles para el usuario (por ejemplo, desde el Explorador de Windows).	Operaciones prohibidas: guardar, mover y copiar
Bloquear (disponible tras activar la protección de datos)	Operaciones prohibidas: todas Ni el dispositivo ni los archivos que este contiene están visibles para el usuario (por ejemplo, desde el Explorador de Windows).	Operaciones prohibidas: guardar, mover y copiar

La función de exploración basada en archivos de OfficeScan complementa y puede invalidar los permisos de los dispositivos. Por ejemplo, si el permiso permite que se abra un archivo pero OfficeScan detecta que está infectado con malware, se llevará a cabo una acción de exploración específica sobre el archivo con el fin de eliminar el malware. Si la acción de exploración es limpiar, el archivo se abrirá una vez se haya limpiado. Sin embargo, si la acción es eliminar, el archivo se eliminará.

Consejo

El control de dispositivos para la protección de datos es compatible con todas las plataformas de 64 bits. Para la supervisión de la prevención de cambios no autorizados en sistemas con los que OfficeScan no es compatible, establezca el permiso en **Bloquear** para limitar el acceso a esos dispositivos.

Permisos avanzados para dispositivos de almacenamiento

Los permisos avanzados son aplicables cuando se conceden permisos limitados a la mayoría de dispositivos de almacenamiento. El permiso puede ser alguno de los siguientes:

- **Modificar**
- **Leer y ejecutar**
- **Leer**
- **Enumerar solo contenido del dispositivo**

Puede mantener limitados los permisos pero conceder permisos avanzados a determinados programas en los dispositivos de almacenamiento y en el endpoint local.

Para definir programas, configure las siguientes listas de programas.

TABLA 10-4. Listas de programas

LISTA DE PROGRAMAS	DESCRIPCIÓN	ENTRADAS VÁLIDAS
Programas con acceso de lectura y escritura en los dispositivos	Esta lista contiene programas locales y programas en dispositivos de almacenamiento que disponen de acceso de lectura y escritura a los dispositivos. Un ejemplo de programa local es Microsoft Word (`winword.exe`), que suele encontrarse en `C:\Archivos de programa\Microsoft Office\Office`. Si el permiso para los dispositivos de almacenamiento USB es "Enumerar solo contenido del dispositivo", pero "`C:\Archivos de programa\Microsoft Office\Office\winword.exe`" está incluido en esta lista: • El usuario tendrá acceso de lectura y escritura a los archivos del dispositivo de almacenamiento USB que se puedan abrir con Microsoft Word. • El usuario podrá guardar, mover o copiar un archivo de Microsoft Word en el dispositivo de almacenamiento USB.	Ruta y nombre de programa Para conocer más detalles, consulte *Especificación de una ruta y nombre de programa en la página 10-9*.
Programas de los dispositivos con permiso de ejecución	Esta lista contiene los programas en los dispositivos de almacenamiento que los usuarios o el sistema pueden ejecutar. Por ejemplo, si desea permitir a los usuarios instalar software desde un CD, agregue la ruta y el nombre del programa de instalación como, por ejemplo, "`E:\InstallerSetup.exe`", a esta lista.	Ruta y nombre de programa o proveedor de firmas digitales Para conocer más detalles, consulte *Especificación de una ruta y nombre de programa en la página 10-9* o *Especificación de un proveedor de firmas digitales en la página 10-8*.

Hay instancias cuando se necesita agregar un programa a ambas listas. Considere la función de bloqueo de datos en un dispositivo de almacenamiento USB que, si se activa, solicita a los usuarios un nombre de usuario válido y una contraseña antes de poder desbloquear el dispositivo. La función de bloqueo de datos utiliza un programa en el dispositivo denominado "`Password.exe`", cuya ejecución se debe permitir para que los usuarios puedan desbloquear el dispositivo correctamente. "`Password.exe`" también debe disponer de acceso de lectura y escritura al dispositivo para que los usuarios puedan cambiar el nombre de usuario o la contraseña.

Cada lista de programas de la interfaz de usuario puede contener hasta 100 programas.

Si desea agregar más programas a una lista de programas, tendrá que agregarlos al archivo `ofcscan.ini`, que tiene cabida para 1.000 programas como máximo. Para obtener instrucciones sobre cómo agregar programas al archivo `ofcscan.ini`, consulte *Adición de programas a las listas de control de dispositivos mediante ofcscan.ini en la página 10-17*.

¡ADVERTENCIA!

Los programas agregados al archivo `ofcscan.ini` se implementarán en el dominio raíz y sobrescribirán programas en agentes y dominios individuales.

Especificación de un proveedor de firmas digitales

Especifique un proveedor de firmas digitales si confía en programas publicados por el proveedor. Por ejemplo, escriba Microsoft Corporation o Trend Micro, Inc. Puede obtener el proveedor de firmas digitales comprobando las propiedades de un programa

(por ejemplo, haciendo clic con el botón derecho en el programa y seleccionando **Propiedades**).

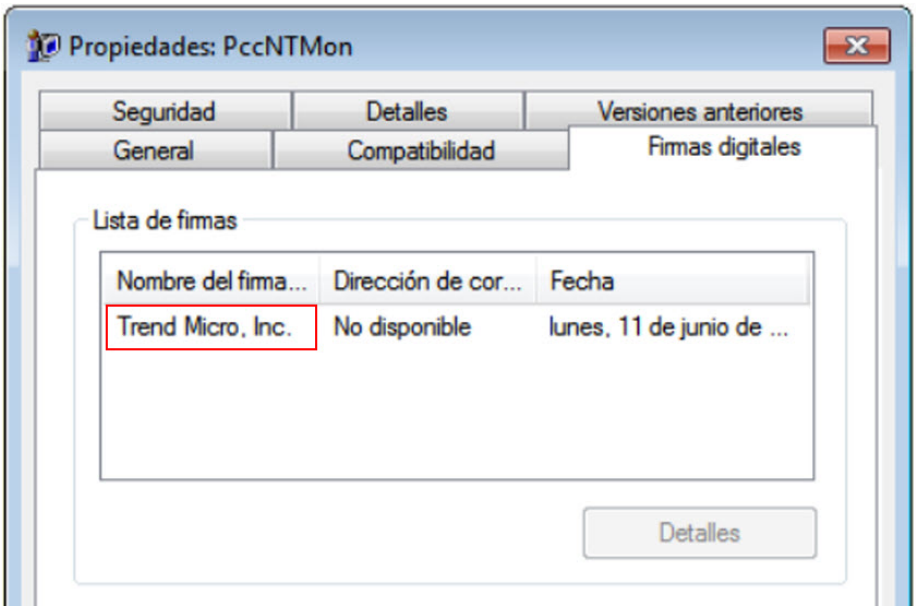


FIGURA 10-1. Proveedor de firmas digitales para el programa del Agente de OfficeScan (`PccNTMon.exe`)

Especificación de una ruta y nombre de programa

El nombre y la ruta de programa deben tener 259 caracteres como máximo y solo pueden contener caracteres alfanuméricos (A-Z, a-z, 0-9). No es posible especificar solo el nombre del programa.

Puede usar comodines en lugar de letras de unidad y nombres de programas. Puede utilizar un signo de interrogación (?) para representar datos de un solo carácter, como por ejemplo la letra de una unidad. Utilice un asterisco (*) para representar datos de varios caracteres, como por ejemplo el nombre de un programa.

Nota

No se pueden utilizar comodines para representar nombres de carpeta. Se debe especificar el nombre exacto de una carpeta.

Los comodines se utilizan correctamente en los ejemplos siguientes:

TABLA 10-5. Uso correcto de comodines

EJEMPLO	DATOS COINCIDENTES
?:\Password.exe	El archivo "Password.exe" ubicado directamente en cualquier unidad
C:\Archivos de programa \Microsoft*.exe	Cualquier archivo en C:\Archivos de programa que tenga una extensión de archivo
C:\Archivos de programa*.*	Cualquier archivo en C:\Archivos de programa que tenga una extensión de archivo
C:\Archivos de programa\a**?** c.exe	Cualquier archivo .exe en C:\Archivos de programa que tenga 3 caracteres empezando por la letra "a" y terminando por la letra "c"
C:*	Cualquier archivo ubicado directamente en la unidad C:\ con o sin extensiones de archivo

Los comodines se utilizan incorrectamente en los ejemplos siguientes:

TABLA 10-6. Uso incorrecto de comodines

EJEMPLO	MOTIVO
??:\Buffalo\Password.exe	?? representa dos caracteres y las letras de unidad solo tienen un único carácter alfabético.
***:\Buffalo\Password.exe	* representa datos de varios caracteres y las letras de unidad solo tienen un único carácter alfabético.
C:*\Password.exe	No se pueden utilizar comodines para representar nombres de carpeta. Se debe especificar el nombre exacto de una carpeta.
C:**?**\Password.exe	

Permisos para dispositivos sin almacenamiento

Puede permitir o bloquear el acceso a dispositivos sin almacenamiento. No hay permisos granulares o avanzados para estos dispositivos.

Administración del acceso a dispositivos externos (protección de datos activada)

Procedimiento

1. Desplácese hasta **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de Control de dispositivos**.
4. Haga clic en la pestaña **Agentes externos** para definir la configuración de los agentes externos o en la pestaña **Agentes internos** para definir la configuración de los clientes internos.
5. Seleccione **Activar Control de dispositivos**.
6. Aplique la siguiente configuración:

    - En el caso de que se encuentre en la pestaña **Agentes externos**, puede aplicar la configuración a los agentes internos si selecciona **Aplicar la configuración a los agentes internos**.
    - En el caso de que se encuentre en la pestaña **Agentes internos**, puede aplicar la configuración de acción a los agentes externos si selecciona **Aplicar la configuración a los agentes externos**.

    Aparecerá un mensaje de confirmación. Deje que transcurra algún tiempo para que el comando de implementación se propague a todos los agentes.

7. Seleccione si desea bloquear o permitir la función de ejecución automática (`autorun.inf`) en los dispositivos de almacenamiento USB.

8. Definir la configuración para dispositivos de almacenamiento.

   a. Seleccione un permiso para cada dispositivo de almacenamiento.

      Para obtener información detallada acerca de los permisos, consulte *Permisos para dispositivos de almacenamiento en la página 10-4*.

   b. Si el permiso para dispositivos de almacenamiento USB es **Bloquear**, configure una lista de dispositivos permitidos. Los usuarios pueden acceder a estos dispositivos y usted puede controlar el nivel de acceso mediante los permisos.

      Consulte el apartado *Configuración de una lista de dispositivos USB permitidos en la página 10-13*.

9. Para dispositivos sin almacenamiento, seleccione **Permitir** o **Bloquear**.

10. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

    - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
    - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración de los permisos avanzados

Aunque puede configurar notificaciones y permisos avanzados para un dispositivo de almacenamiento específico en la interfaz de usuario, los permisos y notificaciones se aplican realmente a todos los dispositivos de almacenamiento. Esto significa que cuando se hace clic en **Permisos avanzados y notificaciones** para CD/DVD, realmente está definiendo permisos y notificaciones para todos los dispositivos de almacenamiento.

Nota

Para obtener más información sobre los permisos avanzados y cómo definir programas correctamente con permisos avanzados, consulte *Permisos avanzados para dispositivos de almacenamiento en la página 10-6*.

Procedimiento

1. Haga clic en **Permisos avanzados y notificaciones**.

   Se abrirá una nueva pantalla.

2. Debajo de **Programas con acceso de lectura y escritura a los dispositivos de almacenamiento**, escriba un nombre de archivo y una ruta de programa y, a continuación, haga clic en **Agregar**.

   No se acepta el proveedor de firmas digitales.

3. Debajo de **Programas de los dispositivos de almacenamiento con permiso de ejecución**, escriba el nombre y la ruta del programa o el proveedor de firmas digitales y, a continuación, haga clic en **Agregar**.

4. Seleccione **Mostrar un mensaje de notificación en el endpoint cuando OfficeScan detecte un acceso no autorizado al dispositivo**.

   - El acceso no autorizado al dispositivo se refiere a operaciones del dispositivo prohibidas. Por ejemplo, si el permiso del dispositivo es "Lectura", los usuarios no podrán guardar, mover, eliminar ni ejecutar un archivo en el dispositivo.
   - Puede modificar el mensaje de notificación. Para conocer más detalles, consulte *Modificación de las notificaciones de Control de dispositivos en la página 10-19*.

5. Haga clic en **Atrás**.

Configuración de una lista de dispositivos USB permitidos

La lista dispositivos USB permitidos es compatible con el uso del asterisco (*) como comodín. Sustituya cualquier campo con el asterisco (*) para incluir todos los

dispositivos que cumplan con los otros campos. Por ejemplo, [proveedor]-[modelo]-* coloca todos los dispositivos USB del proveedor específico y del tipo de modelo específico, independientemente del ID de serie, en la lista permitida.

Procedimiento

1. Haga clic en **Dispositivos permitidos**
2. Escriba el nombre del proveedor de dispositivos.
3. Escriba el modelo de dispositivo y el ID de serie.

Consejo

Utilice la herramienta de lista de dispositivos para realizar consultas en los dispositivos que estén conectados a Endpoints. La herramienta proporciona el distribuidor, el modelo y el ID de serie de cada dispositivo.

4. Seleccione el permiso para el dispositivo.

   Para obtener información detallada acerca de los permisos, consulte *Permisos para dispositivos de almacenamiento en la página 10-4*.

5. Para agregar más dispositivos, haga clic en el icono **+**.
6. Haga clic en **< Atrás**.

Herramienta de lista de dispositivos

Ejecute la herramienta de lista de dispositivos localmente en cada endpoint para realizar consultas en los dispositivos externos que estén conectados al endpoint. La herramienta explora un endpoint en busca de dispositivos externos y, después, muestra información del dispositivo en una ventana del explorador. Puede utilizar la información al configurar los parámetros del dispositivo para la prevención de pérdida de datos y Control de dispositivos.

Ejecución de la herramienta de lista de Dispositivo

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a <*Carpeta de instalación del servidor en la página xviii*>`\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Copie `listDeviceInfo.exe` en el endpoint de destino.
3. En el endpoint, ejecute `listDeviceInfo.exe`.
4. Vea la información del dispositivo que muestra la ventana del navegador. El servicio de prevención de pérdida de datos y el Control de dispositivos utilizan la siguiente información:
   - Proveedor (necesario)
   - Modelo (opcional)
   - ID de serie (opcional)

Administración del acceso a dispositivos externos (protección de datos no activada)

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de Control de dispositivos**.
4. Haga clic en la pestaña **Agentes externos** para definir la configuración de los agentes externos o en la pestaña **Agentes internos** para definir la configuración de los clientes internos.
5. Seleccione **Activar Control de dispositivos**.

6. Aplique la siguiente configuración:

   - En el caso de que se encuentre en la pestaña **Agentes externos**, puede aplicar la configuración a los agentes internos si selecciona **Aplicar la configuración a los agentes internos**.
   - En el caso de que se encuentre en la pestaña **Agentes internos**, puede aplicar la configuración de acción a los agentes externos si selecciona **Aplicar la configuración a los agentes externos**.

   Aparecerá un mensaje de confirmación. Deje que transcurra algún tiempo para que el comando de implementación se propague a todos los agentes.

7. Seleccione si desea bloquear o permitir la función de ejecución automática (`autorun.inf`) en los dispositivos de almacenamiento USB.

8. Seleccione un permiso para cada dispositivo de almacenamiento.

9. Configure las notificaciones y los permisos avanzados si el permiso de un dispositivo de almacenamiento es alguno de los siguientes: **Modificar**, **Leer y ejecutar**, **Leer** o **Enumerar solo contenido del dispositivo**.

   Consulte el apartado *Configuración de los permisos avanzados en la página 10-12*.

10. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

    - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
    - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Adición de programas a las listas de Control de dispositivos mediante ofcscan.ini

Nota

Para obtener información detallada acerca de las listas de programas y cómo definir correctamente programas que se puedan agregar a las listas, consulte *Permisos avanzados para dispositivos de almacenamiento en la página 10-6*.

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a *carpeta de instalación del servidor*> `\PCCSRV`.
2. Abra el archivo `ofcscan.ini` con un editor de texto.
3. Para agregar programas con acceso de lectura y escritura a los dispositivos de almacenamiento:
   a. Localice las siguientes líneas:

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. Sustituya "x" por el número de programas en la lista de programas.
   c. Debajo de Count=x, agregue programas escribiendo lo siguiente:

      ```
      Item<number>=<ruta y nombre de programa o proveedor de firmas digitales>
      ```

      Por ejemplo:

      ```
      [DAC_APPROVED_LIST]

      Count=3

      Item0=C:\Program Files\program.exe

      Item1=?:\password.exe

      Item2=Microsoft Corporation
      ```

4. Para agregar programas de los dispositivos de almacenamiento con permiso de ejecución:

   a. Localice las siguientes líneas:

      ```
      [DAC_EXECUTABLE_LIST]

      Count=x
      ```

   b. Sustituya "x" por el número de programas en la lista de programas.

   c. Debajo de Count=x, agregue programas escribiendo lo siguiente:

      ```
      Item<number>=<ruta y nombre de programa o proveedor de
      firmas digitales>
      ```

      Por ejemplo:

      ```
      [DAC_EXECUTABLE_LIST]

      Count=3

      Item0=?:\Installer\Setup.exe

      Item1=E:\*.exe

      Item2=Trend Micro, Inc.
      ```

5. Guarde y cierre el archivo `ofcscan.ini`.

6. Abra la consola Web de OfficeScan y vaya a **Agentes** > **Configuración global para los agentes**.

7. Haga clic en **Guardar** para implementar las listas de programas en todos los agentes.

Modificación de las notificaciones de Control de dispositivos

Cuando se produzcan infracciones de Control de dispositivos, se mostrarán mensajes de notificación en los Endpoints. Los administradores pueden modificar, en caso de que sea necesario, el mensaje de notificación predeterminado.

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. En el menú desplegable **Tipo**, seleccione **Infracción del control de dispositivos**.
3. Modifique los mensajes predeterminados en el cuadro de texto habilitado para ello.
4. Haga clic en **Guardar**.

Registros de control de dispositivos

Los Agentes de OfficeScan registran los intentos de acceso no autorizado por parte de los dispositivos y envían los registros al servidor. Un agente que se ejecuta de forma continua agrega los registros y los envía cada hora. Un agente que se ha reiniciado comprueba cuándo fue la última vez que se enviaron los registros al servidor. Si ha transcurrido más de una hora, el agente envía los registros en ese mismo instante.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de los registros de Control de dispositivos

Nota

Solo los intentos para acceder a los **dispositivos de almacenamiento** generan datos de registro. Los Agentes de OfficeScan bloquean o permiten el acceso a los **dispositivos sin almacenamiento** según la configuración, pero no registran las acciones.

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de Control de dispositivos** o **Ver registros** > **Registros de control de dispositivos**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora en la que se ha detectado el acceso no autorizado
   - Endpoint al que se conectan los dispositivos externos o donde se asignan los recursos de red
   - Dominio del endpoint al que se conectan los dispositivos externos o donde se asignan los recursos de red
   - Tipo de dispositivo o recurso de red al que se puede acceder
   - Objetivo, que es el elemento del dispositivo o del recurso de red al que se ha podido acceder
   - Origen, donde se especifica desde dónde se ha iniciado el acceso
   - Permisos establecidos para el destino

6. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Capítulo 11

Uso de la Prevención de pérdida de datos

En este capítulo se describe cómo utilizar la función de la Prevención de pérdida de datos.

Los temas que se incluyen son:

- *Acerca de la prevención de pérdida de datos (DLP) en la página 11-2*
- *Políticas de prevención de pérdida de datos en la página 11-3*
- *Tipos de identificadores de datos en la página 11-6*
- *Plantillas de prevención de pérdida de datos en la página 11-21*
- *Canales de la DLP en la página 11-26*
- *Acciones de la prevención de pérdida de datos en la página 11-41*
- *Excepciones de la prevención de pérdida de datos en la página 11-44*
- *Configuración de las políticas de prevención de pérdida de datos en la página 11-50*
- *Notificaciones de la prevención de pérdida de datos en la página 11-56*
- *Registros de prevención de pérdida de datos en la página 11-60*

Acerca de la prevención de pérdida de datos (DLP)

Las soluciones de seguridad tradicionales se centran en evitar que las amenazas de seguridad externas lleguen a la red. En los entornos de seguridad actuales, eso es solo una parte del problema. El acceso no autorizado a datos se ha convertido en algo común, por lo que los datos confidenciales de una organización (lo que se conoce como activos digitales) quedan expuestos a terceras partes no autorizadas. El acceso no autorizado a datos puede producirse a raíz de un error o descuido de un empleado interno, la externalización de datos, el robo o la pérdida de dispositivos informáticos o ataques malintencionados.

Las infracciones de seguridad pueden:

- Dañar la reputación de la marca
- Mermar la confianza del cliente en la organización
- Acarrear costes innecesarios con los que cubrir la solución y pagar sanciones por infringir las normativas de conformidad
- Provocar pérdidas de oportunidades empresariales e ingresos cuando haya robos de propiedad intelectual

Dada la prevalencia y los dañinos efectos de las infracciones de seguridad, las organizaciones ven ahora la protección de archivos digitales como un componente crítico en su infraestructura de seguridad.

El servicio de prevención de pérdida de datos protege los datos confidenciales de la organización frente a fugas accidentales o intencionadas. La prevención de pérdida de datos le permite:

- Identificar la información confidencial que requiera protección mediante los identificadores de datos.
- Crear políticas que limiten o eviten la transmisión de activos digitales a través de canales de transmisión frecuentes, tales como mensajes de correo electrónico y dispositivos externos.
- Aplicar la conformidad a estándares de privacidad establecidos

Antes de poder supervisar la información confidencial en busca de pérdidas potenciales, debe poder responder a las preguntas siguientes:

- ¿Qué datos necesitan protección frente a usuarios no autorizados?
- ¿Dónde residen los datos confidenciales?
- ¿Cómo de transmiten los datos confidenciales?
- ¿Qué usuarios están autorizados a acceder a los datos confidenciales o a transmitirlos?
- ¿Qué acción se debe llevar a cabo si se produce una infracción de seguridad?

Esta importante auditoría implica normalmente a varios departamentos y personal familiarizado con la información confidencial en la organización.

Si ya ha definido las políticas de seguridad e información confidencial, puede comenzar a definir los identificadores de datos y las políticas de empresa.

Políticas de prevención de pérdida de datos

OfficeScan evalúa un archivo o dato en relación con un conjunto de reglas definido en las políticas de DLP. Las políticas determinan qué archivos o datos necesitan protegerse frente a transmisiones sin autorización, así como la acción que OfficeScan llevará a cabo después de detectar dichas transmisiones.

Nota

OfficeScan no supervisa las transmisiones de datos entre el servidor y los Agentes de OfficeScan.

OfficeScan permite a los administradores configurar políticas para Agentes de OfficeScan internos y externos. Los administradores suelen configurar una política más estricta para los agentes externos.

Los administradores pueden aplicar determinadas políticas a grupos de agentes o a agentes individuales.

Después de implementar las políticas, los agentes utilizan los criterios de ubicación que se han definido en la pantalla **Ubicación del Endpoint** (consulte *Ubicación del Endpoint en la página 15-2*) para determinar la configuración de ubicación correcta y la política que se debe aplicar. Los agentes cambian de política cada vez que cambia la ubicación.

Configuración de políticas

Para definir las políticas de DLP, configure las siguientes opciones e implemente la configuración en los agentes seleccionados:

TABLA 11-1. Configuración que define una política de DLP

CONFIGURACIÓN	DESCRIPCIÓN
Reglas	Una regla de DLP puede consistir en varias plantillas, canales y acciones. Cada regla es un subconjunto de la política de DLP que la abarca. **Nota** La prevención de pérdida de datos procesa las reglas y las plantillas según su prioridad. Si una regla está establecida en «Omitir», la prevención de pérdida de datos procesará la siguiente regla de la lista. Si una regla está establecida en «Bloquear» o «Justificación del usuario», la prevención de pérdida de datos bloquea o acepta la acción del usuario y no procesa esta regla o esa plantilla.

Configuración	Descripción
Plantillas	Una plantilla de DLP combina identificadores de datos y operadores lógicos (Y, O, Excepto) para formar condiciones. Solo los archivos o los datos que cumplan con una determinada condición están sujetos a una regla de DLP. La prevención de pérdida de datos incluye un conjunto de plantillas predefinidas y permite que los administradores creen plantillas personalizadas. Una regla de DLP puede contener una o varias plantillas. La prevención de pérdida de datos utiliza la regla de primera coincidencia al comprobar las plantillas. Esto significa que si un archivo o unos datos coinciden con los identificadores de datos en una plantilla, la prevención de pérdida de datos no seguirá comprobando las demás.
Canales	Los canales son entidades que transmiten información confidencial. La prevención de pérdida de datos admite canales de transmisión populares tales como correo electrónico, dispositivos de almacenamiento extraíbles y aplicaciones de mensajería instantánea.
Acciones	La prevención de pérdida de datos realiza una o varias acciones cuando detecta un intento de transmitir información confidencial mediante cualquiera de los canales.
Excepciones	Las excepciones actúan como reemplazos a las reglas DLP configuradas. Configure las excepciones para administrar los destinos no supervisados, los destinos supervisados y la exploración de archivos comprimidos.
Identificadores de datos	La prevención de pérdida de datos utiliza los identificadores de datos para detectar información confidencial. Entre los identificadores de datos se incluyen expresiones, atributos de archivo y palabras clave que actúan como bloques de construcción para las plantillas de DLP.

Tipos de identificadores de datos

Los activos digitales son archivos y datos que una organización debe proteger de las transmisiones sin autorización. Los administradores pueden definir los activos digitales mediante los siguientes identificadores de datos:

- **Expresiones** datos que tienen una determinada estructura.

  Para conocer más detalles, consulte *Expresiones en la página 11-6*.

- **Atributos de archivos**: propiedades de los archivos, como el tipo o el tamaño.

  Para conocer más detalles, consulte *Atributos de archivo en la página 11-11*.

- **Listas de palabras clave**: una lista de palabras o frases especiales.

  Para conocer más detalles, consulte *Palabras clave en la página 11-15*.

Nota

Los administradores no pueden eliminar los identificadores de datos que utilizan las plantillas de DLP. Elimine la plantilla antes de eliminar el identificador de datos.

Expresiones

Una expresión hace referencia a datos con una determinada estructura. Por ejemplo, los números de tarjetas de crédito suelen tener 16 dígitos con el formato "nnnn-nnnn-nnnn-nnnn", lo que los hace apropiados para detecciones basadas en expresiones.

Los administradores pueden utilizar expresiones predefinidas y personalizadas.

Para conocer más detalles, consulte *Expresiones predefinidas en la página 11-6* y *Expresiones personalizadas en la página 11-7*.

Expresiones predefinidas

La prevención de pérdida de datos incluye un conjunto de expresiones predefinidas. Estas expresiones no se pueden modificar ni eliminar.

La prevención de pérdida de datos comprueba estas expresiones utilizando coincidencia de patrones y ecuaciones matemáticas. Una vez que la prevención de pérdida de datos asigna datos potencialmente confidenciales a una expresión, los datos también se pueden someter a comprobaciones de verificación adicionales.

Para ver la lista completa de expresiones predefinidas, consulte el documento *Listas de protección de datos* en http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Visualización de la configuración de las expresiones predefinidas

Nota

Las expresiones predefinidas no se pueden modificar ni eliminar.

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.
2. Haga clic en la pestaña **expresión**.
3. Haga clic en el nombre de la expresión.
4. Vea la configuración en la pantalla que se abre.

Expresiones personalizadas

Cree expresiones personalizadas si no hay ninguna expresión predefinida que satisfaga las necesidades de la empresa.

Las expresiones son una poderosa herramienta de coincidencia de cadenas. Familiarícese con la sintaxis de expresiones antes de crearlas. Una expresión escrita incorrectamente puede tener nefastos resultados en el rendimiento.

Al crear expresiones:

- Consulte las expresiones predefinidas a modo de guía para ver cómo definir expresiones válidas. Si, por ejemplo, desea crear una expresión que incluya una fecha, consulte las expresiones con el prefijo "Date".
- Tenga en cuenta que la prevención de pérdida de datos permite los formatos de expresión definidos en Perl Compatible Regular Expressions (PCRE). Para obtener más información sobre PCRE, visite el siguiente sitio Web:

  http://www.pcre.org/
- Comience con expresiones sencillas. Modifique las expresiones que causen falsas alarmas o ajústelas con mayor precisión para mejorar las detecciones.

Existen varios criterios entre los que puede elegir un administrador a la hora de crear expresiones. Una expresión debe cumplir los criterios que escoja antes de que la prevención de pérdida de datos la supedite a una política de DLP. Para obtener información detallada acerca de las distintas opciones de criterios, consulte *Criterios para las expresiones personalizadas en la página 11-8*.

Criterios para las expresiones personalizadas

TABLA 11-2. Opciones de criterios para las expresiones personalizadas

CRITERIOS	REGLA	EJEMPLO
Ninguna	Ninguna	Todo - Nombres de la Oficina del Censo estadounidense • Expresión: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Caracteres específicos	Una expresión debe incluir los caracteres que haya especificado. Además, el número de caracteres de la expresión debe hallarse dentro de los límites mínimo y máximo.	EE.UU. - Número de enrutamiento ABA • Expresión: [^\d]([0123678]\d{8})[^\d] • Caracteres: 0123456789 • Número mínimo de caracteres: 9 • Número máximo de caracteres: 9

Criterios	Regla	Ejemplo
Sufijo	El sufijo hace referencia al último segmento de una expresión. Un sufijo debe incluir los caracteres que se hayan especificado y contener un determinado número de estos. Además, el número de caracteres de la expresión debe hallarse dentro de los límites mínimo y máximo.	Todo - Dirección particular • Expresión: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] • Caracteres del sufijo: 0123456789- • Número de caracteres: 5 • Número mínimo de caracteres en la expresión: 25 • Número máximo de caracteres en la expresión: 80
Separador de caracteres	Una expresión debe tener dos segmentos separados por un carácter. El carácter debe tener 1 byte de longitud. Además, el número de caracteres a la izquierda del separador debe hallarse dentro de los límites mínimo y máximo. El número de caracteres a la derecha del separador no debe exceder el límite máximo.	Todo - Dirección de correo electrónico • Expresión: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separador: @ • Número mínimo de caracteres a la izquierda: 3 • Número máximo de caracteres a la izquierda: 15 • Número máximo de caracteres a la derecha: 30

Creación de una expresión personalizada

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.

2. Haga clic en la pestaña **expresión**.
3. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.
4. Escriba un nombre para la expresión. El nombre no debe tener más de 100 bytes de longitud ni contener los siguientes caracteres:

   - > < * ^ | & ? \ /
5. Escriba una descripción que no supere los 256 bytes de longitud.
6. Escriba los datos mostrados.

   Si, por ejemplo, está creando una expresión para números de ID, escriba un número de ID de ejemplo. Este dato se utiliza únicamente como referencia y no aparecerá en ningún otro lugar en el producto.
7. Escoja uno de los siguientes criterios y defina la configuración adicional para los criterios elegidos (consulte *Criterios para las expresiones personalizadas en la página 11-8*):

   - Ninguna
   - Caracteres específicos
   - Sufijo
   - Separador de caracteres
8. Contraste la expresión con datos reales.

   Si, por ejemplo, la expresión es para un ID nacional, escriba un número de ID válido en el cuadro de texto **Datos de prueba**, haga clic en **Probar** y, después, compruebe el resultado.
9. Haga clic en **Guardar** si está de acuerdo con el resultado.

Nota

Guarde la configuración únicamente si la prueba se realizó de modo correcto. Una expresión que no puede detectar datos desperdicia recursos del sistema y puede afectar al rendimiento del sistema.

10. Aparece un mensaje que le recuerda que debe implementar la configuración en los agentes. Haga clic en **Cerrar**.

11. Al volver a la pantalla **Identificadores de datos de DLP**, haga clic en **Aplicar a todos los agentes**.

Importación de expresiones personalizadas

Utilice esta opción si cuenta con un archivo `.dat` que tenga el formato correcto y contenga las expresiones. Para generar el archivo, puede exportar las expresiones desde el servidor al cual esté accediendo o desde otro servidor.

Nota

Los archivos de expresiones `.dat` generados por esta versión de la prevención de pérdida de datos no son compatibles con las versiones anteriores.

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.
2. Haga clic en la pestaña **expresión**.
3. Haga clic en **Importar** y, a continuación, encuentre el archivo `.dat` que contenga las expresiones.
4. Haga clic en **Abrir**.

   Aparecerá un mensaje en el que se le informará de que la importación se realizó correctamente. Si la expresión que se va a importar ya existe, esta se omitirá.
5. Haga clic en **Aplicar a todos los agentes**.

Atributos de archivo

Los atributos de archivo son propiedades específicas del mismo. Puede utilizar dos atributos de archivo al definir identificadores de datos; a saber: tipo de archivo y tamaño de archivo. Por ejemplo, puede que una empresa de desarrollo de software desee limitar

el uso compartido del instalador del software de la empresa al departamento de I&D, cuyos miembros son responsables del desarrollo y comprobación del software. En tal caso, el administrador de OfficeScan puede crear una política que bloquee la transmisión de archivos ejecutables que tengan entre 10 y 40 MB a todos los departamentos, excepto a I&D.

En sí mismos, los atributos de archivo son identificadores deficientes de archivos confidenciales. Prosiguiendo con el ejemplo de este tema, la mayoría de los instaladores de software de terceros que se compartan con otros departamentos se bloqueará. Por lo tanto, Trend Micro recomienda que se combinen atributos de archivo con otros identificadores de datos de DLP para así conseguir una detección de archivos confidenciales más específica.

Para ver la lista completa de tipos de archivos compatibles, consulte el documento *Listas de protección de datos* en http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Lista de atributos de archivo predefinidos

La prevención de pérdida de datos incluye una lista de atributos de archivo predefinidos. Esta lista no se puede modificar ni eliminar. La lista presenta sus propias condiciones integradas que determinan si la plantilla debe activar una infracción de política.

Utilice la lista de atributos de archivos predefinidos para limitar el acceso a los grabadores de datos (CD/DVD).

Para conocer más detalles, consulte *Bloqueo de acceso a grabadores de datos (CD/DVD) en la página 11-36*.

Creación de una lista de atributos de archivo

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.
2. Haga clic en la pestaña **atributo de archivo**.
3. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.

4. Escriba un nombre para la lista de atributos de archivo. El nombre no debe tener más de 100 bytes de longitud ni contener los siguientes caracteres:

   - > < * ^ | & ? \ /

5. Escriba una descripción que no supere los 256 bytes de longitud.

6. Seleccione sus tipos de archivo verdadero preferidos.

7. Si no figura el tipo de archivo que desea incluir, seleccione **Extensiones de archivo** y, a continuación, escriba la extensión del tipo de archivo. La prevención de pérdida de datos comprueba los archivos con la extensión especificada pero no comprueba sus tipos de archivo verdadero. Directrices al especificar extensiones de archivo:

   - Cada extensión debe comenzar por un asterisco (*), seguida de un punto (.) y, a continuación, la extensión. El asterisco es un comodín, que representa el nombre real de un archivo. Por ejemplo, `*.pol` coincide con `12345.pol` y `test.pol`.

   - Puede incluir comodines en las extensiones. Utilice un signo de interrogación (?) para representar un carácter único y un asterisco (*) para representar dos o más caracteres. Consulte los siguientes ejemplos:

     - `*.*m` coincide con los siguientes archivos: `ABC.dem`, `ABC.prm` y `ABC.sdcm`.

     - `*.m*r` coincide con los siguientes archivos: `ABC.mgdr`, `ABC.mtp2r` y `ABC.mdmr`.

     - `*.fm?` coincide con los siguientes archivos: `ABC.fme`, `ABC.fml` y `ABC.fmp`.

   - Tenga cuidado al agregar un asterisco al final de una extensión, ya que esto podría hacer coincidir partes de un nombre de archivo y una extensión no relacionada. Por ejemplo: `*.do*` coincide con `abc.doctor_john.jpg` y `abc.donor12.pdf`.

   - Separe las extensiones de archivo con punto y coma (;). No es necesario agregar un espacio después de punto y coma.

8. Escriba los tamaños mínimo y máximo del archivo en bytes. Ambos tamaños de archivo han de ser números enteros mayores que cero.

9. Haga clic en **Guardar**.

10. Aparece un mensaje que le recuerda que debe implementar la configuración en los agentes. Haga clic en **Cerrar**.

11. Al volver a la pantalla **Identificadores de datos de DLP**, haga clic en **Aplicar a todos los agentes**.

Importación de una lista de atributos de archivo

Utilice esta opción si cuenta con un archivo `.dat` que tenga el formato correcto y contenga las listas de atributos de archivo. Para generar el archivo al exportar las listas de atributos de archivo desde el servidor al cual esté accediendo o desde otro servidor.

Nota

Los atributos de archivos de expresiones `.dat` generados por esta versión de la prevención de pérdida de datos no son compatibles con las versiones anteriores.

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.

2. Haga clic en la pestaña **atributo de archivo**.

3. Haga clic en **Importar** y, después, encuentre el archivo `.dat` que contenga las listas de atributos de archivo.

4. Haga clic en **Abrir**.

   Aparecerá un mensaje en el que se le informará de que la importación se realizó correctamente. Si la lista de atributos de archivo que se va a importar ya existe, esta se omitirá.

5. Haga clic en **Aplicar a todos los agentes**.

Palabras clave

Las palabras clave son palabras o frases especiales. Puede agregar palabras clave relacionadas a una lista de palabras clave para identificar tipos de datos específicos. Por ejemplo, en un certificado médico pueden aparecer las palabras clave "pronóstico", "grupo sanguíneo", "vacunación" y "médico". Si desea evitar la transmisión de archivos de certificados médicos, puede utilizar estas palabras clave en la política de DLP y, a continuación, configurar la prevención de pérdida de datos para que bloquee los archivos que las contengan.

Se pueden combinar palabras de uso común para que formen palabras clave significativas. Por ejemplo, "end" ('fin', 'final', 'finalizar'), "read" ('lectura', 'leer'), "if" ('si') y "at" ('a', 'al') se pueden combinar para formar palabras clave que se pueden encontrar en códigos fuente, tales como "END-IF" ('finalizar si'), "END-READ" ('finalizar lectura') y "AT END" ('al final').

Puede utilizar listas de palabras clave predefinidas y personalizadas. Para conocer más detalles, consulte *Listas de palabras clave predefinidas en la página 11-15* y *Listas de palabras clave personalizadas en la página 11-16*.

Listas de palabras clave predefinidas

La prevención de pérdida de datos incluye una lista de palabras clave predefinidas. Estas listas de palabras clave no se pueden modificar ni eliminar. Cada lista presenta sus propias condiciones integradas que determinan si la plantilla debe activar una infracción de política.

Para ver la lista completa de palabras clave predefinidas de la prevención de pérdida de datos, consulte el documento *Listas de protección de datos* en http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Funcionamiento de las listas de palabras clave

Número de condición de palabras clave

Cada lista de palabras clave contiene una condición que requiere que haya un determinado número de palabras clave en un documento para que la lista active una infracción.

La condición de número de palabras clave contiene los siguientes valores:

- **Todas**: todas las palabras clave de la lista deben estar presentes en el documento.
- **Cualquiera**: cualquiera de las palabras clave de la lista debe estar presente en el documento.
- **Número específico**: debe haber al menos el número especificado de palabras clave en el documento. Si el número de palabras clave en el documento es superior al número especificado, la prevención de pérdida de datos activa una infracción.

Condición de distancia

Algunas de las listas contienen una condición de "distancia" para determinar si se ha producido una infracción. La "distancia" hace referencia a la cantidad de caracteres entre el primero de una palabra clave y el último de otra palabra clave. Tenga en cuenta la siguiente entrada:

F**irst Name:_John_ L**ast Name:_Smith_

La lista **Formularios - Nombre, apellido** presenta una condición de "distancia" de cincuenta (50) y los campos de formulario utilizados habitualmente "Nombre" y "Apellido". En el ejemplo anterior, la prevención de pérdida de datos activa una infracción si el número de caracteres entre la "F" de "First Name" y la "L" de "Last Name" es igual a dieciocho (18).

A continuación se muestra un ejemplo de una entrada que no activa una infracción:

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

En este ejemplo, el número de caracteres entre la "f" de "first name" y la "l" de "last name" es sesenta y uno (61). Esta separación supera el umbral de distancia y no activa una infracción.

Listas de palabras clave personalizadas

Cree listas de palabras clave personalizadas si no hay ninguna lista de palabras clave predefinidas que satisfaga sus necesidades.

Son varios los criterios entre los que puede elegir a la hora de configurar una lista de palabras clave. Una lista de palabras clave debe cumplir con los criterios que escoja antes de que la prevención de pérdida de datos la supedite a una política. Escoja uno de los siguientes criterios para cada lista de palabras clave:

- **Cualquier palabra clave**
- **Todas las palabras clave**
- **Todas las palabras clave de <x> caracteres**
- **El resultado combinado de las palabras clave es mayor que el umbral**

Para obtener información acerca de las reglas de criterios, consulte *Criterios de la lista de palabras clave personalizada en la página 11-17*.

Criterios de la lista de palabras clave personalizada

TABLA 11-3. Criterios para una lista de palabras clave

CRITERIOS	REGLA
Cualquier palabra clave	Un archivo debe contener al menos una palabra clave de la lista de palabras clave.
Todas las palabras clave	Un archivo debe contener todas las palabras clave de la lista de palabras clave.

Criterios	Regla
Todas las palabras clave de <x> caracteres	Un archivo debe contener todas las palabras clave de la lista de palabras clave. Además, entre cada par de palabras clave deben haber <x> caracteres. Por ejemplo, supongamos que se usan las palabras clave WEB, DISK y USB, y que el número especificado de caracteres es 20. Si la prevención de pérdida de datos detecta todas las palabras clave en el orden DISK, WEB y USB, el número de caracteres de "D" (en DISK) a "W" (en WEB) y de "W" a "U" (en USB) debe ser de 20 como máximo. Los siguientes datos coinciden con los criterios: DISK####WEB############USB Los siguientes datos no coinciden con los criterios: DISK******************WEB****USB (en este caso, hay 23 caracteres entre "D" y "W") Al decidir el número de caracteres, recuerde que un número pequeño, como puede ser 10, suele permitir tiempos de exploración más reducidos, pero abarca un área relativamente pequeña. Esto puede disminuir la probabilidad de detectar datos confidenciales, sobre todo en archivos de gran tamaño. Al incrementar el número, el área abarcada también aumentará, pero el tiempo de exploración puede ser superior.
El resultado combinado de las palabras clave es mayor que el umbral	Un archivo debe contener una o más palabras clave de la lista de palabras clave. Si solo se detecta una palabra clave, su puntuación debe ser superior al umbral. Si hay varias palabras clave, su puntuación combinada debe ser superior al umbral. Asigne a cada palabra clave una puntuación del 1 al 10. Una palabra o frase muy confidenciales, como puede ser "aumento salarial" para el departamento de Recursos Humanos, debe tener una puntuación relativamente alta. Las palabras o frases que, por sí mismas, no tengan mucho peso deben tener puntuaciones menores. Cuando configure el umbral, tenga en cuenta las puntuaciones que haya asignado a las palabras clave. Si, por ejemplo, tiene cinco palabras clave y tres de ellas son de alta prioridad, el umbral puede ser igual o inferior a la puntuación combinada de las tres palabras clave de alta prioridad. Esto quiere decir que la detección de estas tres palabras clave basta para tratar el archivo como confidencial.

Creación de una lista de palabras clave

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.
2. Haga clic en la pestaña **palabra clave**.
3. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.
4. Escriba un nombre para la lista de palabras clave. El nombre no debe tener más de 100 bytes de longitud ni contener los siguientes caracteres:
   - > < * ^ | & ? \ /
5. Escriba una descripción que no supere los 256 bytes de longitud.
6. Escoja uno de los siguientes criterios y defina la configuración adicional para los criterios elegidos:
   - **Cualquier palabra clave**
   - **Todas las palabras clave**
   - **Todas las palabras clave de <x> caracteres**
   - **El resultado combinado de las palabras clave es mayor que el umbral**
7. Para añadir de forma manual palabras clave a la lista:
   a. Escriba una palabra clave que tenga entre 3 y 40 bytes de longitud y especifique si distingue entre mayúsculas y minúsculas.
   b. Haga clic en **Agregar**.
8. Para añadir palabras clave mediante la opción "importar":

Nota

Utilice esta opción si cuenta con un archivo `.csv` que tenga el formato correcto y contenga las palabras clave. Para generar el archivo, puede exportar las palabras clave desde el servidor al cual esté accediendo o desde otro servidor.

a. Haga clic en **Importar** y, a continuación, busque el archivo `.csv` que contiene las palabras clave.

b. Haga clic en **Abrir**.

Aparecerá un mensaje en el que se le informará de que la importación se realizó correctamente. Si la palabra clave que se va a importar ya está en la lista, esta se omitirá.

9. Para eliminar palabras clave, selecciónelas y haga clic en **Eliminar**.

10. Para exportar palabras clave:

Nota

Utilice la función "Exportar" para realizar una copia de seguridad de las palabras clave o para importarlas a otro servidor. Se exportarán todas las palabras clave de la lista de palabras clave. No se pueden exportar palabras clave de forma individual.

a. Haga clic en **Exportar**.

b. Guarde el archivo `.csv` resultante en la ubicación que prefiera.

11. Haga clic en **Guardar**.

12. Aparece un mensaje que le recuerda que debe implementar la configuración en los agentes. Haga clic en **Cerrar**.

13. Al volver a la pantalla **Identificadores de datos de DLP**, haga clic en **Aplicar a todos los agentes**.

Importación de una lista de palabras clave

Utilice esta opción si cuenta con un archivo `.dat` que tenga el formato correcto y contenga las listas de palabras clave. Para generar el archivo, puede exportar las listas de palabras clave desde el servidor al cual esté accediendo o desde otro servidor.

Nota

Los archivos de listas de palabras clave `.dat` generados por esta versión de la prevención de pérdida de datos no son compatibles con las versiones anteriores.

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Identificadores de datos**.
2. Haga clic en la pestaña **palabra clave**.
3. Haga clic en **Importar** y, a continuación, busque el archivo `.dat` que contiene las listas de palabras clave.
4. Haga clic en **Abrir**.

   Aparecerá un mensaje en el que se le informará de que la importación se realizó correctamente. Si la lista de palabras clave que se va a importar ya existe, esta se omitirá.
5. Haga clic en **Aplicar a todos los agentes**.

Plantillas de prevención de pérdida de datos

Una plantilla de DLP combina identificadores de datos de DLP y operadores lógicos (Y, O, Excepto) para formar condiciones. Solo los archivos o los datos que cumplan con una determinada condición estarán sujetos a una política de DLP.

Por ejemplo, un archivo debe ser un archivo de Microsoft Word (atributo de archivo) Y contener determinados términos legales (palabras clave) Y números de ID (expresiones) para estar sujeto a una política de "contratos de empleo". Esta política permite que el personal de Recursos Humanos transmita el archivo mediante impresión, de modo que un empleado pueda firmar la copia impresa. La transmisión mediante todos los demás canales posibles, tales como el correo electrónico, se bloqueará.

Puede crear sus propias plantillas si ha configurado los identificadores de datos de DLP. También puede utilizar las plantillas predefinidas. Para conocer más detalles, consulte *Plantillas personalizadas de la DLP en la página 11-22* y *Plantillas predefinidas de la DLP en la página 11-22*.

Nota

No se puede eliminar una plantilla que se esté utilizando en una política de DLP. Elimine de la política la plantilla antes de eliminarla por completo.

Plantillas predefinidas de la DLP

La prevención de pérdida de datos incluye el siguiente conjunto de plantillas predefinidas que se pueden utilizar para cumplir con varios estándares reguladores. Estas plantillas no se pueden modificar ni eliminar.

- **GLBA**: Ley Gramm-Leach-Billey
- **HIPAA**: Ley de Portabilidad y Contabilidad de Seguros de Salud
- **PCI-DSS**: Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago
- **SB-1386**: Ley del Senado de EE. UU. 1386
- **US PII**: Información personal identificable de EE. UU.

Para obtener una lista detallada sobre la finalidad de todas las plantillas predefinidas y ejemplos de datos protegidos, consulte el documento *Listas de protección de datos* enhttp://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Plantillas personalizadas de la DLP

Cree sus propias plantillas si ha configurado los identificadores de datos. Una plantilla combina identificadores de datos y operadores lógicos (Y, O, Excepto) para formar condiciones.

Para obtener más información y ejemplos acerca del funcionamientos de las condiciones y los operadores lógicos, consulte *Condiciones y operadores lógicos en la página 11-22*.

Condiciones y operadores lógicos

La prevención de pérdida de datos evalúa las condiciones de izquierda a derecha. Proceda con cautela a la hora de utilizar operadores lógicos al configurar condiciones. El

uso incorrecto puede acarrear una condición errónea, la cual es muy probable que produzca resultados inesperados.

Consulte los ejemplos de la siguiente tabla.

TABLA 11-4. Condiciones de ejemplo

CONDICIÓN	INTERPRETACIÓN Y EJEMPLO
[Identificador de datos 1] **Y** [Identificador de datos 2] **Excepto** [Identificador de datos 3]	Un archivo debe cumplir con [Identificador de datos 1] y [Identificador de datos 2], pero no con [Identificador de datos 3]. Por ejemplo: Un archivo debe ser [un documento Adobe PDF] y contener [una dirección de correo electrónico], pero no debe contener [todas las palabras clave de la lista de palabras clave].
[Identificador de datos 1] **O** [Identificador de datos 2]	Un archivo debe cumplir con [Identificador de datos 1] o [Identificador de datos 2]. Por ejemplo: Un archivo debe ser [un documento Adobe PDF] o [un documento de Microsot Word].
Excepto [Identificador de datos 1]	Un archivo no debe cumplir con [Identificador de datos 1]. Por ejemplo: Un archivo no debe ser [un archivo multimedia].

Como se muestra en el último ejemplo de la tabla, el primer identificador de datos de la condición puede tener el operador "Excepto" en el caso de que un archivo no deba cumplir con todos los identificadores de datos de la condición. Sin embargo, en la mayoría de los casos, la definición del identificador de datos no cuenta con un operador.

Creación de una plantilla

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Plantillas de DLP**.

2. Haga clic en **Agregar**.

   Se abrirá una nueva pantalla.

3. Escriba un nombre para la plantilla. El nombre no debe tener más de 100 bytes de longitud ni contener los siguientes caracteres:

   - > < * ^ | & ? \ /

4. Escriba una descripción que no supere los 256 bytes de longitud.

5. Seleccione los identificadores de datos y, a continuación, haga clic en el icono "añadir".

   Al seleccionar definiciones:

   - Para seleccionar varias entradas, pulse y mantenga pulsada la tecla Ctrl y, a continuación, seleccione los identificadores de datos.
   - Utilice la función de búsqueda si tiene en mente una definición específica. Puede escribir el nombre completo o parcial del identificador de datos.
   - Cada plantilla puede contener un máximo de 30 identificadores de datos.

6. Para crear una nueva expresión, haga clic en **expresiones** y, a continuación, en **Agregar nueva expresión**. Defina la configuración de la expresión en la pantalla en la que aparezca.

7. En la nueva lista de atributos de archivos, haga clic en **atributos de archivo** y, a continuación, en **Agregar nuevo atributo de archivo**. En la pantalla que aparece, defina la configuración de la lista de atributos de archivo.

8. Para crear una nueva palabra clave, haga clic en **Palabras clave** y, a continuación, en **Agregar nueva palabra clave**. Defina la configuración de la lista de palabras clave en la pantalla en la que aparezca.

9. Si ha seleccionado una expresión, escriba el número de apariciones, el cual indica las veces que una expresión ha de tener lugar antes de que la prevención de pérdida de datos la supedite a una política.

10. Escoja un operador lógico para cada definición.

Nota

Proceda con cautela a la hora de utilizar operadores lógicos al configurar condiciones. El uso incorrecto puede acarrear una condición errónea, la cual es muy probable que produzca resultados inesperados. Consulte *Condiciones y operadores lógicos en la página 11-22* para observar ejemplos del uso correcto.

11. Haga clic en el icono de la papelera para eliminar un identificador de datos de la lista de identificadores seleccionados.

12. Debajo de **Vista previa**, compruebe la condición y realice cambios si no es la condición deseada.

13. Haga clic en **Guardar**.

14. Aparece un mensaje que le recuerda que debe implementar la configuración en los agentes. Haga clic en **Cerrar**.

15. Al volver a la pantalla **Plantillas de DLP**, haga clic en **Aplicar a todos los agentes**.

Importación de plantillas

Utilice esta opción si cuenta con un archivo `.dat` que tenga el formato correcto y contenga las plantillas. Para generar el archivo, puede exportar las plantillas desde el servidor al cual esté accediendo o desde otro servidor.

Nota

Para importar plantillas de DLP desde OfficeScan 10.6, primero debe importar los identificadores de datos asociados (antes llamados Definiciones). La prevención de pérdida de datos no puede importar plantillas que no tengan identificadores de datos asociados.

Procedimiento

1. Vaya a **Agentes** > **Prevención de pérdida de datos** > **Plantillas de DLP**.

2. Haga clic en **Importar** y, a continuación, busque el archivo `.dat` que contenga las plantillas.

3. Haga clic en **Abrir**.

   Aparecerá un mensaje en el que se le informará de que la importación se realizó correctamente. Si la plantilla que se va a importar ya existe, esta se omitirá.

4. Haga clic en **Aplicar a todos los agentes**.

Canales de la DLP

Los usuarios pueden transmitir información confidencial mediante varios canales. OfficeScan puede supervisar los siguientes canales:

- **Canales de red**: la información confidencial se transmite mediante protocolos de red como, por ejemplo, HTTP y FTP.
- **Canales de aplicaciones y sistemas**: la información confidencial se transmite mediante las aplicaciones y periféricos de un endpoint local.

Canales de red

OfficeScan puede supervisar transmisiones de datos a través de los siguientes canales de red:

- Clientes de correo electrónico
- FTP
- HTTP y HTTPS
- Aplicaciones de MI
- Protocolo SMB
- Correo electrónico Web

Para determinar las transmisiones de datos que supervisar, OfficeScan comprueba el alcance de la transmisión, que se tiene que configurar. Dependiendo del alcance que haya seleccionado, OfficeScan supervisará todas las transmisiones de datos o sólo las transmisiones externas a la Red de área local (LAN).

Consulte *Destinos y alcance de la transmisión para canales de red en la página 11-31* para obtener información detallada sobre el alcance de la transmisión.

Clientes de correo electrónico

OfficeScan supervisa el correo electrónico transmitido a través de varios agentes de correo electrónico. OfficeScan comprueba la presencia de identificadores de datos en el asunto, el cuerpo y los archivos adjuntos del mensaje de correo electrónico. Para obtener una lista de los agentes de correo compatibles, consulte el documento *Listas de protección de datos* que se encuentra en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

La supervisión tiene lugar cuando un usuario intenta enviar el mensaje de correo electrónico. Si el mensaje de correo electrónico contiene identificadores de datos, OfficeScan permitirá o bloqueará su envío.

Puede definir los dominios de correo electrónico internos no supervisados y subdominios supervisados.

- **dominios de correo electrónico no supervisados**: OfficeScan permite inmediatamente la transmisión de correos electrónicos enviados a dominios no supervisados.

  Nota

  Las transmisiones de datos a dominios de correo electrónico no supervisados y a subdominios de correo electrónico supervisados en los que la acción es "Supervisar" se asemejan en que se permite la transmisión. La única diferencia es que, para los dominios de correo electrónico no supervisados, OfficeScan no registra la transmisión, mientras que, para los subdominios de correo electrónico supervisados, la transmisión siempre se registra.

- **Subdominios de correo electrónico supervisados**: Cuando OfficeScan detecta correo electrónico transmitido a un subdominio supervisado, comprueba la acción en el marco de la política. Dependiendo de la acción, la transmisión se permite o se bloquea.

Nota

Si selecciona agentes de correo electrónico como un canal supervisado, un correo electrónico debe coincidir con una política para que se supervise. Por el contrario, un correo electrónico enviado a subdominios de correo electrónico supervisados se supervisa automáticamente, incluso si no coincide con una política.

Especifique los dominios mediante cualquiera de los formatos siguientes, separando varios dominios por comas:

- Formato X400, como, por ejemplo, /O=Trend/OU=USA, /O=Trend/OU=China
- Dominios de correo electrónico, como `ejemplo.com`

Para correos electrónicos enviados mediante el protocolo SMTP, OfficeScan comprueba si el servidor SMTP de destino se encuentra en las listas siguientes:

1. Destinos supervisados
2. Destinos no supervisados

Nota

Para obtener información sobre destinos supervisados y no supervisados, consulte *Definición de destinos no supervisados y supervisados en la página 11-44*.

3. Dominios de correo electrónico no supervisados
4. Subdominios de correo electrónico supervisados

Esto significa que si se envía un correo electrónico a un servidor SMTP en la lista de destinos supervisados, el correo electrónico se supervisa. Si el servidor SMTP no está en la lista de destinos supervisados, OfficeScan comprueba las demás listas.

Para correos electrónicos enviados a través de otros protocolos, OfficeScan solo comprueba las listas siguientes:

1. Dominios de correo electrónico no supervisados
2. Subdominios de correo electrónico supervisados

FTP

Cuando OfficeScan detecta que un cliente FTP está intentando cargar archivos en el servidor FTP, comprueba la presencia de identificadores de datos en dichos archivos. Aún no se ha cargado ningún archivo. En función de la política de DLP, OfficeScan permitirá o bloqueará la carga.

Cuando defina una política que bloquee las cargas de archivos, recuerde lo siguiente:

- Cuando OfficeScan bloquea una carga, algunos clientes FTP intentan volver a cargar los archivos. En este caso, OfficeScan finaliza el cliente FTP para evitar que esto suceda. Los usuarios no reciben ninguna notificación cuando el cliente FTP finaliza. Infórmeles de esta situación cuando implemente sus políticas de DLP.
- Si la carga de un archivo produce la sobrescritura de otro en el servidor FTP, puede que se elimine el que se encuentre en dicho servidor.

Para obtener una lista de los clientes FTP compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP y HTTPS

OfficeScan supervisa los datos que se transmitirán mediante HTTP y HTTPS. En el caso de HTTPS, OfficeScan comprueba los datos antes de que se cifren y transmitan.

Para obtener una lista de las aplicaciones y exploradores Web compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Aplicaciones de MI

OfficeScan supervisa los mensajes y archivos que los usuarios envían mediante aplicaciones de mensajería instantánea (MI). Los mensajes y archivos que reciben los usuarios no se supervisan.

Para obtener una lista de las aplicaciones IM compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Cuando OfficeScan bloquea un mensaje o archivo que se ha enviado mediante AOL Instant Messenger, MSN, Windows Messenger o Windows Live Messenger, también finaliza la aplicación. Si OfficeScan no realiza esta acción, la aplicación no responderá y los usuarios se verán obligados a finalizarla de todos modos. Los usuarios no reciben ninguna notificación cuando la aplicación finaliza. Infórmeles de esta situación cuando implemente sus políticas de DLP.

Protocolo SMB

OfficeScan supervisa las transmisiones de datos mediante el protocolo Server Message Block (SMB), el cual facilita el acceso a los archivos compartidos. Cuando otro usuario intenta copiar o leer un archivo compartido del usuario, OfficeScan comprueba que dicho archivo no sea ni contenga un identificador de datos y, después, permite o bloquea la operación.

Nota

La acción de la función Control de dispositivos tiene mayor prioridad que la acción de la función DLP. Si, por ejemplo, la función Control de dispositivos no permite que se muevan archivos en unidades de red asignadas, no se producirá la transmisión de información confidencial aunque la función DLP sí lo permita.

Para obtener información detallada acerca de las acciones de Control de dispositivos, consulte *Permisos para dispositivos de almacenamiento en la página 10-4*.

Para obtener una lista de aplicaciones que OfficeScan supervise para acceso de archivos compartido, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Correo electrónico Web

Los servicios de correo electrónico basado en Web transmiten datos mediante HTTP. Si OfficeScan detecta datos salientes desde los servicios compatibles, comprueba la presencia de identificadores de datos en dichos datos.

Para obtener una lista de los servicios de correo electrónico basados en Web compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Destinos y alcance de la transmisión para canales de red

Los destinos y alcance de transmisión definen transmisiones de datos en canales de red que OfficeScan debe supervisar. Para las transmisiones que se deben supervisar, OfficeScan comprueba la presencia de identificadores de datos antes de permitir o bloquear la transmisión. Para las transmisiones que no se deben supervisar, OfficeScan no comprueba la presencia de identificadores de datos y permite inmediatamente la transmisión.

Alcance de la transmisión Todas las transmisiones

OfficeScansupervisa los datos transmitidos fuera del equipo host.

Nota

Trend Micro recomienda seleccionar esta opción para los agentes externos.

Si no desea supervisar las transmisiones de datos a determinados destinos fuera del equipo host, defina lo siguiente:

- **Destinos no supervisados**: OfficeScan no supervisa los datos transmitidos a estos destinos.

Nota

Las transmisiones de datos a destinos no supervisados y a destinos supervisados en los que la acción es "Supervisar" se asemejan en que la transmisión es permitida. La única diferencia es que para los destinos no supervisados, OfficeScan no registra la transmisión, mientras que para los destinos supervisados, la transmisión siempre se registra.

- **Destinos supervisados**: son destinos específicos incluidos en los destinos no supervisados que deben supervisarse. Los destinos supervisados son:
  - Opcionales si se definen destinos no supervisados.
  - No configurables si no se han definido destinos no supervisados.

Por ejemplo:

Las siguientes direcciones IP se asignan al Departamento legal de su empresa:

- `10.201.168.1` a `10.201.168.25`

Está creando una política que supervisa la transmisión de certificados de empleo a todos los empleados, excepto a la plantilla a jornada completa del Departamento legal. Para ello, seleccionaría **Todas las transmisiones** como alcance de la transmisión y, a continuación:

Opción	Pasos
Opción 1	1. Agregue `10.201.168.1-10.201.168.25` a los destinos no supervisados. 2. Agregue las direcciones IP del personal a tiempo parcial del Departamento legal a los destinos supervisados. Suponga que hay 3 direcciones IP, `10.201.168.21-10.201.168.23`.
Opción 2	Agregue las direcciones IP del personal a jornada completa del Departamento legal a los destinos no supervisados: • `10.201.168.1-10.201.168.20` • `10.201.168.24-10.201.168.25`

Para obtener información sobre la definición de destinos supervisados y no supervisados, consulte *Definición de destinos no supervisados y supervisados en la página 11-44*.

Alcance de la transmisión Solo las transmisiones externas a la red de área local

OfficeScan supervisa los datos transmitidos a cualquier destino fuera de la red de área local (LAN).

Nota

Trend Micro recomienda seleccionar esta opción para los agentes internos.

"Red" hace referencia a la red local o a la de la empresa. Esto incluye la red actual (dirección IP del endpoint y máscara de red) y las siguientes direcciones IP privadas estándar:

- Clase A: `10.0.0.0` a `10.255.255.255`
- Clase B: `172.16.0.0` a `172.31.255.255`
- Clase C: `192.168.0.0` a `192.168.255.255`

Si ha seleccionado este alcance de transmisión, puede definir lo siguiente:

- **Destinos no supervisados**: defina destinos fuera de la red de área local que considere seguros y, por tanto, no se deben supervisar.

  Nota

  Las transmisiones de datos a destinos no supervisados y a destinos supervisados en los que la acción es "Supervisar" se asemejan en que la transmisión es permitida. La única diferencia es que para los destinos no supervisados, OfficeScan no registra la transmisión, mientras que para los destinos supervisados, la transmisión siempre se registra.

- **Destinos supervisados**: defina destinos dentro de la red de área local que desee supervisar.

Para obtener información sobre la definición de destinos supervisados y no supervisados, consulte *Definición de destinos no supervisados y supervisados en la página 11-44*.

Resolución de conflictos

Si la configuración para el alcance de transmisión, los destinos supervisados y los destinos no supervisados provoca conflictos, OfficeScan reconoce las siguientes prioridades, en orden de prioridad más alta a más baja:

- Destinos supervisados
- Destinos no supervisados
- Alcance de la transmisión

Canales de aplicaciones y sistemas

OfficeScan puede supervisar los siguientes canales de aplicaciones y sistemas:

- Cloud Storage Services
- Grabadores de datos (CD/DVD)
- Aplicaciones de igual a igual
- Cifrado PGP
- Impresora
- Almacenamiento extraíble
- Software de sincronización (ActiveSync)
- Portapapeles de Windows

Cloud Storage Service

OfficeScan supervisa los archivos a los que acceden los usuarios a través de los Cloud Storage Services. Para obtener una lista de los Cloud Storage Services compatibles, consulte el documento *Listas de protección de datos* que se encuentra en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Nota

La prevención de pérdida de datos admite el cifrado en los Cloud Storage Services cuando Endpoint Encryption está instalado en el endpoint del agente.

Grabadores de datos (CD/DVD)

OfficeScan supervisa los datos grabados en un CD o DVD. Para obtener una lista de los dispositivos y software de grabación de datos compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Cuando OfficeScan detecta un comando "grabar" que se haya iniciado en cualquiera de los dispositivos o software compatibles y la acción sea Omitir, procederá con la grabación de datos. Si la acción es Bloquear, OfficeScan comprueba que ninguno de los archivos que se vayan a grabar no sea ni contenga un identificador de datos. Si OfficeScan detecta al menos un identificador de datos, no se grabará ningún archivo (incluidos aquellos que no sean identificadores de datos, ni los contengan). OfficeScan también impide que se expulse el CD/DVD. Si se produce este problema, indique a los usuarios que reinicien el proceso de software o restablezcan el dispositivo.

OfficeScan implementa reglas adicionales para la grabación de CD/DVD:

- Con el fin de reducir los falsos positivos, OfficeScan no supervisa los siguientes archivos:

```
.bud      .dll      .gif      .gpd      .htm      .ico      .ini

.jpg      .lnk      .sys      .ttf      .url      .xml
```

- Con el fin de aumentar el rendimiento, no se supervisan dos tipos de archivos utilizados por los grabadores Roxio (`*.png` y `*.skn`).
- OfficeScan no supervisa los archivos de los siguientes directorios:

```
*:\autoexec.bat                    *:\Windows

..\Application Data                ..\Cookies
```

..\Local Settings	..\ProgramData
..\Archivos de programa	..\Users*\AppData
..\WINNT	

- No se supervisan las imágenes ISO creadas por los dispositivos y el software.

Bloqueo de acceso a grabadores de datos (CD/DVD)

El control de dispositivos solo puede limitar el acceso de dispositivos de grabación de CD/DVD que usan el formato del sistema de archivos LFS. Algunas aplicaciones de otros fabricantes que usan Master Format pueden realizar operaciones de lectura o escritura incluso cuando el control de dispositivos está activado. Utilice la prevención de pérdida de datos para limitar el acceso de dispositivos de grabación de CD/DVD que usan cualquier tipo de formato.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de DLP**.
4. Haga clic en la pestaña **Agentes externos** para configurar una política para agentes externos o en la pestaña **Agentes internos** para configurar una política para agentes internos.

   Nota

   Configure la ubicación del agente si aún no lo ha hecho. Los agentes usan esta configuración de ubicación para determinar la política de prevención de pérdida de datos que se aplicará. Para conocer más detalles, consulte *Ubicación del Endpoint en la página 15-2*.

5. Seleccione una de las siguientes opciones:

   - Si se encuentra en la pestaña **Agentes externos**, puede aplicar todas las opciones de prevención de pérdida de datos a los agentes internos. Para ello,

seleccione **Aplicar todos los valores de configuración en los agentes internos**.

- Si se encuentra en la pestaña **Agentes internos**, puede aplicar todas las opciones de la prevención de pérdida de datos a los agentes externos. Para ello, seleccione **Aplicar todos los valores de configuración en los agentes externos**.

6. En la pestaña **Reglas**, haga clic en **Agregar**.
7. Seleccione **Activar esta regla**.
8. Especifique un nombre para la regla.
9. Haga clic en la pestaña **Plantilla**.
10. Seleccione la plantilla **Todas las extensiones de archivo** en la lista y haga clic en **Agregar**.
11. Haga clic en la pestaña **Canal**.
12. En la sección **Canales de aplicaciones y sistemas**, seleccione **Grabadores de datos (CD/DVD)**.
13. Haga clic en la pestaña **Acción**.
14. Seleccione la acción **Bloquear**.
15. Haga clic en **Guardar**.
16. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

    - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
    - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Aplicaciones de igual a igual

OfficeScan supervisa los archivos que los usuarios compartan mediante aplicaciones de igual a igual.

Para obtener una lista de las aplicaciones de igual a igual, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Cifrado PGP

OfficeScan supervisa los datos que se deben cifrar mediante el software de cifrado PGP y comprueba los datos antes de que se realice el cifrado.

Para obtener una lista del software de cifrado PGP compatible, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Impresora

OfficeScan supervisa las operaciones de impresoras que se hayan iniciado desde varias aplicaciones.

OfficeScan no bloquea las operaciones de impresoras en archivos nuevos que no se hayan guardado porque hasta este momento la información de impresión solo se ha almacenado en la memoria.

Para obtener una lista de las aplicaciones que pueden iniciar operaciones de impresora, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Almacenamiento extraíble

OfficeScan supervisa las transmisiones de datos entrantes y salientes de los dispositivos de almacenamiento extraíbles. Entre las actividades relacionadas con la transmisión de datos se incluyen:

- Creación de un archivo dentro del dispositivo
- Copia de un archivo desde el equipo host en el dispositivo
- Cierre de un archivo modificado dentro del dispositivo
- Modificación de información del archivo (como puede ser la extensión) en el dispositivo

Cuando un archivo que se va a transmitir contiene un identificador de datos, OfficeScan bloquea o permite la transmisión.

Nota

- La acción de la función Control de dispositivos tiene mayor prioridad que la acción de la función DLP. Si, por ejemplo, la función Control de dispositivos no permite que se copien archivos en un dispositivo de almacenamiento extraíble, no se producirá la transmisión de información confidencial aunque la función DLP sí lo permita.
- La prevención de pérdida de datos admite el cifrado en dispositivos de almacenamiento extraíble cuando Endpoint Encryption está instalado en el endpoint del agente.

Para obtener una lista de las aplicaciones y los dispositivos de almacenamiento extraíble compatibles, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

La gestión de transmisión de archivos a un dispositivo de almacenamiento extraíble es un proceso sencillo. Por ejemplo, un usuario que cree un archivo con Microsoft Word puede que quiera guardarlo en una tarjeta SD (sin que importe con qué tipo de archivo lo guarde el usuario). Si el archivo contiene un identificador de datos que no se debe transmitir, OfficeScan impide que se guarde el archivo.

Para transmisiones de archivos dentro del dispositivo, OfficeScan realiza primero una copia de seguridad del archivo (si ocupa 75 MB o menos) en `%WINDIR%\system32\dgagent\temp` antes de procesarlo. OfficeScan elimina la copia de seguridad del archivo si permitió la transmisión del mismo. Si OfficeScan bloqueó la transmisión, puede que dicho archivo se haya eliminado en el proceso. En este caso, OfficeScan copiará el archivo de copia de seguridad en la carpeta que contenga el archivo original.

OfficeScan le permite definir excepciones. OfficeScan siempre permite las transmisiones de datos hacia o en estos dispositivos. Identifique los dispositivos por sus proveedores y, opcionalmente, proporcione los ID de serie y modelo de los dispositivos.

Consejo

Utilice la herramienta de lista de dispositivos para realizar consultas en los dispositivos que estén conectados a Endpoints. La herramienta proporciona el distribuidor, el modelo y el ID de serie de cada dispositivo. Para conocer más detalles, consulte *Herramienta de lista de dispositivos en la página 10-14*.

Software de sincronización (ActiveSync)

OfficeScan supervisa los datos transmitidos a un dispositivo móvil mediante el software de sincronización.

Para obtener una lista de software de sincronización compatible, consulte el documento *Listas de protección de datos* en:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Si los datos tienen una dirección IP de origen de 127.0.0.1 y se envían mediante los puertos 990 o 5678 (aquellos que se utilizan para la sincronización), OfficeScan comprueba que los datos no sean un identificador de datos antes de permitir o bloquear la transmisión.

Cuando OfficeScan bloquea un archivo que se ha transmitido mediante el puerto 990, puede que aún se cree en la carpeta de destino del dispositivo móvil un archivo con el mismo nombre y que contenga caracteres con un formato incorrecto. Esto se debe a

que ciertas partes del archivo se habrían copiado en el dispositivo antes de que OfficeScan bloquease la transmisión.

Portapapeles de Windows

OfficeScan supervisa los datos que transmitirán al Portapapeles de Windows antes de permitir o bloquear la transmisión.

OfficeScan también puede supervisar las actividades del Portapapeles entre el equipo host y VMWare o Remote Desktop. La supervisión tiene lugar en la entidad con el Agente de OfficeScan. Por ejemplo, el Agente de OfficeScan en una máquina virtual de VMware puede impedir que se transmitan datos del Portapapeles de dicha máquina virtual al equipo host. De forma similar, es posible que un equipo host con el Agente de OfficeScan no copie los datos del Portapapeles en un endpoint al que se ha accedido mediante Escritorio remoto.

Acciones de la prevención de pérdida de datos

Cuando la prevención de pérdida de datos detecta la transmisión de identificadores de datos, comprueba la política de DLP de los identificadores de datos detectados y realiza la acción configurada para la política.

En la siguiente tabla figuran las acciones de Prevención de pérdida de datos.

TABLA 11-5. Acciones de la prevención de pérdida de datos

ACCIÓN	DESCRIPCIÓN
Acciones	
Omitir	La prevención de pérdida de datos permite y registra la transmisión.
Bloquear	La prevención de pérdida de datos bloquea y registra la transmisión.
Acciones adicionales	

Acción	Descripción
Enviar notificación al usuario del agente	La prevención de pérdida de datos muestra un mensaje de notificación para informar de la transmisión de datos al usuario y si esta se ha omitido o bloqueado.
Grabar datos	Independientemente de la acción principal, la prevención de pérdida de datos guarda la información confidencial en `<carpeta de instalación del cliente>\DLPLite\Forensic`. Seleccione esta acción para evaluar la información confidencial que la función Prevención de pérdida de datos esté marcando. Es posible que la información confidencial guardada consuma demasiado espacio en el disco duro. Por tanto, Trend Micro recomienda encarecidamente que elija esta opción solo para información muy confidencial.

Acción	Descripción
Cifrar canales compatibles con la contraseña o la clave especificadas (solo disponible si Endpoint Encryption está instalado) **Nota** Esta opción solo está disponible para los canales de servicio de almacenamiento extraíble y en la nube, y cuando se selecciona la acción **Omitir**.	Si Trend Micro Endpoint Encryption se instala junto con el agente de OfficeScan, la prevención de pérdida de datos puede cifrar automáticamente los archivos antes de permitir que un usuario los transfiera a otra ubicación. Si no se instala Endpoint Encryption, la prevención de pérdida de datos llevará a cabo la acción Bloquear en los archivos. Elija una se las siguientes claves de cifrado o una contraseña fija: • **Clave de usuario**: esta clave, también conocida como **Clave local**, es exclusiva para cada usuario y limita el acceso del archivo cifrado al usuario que lo creó. • **Clave compartida**: esta clave se refiere a los tipos de clave **Clave de grupo** o **Clave empresarial** que configura el administrador de Endpoint Encryption mediante la consola MMC de PolicyServer. • **Contraseña fija**: los usuarios proporcionan una contraseña fija manualmente cuando aparece una solicitud en la pantalla. Endpoint Encryption crea un paquete autoextraíble al que los usuarios pueden acceder desde cualquier endpoint tras facilitar la contraseña de descifrado. **Importante** • Endpoint Encryption debe estar instalado en el endpoint de destino, y el usuario debe iniciar sesión en Endpoint Encryption para poder cifrar los datos. • Los archivos cifrados ubicados en dispositivos USB están sujetos a la exploración de prevención de pérdida de datos cuando los usuarios intentan descifrar los archivos. El descifrado de archivos que contienen datos confidenciales en dispositivos USB activa el protocolo de cifrado USB, lo que da lugar a que el sistema solicite que se cifren (de nuevo) los datos confidenciales. Para evitar que OfficeScan intente “volver a cifrar” los datos, mueva los archivos cifrados a una unidad local antes de intentar acceder a los datos. • La prevención de pérdida de datos bloquea los intentos de carga de archivos al almacenamiento en la nube cuando se utiliza un cliente Web. Cifre los archivos

Acción	Descripción
Justificación del usuario **Nota** Esta opción solo está disponible después de haber seleccionado la acción **Bloquear**.	La prevención de pérdida de datos informa al usuario antes de realizar la acción «Bloquear». El usuario puede sobrescribir la acción «Bloquear» si explica el motivo por el que es seguro omitir los datos confidenciales. Las razones de justificación disponibles son: • **Es parte de un proceso de negocio estándar.** • **Mi supervisor aprobó la transferencia de datos.** • **Los datos de este archivo no son confidenciales.** • **Otros**: los usuarios proporcionan una explicación alternativa en el campo de texto disponible.

Excepciones de la prevención de pérdida de datos

Las excepciones de DLP se aplican a toda la política, incluyendo todas las reglas definidas dentro de la misma. La prevención de pérdida de datos aplica la configuración de las excepciones a todas las transmisiones antes de buscar activos. Si una transmisión coincide con una regla de excepción, la prevención de pérdida de datos permite o explora de forma inmediata la transmisión dependiendo del tipo de excepción.

Definición de destinos no supervisados y supervisados

Defina los destinos supervisados y no supervisados en base al alcance de transmisión configurado en la pestaña **Canal**. Para obtener información sobre cómo definir los destinos no supervisados y supervisados para **Todas las transmisiones**, consulte *Alcance de la transmisión Todas las transmisiones en la página 11-31*. Para obtener información sobre cómo definir los destinos no supervisados y supervisados para **Solo las transmisiones fuera de la red de área local**, consulte *Alcance de la transmisión Solo las transmisiones externas a la red de área local en la página 11-33*.

Siga estas directrices al definir destinos supervisados y no supervisados:

1. Defina cada objetivo a través de:
   - Dirección IP
   - Nombre del host
   - FQDN
   - Dirección de red y máscara de subred, como 10.1.1.1/32

Nota

Para la máscara de subred, la prevención de pérdida de datos solo admite un puerto de tipo encaminamiento inter-dominios sin clase (CIDR). Esto significa que solo puede escribir un número como 32 en lugar de 255.255.255.0.

2. Para indicar como destino unos canales específicos, incluya los números de puerto predeterminados o definidos por la empresa correspondientes a dichos canales. Por ejemplo, el puerto 21 suele corresponder al tráfico FTP, el puerto 80 al HTTP y el puerto 443 al HTTPS. Separe el destino de los números de puerto mediante dos puntos.
3. También puede incluir rangos de puertos. Para incluir todos los puertos, ignore el intervalo de puertos.

   Ejemplos de destinos con números de puerto e intervalos de puertos:
   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. Separe los destinos mediante comas.

Reglas de descompresión

Se puede explorar el contenido de los archivos comprimidos para detectar activos digitales. Para determinar los archivos que se van a explorar, la prevención de pérdida de datos aplica las siguientes reglas a los archivos comprimidos:

- **El tamaño de un archivo descomprimido es mayor que: __ MB (1-512 MB)**
- **Las capas de compresión son mayores que: __ (1-20)**
- **El número de archivos para explorar es mayor que: __ (1-2000)**

Regla 1: tamaño máximo de un archivo descomprimido

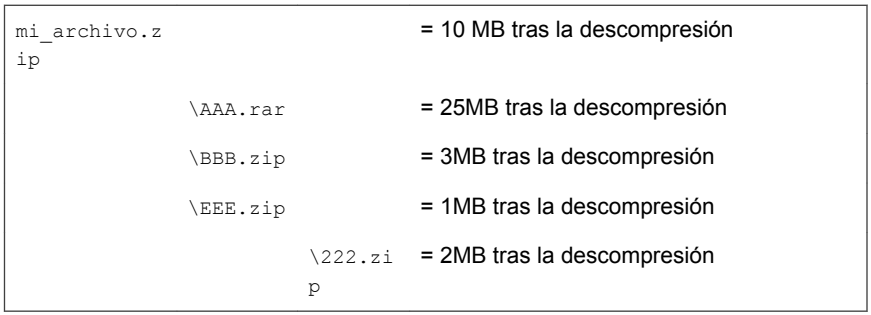
Un archivo comprimido, tras la descompresión, debe cumplir el límite especificado.

Ejemplo: ha establecido el límite en 20 MB.

Caso 1: si el tamaño de `archivo.zip` tras la descompresión es de 30 MB, no se explorará ninguno de los archivos contenidos en `archivo.zip`. Las otras dos reglas ya no se comprobarán.

Caso 2: si el tamaño de `mi_archivo.zip` tras la descompresión es de 10 MB, ocurre lo siguiente.

- Si `mi_archivo.zip` no contiene archivos comprimidos, OfficeScan omite la Regla 2 y continúa con la Regla 3.
- Si `mi_archivo.zip` contiene archivos comprimidos, el tamaño de todos los archivos descomprimidos debe estar dentro del límite. Por ejemplo, si `mi_archivo.zip` contiene `AAA.rar`, `BBB.zip` y `EEE.zip`, y `EEE.zip` contiene `222.zip`:



`mi_archivo.zip`, `BBB.zip`, `EEE.zip` y `222.zip` se comprobarán con la Regla 2 dado que el tamaño combinado de estos archivos está dentro del límite de 20 MB. `AAA.rar` se omite.

Regla 2: número máximo de capas de descompresión

Los archivos dentro del número especificado de capas se marcarán para exploración.

Por ejemplo:

```
mi_archivo.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

Si ha establecido el límite en dos capas:

- OfficeScan ignorará `333.txt` dado que está ubicado en la tercera capa.
- OfficeScan marcará los siguientes archivos para exploración y, a continuación, comprobará la Regla 3:
  - `DDD.txt` (ubicado en la primera capa)
  - `CCC.xls` (ubicado en la segunda capa)
  - `111.pdf` (ubicado en la segunda capa)

Regla 3: número máximo de archivos para explorar

OfficeScan explora archivos hasta el límite especificado. OfficeScan explora los archivos y carpetas en orden numérico y, luego, en orden alfabético.

Continuando a partir del ejemplo en Regla 2, OfficeScan ha marcado los archivos resaltados para exploración:

```
mi_archivo.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
```

```
                    \EEE.zip            \111.pdf

                                        \222.zip            \333.txt
```

Además, `mi_archivo.zip` contiene una carpeta llamada `Carpeta7`, que no se ha comprobado con la Regla 2. Esta carpeta contiene `FFF.doc` y `GGG.ppt`. Esto hace que el número total de archivos que deben explorarse sea 5, como se destaca más abajo:

```
mi_archivo.zip
                    \7Folder            \FFF.doc

                    \7Folder            \GGG.ppt

                    \BBB.zip            \CCC.xls

                    \DDD.txt

                    \EEE.zip            \111.pdf

                                        \222.zip            \333.txt
```

Si ha establecido el límite en 4 archivos, se exploran los archivos siguientes:

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`

Nota

Para los archivos que contienen archivos incrustados, OfficeScan extrae el contenido de los archivos incrustados.

Si el contenido extraído es texto, el archivo host (como, por ejemplo, `123.doc`) y los archivos incrustados (como, por ejemplo, `abc.txt` y `xyz.xls`) se cuentan como uno.

Si el contenido extraído no es texto, el archivo host (como, por ejemplo, `123.doc`) y los archivos incrustados (como, por ejemplo, `abc.exe`) se cuentan por separado.

Sucesos que activan reglas de descompresión

Los sucesos siguientes activan reglas de descompresión:

TABLA 11-6. Sucesos que activan reglas de descompresión

Un archivo comprimido que se va a transmitir coincide con una política y la acción sobre el archivo comprimido es Omitir (transmitir el archivo).	Por ejemplo, para supervisar archivos .ZIP que los usuarios están transmitiendo, ha definido un atributo de archivo (.ZIP), lo ha agregado a una plantilla, ha utilizado la plantilla en una política y, a continuación, ha configurado la acción en **Omitir**. **Nota** Si la acción es Bloquear, no se transmite todo el archivo comprimido y, por tanto, no hay necesidad de explorar los archivos que contiene.
Un archivo comprimido que se va a transmitir no coincide con una política.	En este caso, OfficeScan seguirá sometiendo el archivo comprimido a las reglas de descompresión para determinar cuáles de los archivos que contiene se deben explorar en busca de activos digitales y si se debe transmitir todo el archivo comprimido.

Ambos sucesos tienen el mismo resultado. Cuando OfficeScan encuentra un archivo comprimido:

- Si la Regla 1 no se satisface, OfficeScan permite la transmisión de todo el archivo comprimido.
- Si la Regla 1 se cumple, se comprueban las otras dos reglas. OfficeScan permite la transmisión de todo el archivo comprimido si:
  - Todos los archivos explorados no coinciden con una política.
  - Todos los archivos explorados coinciden con una política y la acción es **Omitir**.

La transmisión de todo el archivo comprimido se bloquea si al menos uno de los archivos explorados coincide con una política y la acción es **Bloquear**.

Configuración de las políticas de prevención de pérdida de datos

Una vez que haya configurado los identificadores de datos y los haya organizado en plantillas, puede comenzar a crear políticas de Prevención de pérdida de datos.

Al crear una política, además de los identificadores de datos y las plantillas, es necesario configurar los canales y las acciones. Para obtener información detallada acerca de las políticas, consulte *Políticas de prevención de pérdida de datos en la página 11-3*.

Crear una política de prevención de pérdida de datos

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Configuración de DLP**.
4. Haga clic en la pestaña **Agentes externos** para configurar una política para agentes externos o en la pestaña **Agentes internos** para configurar una política para agentes internos.

   Nota

   Configure la ubicación del agente si aún no lo ha hecho. Los agentes usan esta configuración de ubicación para determinar la política de prevención de pérdida de datos que se aplicará. Para conocer más detalles, consulte *Ubicación del Endpoint en la página 15-2*.

5. Seleccione **Activar la prevención de pérdida de datos**.

6. Seleccione una de las siguientes opciones:

   - Si se encuentra en la pestaña **Agentes externos**, puede aplicar todas las opciones de prevención de pérdida de datos a los agentes internos. Para ello, seleccione **Aplicar todos los valores de configuración en los agentes internos**.

   - Si se encuentra en la pestaña **Agentes internos**, puede aplicar todas las opciones de la prevención de pérdida de datos a los agentes externos. Para ello, seleccione **Aplicar todos los valores de configuración en los agentes externos**.

7. En la pestaña **Reglas**, haga clic en **Agregar**.

   Una política solo puede contener 40 reglas como máximo.

8. Defina la configuración de las reglas.

   Para obtener información detallada sobre cómo crear reglas de DLP, consulte *Crear reglas de prevención de pérdida de datos en la página 11-52*.

9. Haga clic en la pestaña **Excepciones** y configure cualquier valor de excepción necesario.

   Para obtener información detallada sobre la configuración de excepciones disponibles, consulte *Excepciones de la prevención de pérdida de datos en la página 11-44*.

10. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

    - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

    - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Crear reglas de prevención de pérdida de datos

Nota

La prevención de pérdida de datos procesa las reglas y las plantillas según su prioridad. Si una regla está establecida en «Omitir», la prevención de pérdida de datos procesará la siguiente regla de la lista. Si una regla está establecida en «Bloquear» o «Justificación del usuario», la prevención de pérdida de datos bloquea o acepta la acción del usuario y no procesa esta regla o esa plantilla.

Procedimiento

1. Seleccione **Activar esta regla**.
2. Especifique un nombre para la regla.

   Defina la configuración de la plantilla:
3. Haga clic en la pestaña **Plantilla**.
4. Seleccione plantillas de la lista **Plantillas disponibles** y, después, haga clic en **Agregar**.

   Al seleccionar plantillas:

   - Seleccione varias entradas haciendo clic en los nombres de plantilla que tengan el nombre resaltado.
   - Utilice la función de búsqueda si tiene en mente una plantilla específica. Puede escribir el nombre completo o parcial de la plantilla.

   Nota

   Cada regla puede contener un máximo de 200 plantillas.
5. Si no se encuentra su plantilla preferida en la lista **Plantillas disponibles**:

   a. Haga clic en **Agregar nueva plantilla**.

      Aparece la pantalla **Plantillas de la Prevención de pérdida de datos**.

Para obtener instrucciones sobre cómo agregar plantillas en la **pantalla de plantillas de la Prevención de datos**, consulte *Plantillas de prevención de pérdida de datos en la página 11-21*.

b. Después de crear la plantilla, selecciónela y, después, haga clic en **Agregar**.

Nota

OfficeScan utiliza la regla de primera coincidencia al comprobar las plantillas. Esto significa que si un archivo o datos coinciden con la definición en una plantilla, OfficeScan no seguirá comprobando las demás plantillas. La prioridad se basa en el orden de las plantillas de la lista.

Defina la configuración del canal:

6. Haga clic en la pestaña **Canal**.

7. Seleccione los canales para la regla.

   Para obtener información detallada acerca de los canales, consulte *Canales de red en la página 11-26* y *Canales de aplicaciones y sistemas en la página 11-34*.

8. Si ha seleccionado alguno de los canales de red, seleccione el alcance de la transmisión:

   - **Todas las transmisiones**
   - **Solo las transmisiones externas a la red de área local**

   Consulte *Destinos y alcance de la transmisión para canales de red en la página 11-31* para conocer los detalles sobre el alcance de la transmisión, cómo funcionan los destinos en función del alcance de transmisión y cómo se definen los destinos correctamente.

9. Si ha seleccionado **Clientes de correo electrónico**:

   a. Haga clic en **Excepciones**.

   b. Especifique los dominios de correo electrónico internos supervisados y no supervisados.

      Para obtener detalles sobre los dominios de correo electrónico supervisados y no supervisados, consulte *Clientes de correo electrónico en la página 11-27*.

10. Si ha seleccionado **Almacenamiento extraíble**:

    a. Haga clic en **Excepciones**.

    b. Agregue dispositivos de almacenamiento extraíble no supervisado, identificados mediante sus proveedores. El modelo y la ID de serie son opcionales.

       La lista dispositivos USB permitidos es compatible con el uso del asterisco (*) como comodín. Sustituya cualquier campo con el asterisco (*) para incluir todos los dispositivos que cumplan con los otros campos.

       Por ejemplo, [proveedor]-[modelo]-* coloca todos los dispositivos USB del proveedor específico y del tipo de modelo específico, independientemente del ID de serie, en la lista permitida.

    c. Para agregar más dispositivos, haga clic en el icono **+**.

Consejo

Utilice la herramienta de lista de dispositivos para realizar consultas en los dispositivos que estén conectados a Endpoints. La herramienta proporciona el distribuidor, el modelo y el ID de serie de cada dispositivo. Para conocer más detalles, consulte *Herramienta de lista de dispositivos en la página 10-14*.

Defina la configuración de la acción:

11. Haga clic en la pestaña **Acción**.

12. Seleccione una acción principal y las acciones adicionales que desee.

Para obtener información detallada acerca de las acciones, consulte *Acciones de la prevención de pérdida de datos en la página 11-41*.

Nota

La prevención de pérdida de datos solo admite el cifrado de datos confidenciales en dispositivos extraíbles y Cloud Storage Services. La prevención de pérdida de datos lleva a cabo la acción «Omitir» sin cifrado en todos los canales que no admiten cifrado. Endpoint Encryption debe estar instalado en el endpoint de destino, y el usuario debe iniciar sesión en Endpoint Encryption para poder cifrar los datos.

13. Después de definir la configuración de la **Plantilla**, **Canal** y **Acción**, haga clic en **Guardar**.

Importar, Exportar y Copiar reglas de DLP

Los administradores pueden importar reglas definidas previamente (contenidas en un archivo `.dat` con el formato correcto) o exportar la lista de reglas de DLP configuradas. Copiar una regla de DLP permite a un administrador modificar el contenido de una regla definida previamente para ahorrar tiempo.

La siguiente tabla describe cómo funciona cada función.

TABLA 11-7. Importar, Exportar y Copiar funciones para reglas de DLP

FUNCIÓN	DESCRIPCIÓN
Importar	Importar una lista de reglas añade reglas no existentes a la lista de reglas de DLP existente. La prevención de pérdida de datos omite las reglas que ya existen en la lista de destino. La prevención de pérdida de datos mantiene toda la configuración definida previamente para cada regla, incluyendo el estado activado o desactivado.
Exportar	Exportar una lista de reglas exporta la lista entera a un archivo `.dat` que los administradores pueden, a continuación, importar e implementar en otros dominios o agentes. La prevención de pérdida de datos guarda toda la configuración de reglas en función de la configuración actual. **Nota** • Los administradores deben guardar o aplicar cualquier regla nueva o modificada antes de exportar la lista. • La prevención de pérdida de datos no exporta ninguna excepción configurada para la política, solo la configuración definida para cada regla.
Copiar	Copiar una regla crea una réplica exacta de la configuración actual definida para la regla. Los administradores deben introducir un nuevo nombre para la regla y pueden realizar cualquier modificación necesaria en la configuración de la nueva regla.

Notificaciones de la prevención de pérdida de datos

OfficeScan incluye un conjunto de mensajes de notificación predeterminados que informa a los administradores de OfficeScan y a los usuarios de agentes de las transmisiones de activos digitales.

Para obtener más información sobre las notificaciones que se envían a los administradores, consulte *Notificaciones de la prevención de pérdida de datos para administradores en la página 11-56*.

Para obtener más información sobre las notificaciones que se envían a los usuarios del agente, consulte *Notificaciones de prevención de pérdida de datos para los usuarios del agente en la página 11-60*.

Notificaciones de la prevención de pérdida de datos para administradores

Configure OfficeScan para que envíe a los administradores una notificación cuando se detecte la transmisión de activos digitales o solo cuando dicha transmisión se bloquee.

OfficeScan incluye un conjunto de mensajes de notificación predefinidos que informan a los administradores de las transmisiones de activos digitales. Modifique las notificaciones y defina la configuración de notificaciones adicionales según las necesidades de la empresa.

Nota

OfficeScan puede enviar notificaciones mediante correo electrónico, captura SNMP y registros de sucesos de Windows NT. Defina la configuración cuando OfficeScan envíe notificaciones mediante estos canales. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

Configurar las notificaciones de prevención de pérdida de datos para los administradores

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Administrador**.
2. En la pestaña **Criterios**:
   a. Vaya a la sección **Transmisiones de activos digitales**.
   b. Especifique si desea enviar notificaciones cuando se detecte la transmisión de activos digitales (la acción puede bloquearse u omitirse) o solo cuando se bloquee dicha transmisión.
3. En la pestaña **Correo electrónico**:
   a. Vaya a la sección **Transmisiones de activos digitales**.
   b. Seleccione **Activar la notificación por correo electrónico**.
   c. Seleccione **Enviar notificaciones a los usuarios con permisos de dominio del árbol de agentes**.

      Utilice la administración basada en funciones para conceder a los usuarios permisos de dominio del árbol de agentes. Si se produce una transmisión en un agente que pertenezca a un dominio específico, se enviará un correo electrónico a las direcciones de correo electrónico de los usuarios con permisos de dominio. Consulte los ejemplos de la siguiente tabla:

TABLA 11-8. Dominios y permisos del árbol de agentes

DOMINIO DEL ÁRBOL DE AGENTES	FUNCIONES CON PERMISOS DE DOMINIO	CUENTA DE USUARIO CON LA FUNCIÓN	DIRECCIÓN DE CORREO ELECTRÓNICO PARA LA CUENTA DE USUARIO
Dominio A	Administrador (integrado)	raíz	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Dominio B	Administrador (integrado)	raíz	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un Agente de OfficeScan que pertenece al dominio A detecta la transmisión de un activo digital, se enviará el mensaje de correo electrónico a las direcciones mary@xyz.com, john@xyz.com y chris@xyz.com.

Si un Agente de OfficeScan que pertenece al dominio B detecta la transmisión, el mensaje de correo electrónico se enviará a las direcciones mary@xyz.com y jane@xyz.com.

Nota

Si se activa esta opción, todos los usuarios con permisos de dominio deben tener una dirección de correo electrónico correspondiente. El correo electrónico de notificación no se enviará a los usuarios sin dirección de correo electrónico. Los usuarios y las direcciones de correo electrónico se configuran en **Administración** > **Administración de cuentas** > **Cuentas de usuario**.

d. Seleccione **Enviar notificaciones a la(s) siguiente(s) dirección(es) de correo electrónico** y, después, escriba las direcciones de correo electrónico.

e. Acepte o modifique el asunto y el mensaje predeterminados. Utilice variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 11-9. Variables de símbolo para las notificaciones de prevención de pérdida de datos

VARIABLE	DESCRIPCIÓN
%USER%	El usuario conectado al endpoint cuando se detectó la transmisión.
%COMPUTER%	El endpoint en el que se detectó la transmisión.
%DOMAIN%	El dominio del endpoint.
%DATETIME%	La fecha y hora en las que se detectó la transmisión
%CHANNEL%	El canal mediante el cual se detectó la transmisión
%TEMPLATE%	La plantilla de activo digital que activó la transmisión
%RULE%	El nombre de la regla que activó la detección **Nota** Para mostrar el nombre de la regla en el mensaje, añada esta variable al campo **Mensaje**.

4. En la pestaña **Captura SNMP**:

   a. Vaya a la sección **Transmisiones de activos digitales**.

   b. Seleccione **Activar la notificación por captura SNMP**.

   c. Acepte o modifique el mensaje predeterminado. Utilice variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 11-9: Variables de símbolo para las notificaciones de prevención de pérdida de datos en la página 11-59* para obtener más información.

5. En la pestaña **Registro de sucesos de NT**:

   a. Vaya a la sección **Transmisiones de activos digitales**.

   b. Seleccione **Activar la notificación por el registro de sucesos de NT**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 11-9:*

Variables de símbolo para las notificaciones de prevención de pérdida de datos en la página 11-59 para obtener más información.

6. Haga clic en **Guardar**.

Notificaciones de prevención de pérdida de datos para los usuarios del agente

OfficeScan puede mostrar mensajes de notificación en equipos del agente inmediatamente después de permitir o bloquear la transmisión de activos digitales.

Para informar a los usuarios de que se ha permitido o bloqueado una transmisión de activos digitales, seleccione la opción **Enviar notificación al usuario del agente** al crear una política de prevención de pérdida de datos. Para obtener instrucciones sobre cómo crear una política, consulte *Configuración de las políticas de prevención de pérdida de datos en la página 11-50*.

Configuración de las notificaciones de prevención de pérdida de datos para los agentes

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. En el menú desplegable **Tipo**, seleccione **Transmisión de activos digitales**.
3. Acepte o modifique el mensaje predeterminado.
4. Haga clic en **Guardar**.

Registros de prevención de pérdida de datos

Los agentes registran las transmisiones de activos digitales (tanto las bloqueadas como las permitidas) y envían los registros inmediatamente al servidor. Si el agente no puede enviar los registros, lo vuelve a intentar 5 minutos después.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Visualización de los registros de prevención de pérdida de datos

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes** o **Registros** > **Agentes** > **Riesgos de seguridad**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros de prevención de pérdida de datos** o **Ver registros** > **Registros de DLP**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros.

   Los registros contienen la siguiente información:

   TABLA 11-10. Información de los registros de la Prevención de pérdida de datos

COLUMNA	DESCRIPCIÓN
Fecha/hora	La fecha y la hora en las que la prevención de pérdida de datos registró el incidente
Usuario	El nombre de usuario conectado al endpoint
Endpoint	El nombre del endpoint en el que la prevención de pérdida de datos ha detectado la transmisión
Dominio	El dominio del endpoint
IP	La dirección IP del endpoint

COLUMNA	DESCRIPCIÓN
Nombre de la regla	Los nombre de regla que desencadenaron el incidente **Nota** Las políticas creadas en una versión anterior de OfficeScan muestran el nombre predeterminado de LEGACY_DLP_Policy.
Canal	El canal mediante el cual se produjo la transmisión
Proceso	El proceso que facilitó la transmisión del activo digital (el proceso depende del canal) Para conocer más detalles, consulte *Procesos por canal en la página 11-62*.
Fuente	El origen del archivo que contiene el activo digital o canal (si no hay ningún origen disponible)
Destino	El destino intencionado del archivo que contiene el activo digital o canal (si no hay ningún origen disponible)
Acción	Acción realizada sobre la transmisión
Detalles	Un enlace que incluye detalles adicionales acerca de la transmisión Para conocer más detalles, consulte *Detalles de los registros de prevención de pérdida de datos en la página 11-65*.

6. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Procesos por canal

En la siguiente tabla se enumeran los procesos que se muestran bajo la columna **Proceso** en los registros de prevención de pérdida de datos.

TABLA 11-11. Procesos por canal

CANAL	PROCESO
Software de sincronización (ActiveSync)	Ruta completa y nombre del proceso del software de sincronización Ejemplo: `C:\Windows\system32\WUDFHost.exe`
Grabador de datos (CD/DVD)	Ruta completa y nombre de proceso del grabador de datos Ejemplo: `C:\Windows\Explorer.exe`
Portapapeles de Windows	No aplicable
Cliente de correo electrónico: Lotus Notes	Ruta completa y nombre de proceso de Lotus Notes Ejemplo: `C:\Archivos de programa\IBM\Lotus\Notes\nlnotes.exe`
Cliente de correo electrónico: Microsoft Outlook	Ruta completa y nombre de proceso de Microsoft Outlook Ejemplo: `C:\Archivos de programa\Microsoft Office \Office12\OUTLOOK.EXE`
Cliente de correo electrónico: todos los clientes que utilizan el protocolo SMTP	Ruta completa y nombre de proceso del cliente de correo electrónico Ejemplo: `C:\Archivos de programa\Mozilla Thunderbird \thunderbird.exe`
Almacenamiento extraíble	Nombre de proceso de la aplicación que realizó la transmisión de datos al dispositivo de almacenamiento o dentro de este Ejemplo: `explorer.exe`

CANAL	PROCESO
FTP	Ruta completa y nombre de proceso del cliente FTP Ejemplo: `D:\Archivos de programa\FileZilla FTP Client\filezilla.exe`
HTTP	"Aplicación HTTP"
HTTPS	Ruta completa y nombre de proceso del explorador o la aplicación Ejemplo: `C:\Archivos de programa\Internet Explorer\iexplore.exe`
Aplicación de MI	Ruta completa y nombre de proceso de la aplicación de MI Ejemplo: `C:\Archivos de programa\Skype\Phone\Skype.exe`
Aplicación de MI: MSN	• Ruta completa y nombre de proceso de MSN Ejemplo: `C:\Archivos de programa\Windows Live\Messenger\msnmsgr.exe` • "Aplicación HTTP" si los datos se transmiten desde una ventana de chat
Aplicación de igual a igual	Ruta completa y nombre de proceso de la aplicación de igual a igual Ejemplo: `D:\Archivos de programa\BitTorrent\bittorrent.exe`
Cifrado PGP	Ruta completa y nombre de proceso del software de cifrado PGP Ejemplo: `C:\Archivos de programa\PGP Corporation\PGP Desktop\PGPmnApp.exe`

CANAL	PROCESO
Impresora	Ruta completa y nombre de proceso de la aplicación que inició la operación de impresora Ejemplo: `C:\Archivos de programa\Microsoft Office\Office12\WINWORD.EXE`
Protocolo SMB	Ruta completa y nombre de proceso de la aplicación con la que se llevó a cabo la operación de acceso compartido (copia o creación de un archivo nuevo) Ejemplo: `C:\Windows\Explorer.exe`
Correo electrónico Web (modo HTTP)	"Aplicación HTTP"
Correo electrónico Web (modo HTTPS)	Ruta completa y nombre de proceso del explorador o la aplicación Ejemplo: `C:\Archivos de programa\Mozilla Firefox\firefox.exe`

Detalles de los registros de prevención de pérdida de datos

La pantalla **Detalles del registro de la Prevención de pérdida de datos** muestra detalles adicionales acerca de la transmisión de activos digitales. Los detalles de una transmisión varían dependiendo del canal y el proceso a través del cual OfficeScan detectó el incidente.

En la siguiente tabla figuran los detalles que se muestran.

TABLA 11-12. Detalles de los registros de prevención de pérdida de datos

DETALLES	DESCRIPCIÓN
Fecha/hora	La fecha y la hora en las que la prevención de pérdida de datos registró el incidente
ID de infracción	El ID exclusivo del incidente

Detalles	Descripción
Usuario	El nombre de usuario conectado al endpoint
Endpoint	El nombre del endpoint en el que la prevención de pérdida de datos ha detectado la transmisión
Dominio	El dominio del endpoint
IP	La dirección IP del endpoint
Canal	El canal mediante el cual se produjo la transmisión
Proceso	El proceso que facilitó la transmisión del activo digital (el proceso depende del canal) Para conocer más detalles, consulte *Procesos por canal en la página 11-62*.
Fuente	El origen del archivo que contiene el activo digital o canal (si no hay ningún origen disponible)
El correo electrónico del remitente	La dirección de correo electrónico en la que se originó la transmisión
Asunto del mensaje	La línea del asunto del mensaje de correo electrónico que contiene el activo digital
El destinatario del correo electrónico	Las direcciones de correo electrónico de destino del mensaje de correo electrónico
URL	La URL de un sitio o una página Web
El usuario de FTP	El nombre de usuario utilizado para conectarse al servidor FTP
La clase de archivo	El tipo de archivo en el que la prevención de pérdida de datos detectó el activo digital

DETALLES	DESCRIPCIÓN
Regla/Plantilla	Una lista de los nombres exactos y plantillas de regla que desencadenaron la detección **Nota** Cada regla puede contener varias plantillas que desencadenaron el incidente. Cuando hay varios nombres de plantillas se separan con comas.
Acción	Acción realizada sobre la transmisión
La razón de justificación del usuario	La razón que proporcionó el usuario para continuar transfiriendo los datos confidenciales

Activar el registro de depuración del módulo de Protección de datos

Procedimiento

1. Obtenga el archivo `logger.cfg` de su proveedor de asistencia.
2. Añada los siguientes datos en `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` (para sistemas de 32 bits) o `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite` (para sistemas de 64 bits):
   - **Tipo**: `String`
   - **Nombre**: `debugcfg`
   - **Valor**: `C:\Log\logger.cfg`
3. Cree una carpeta con el nombre «Log» en el directorio `C:\`.
4. Copie el archivo `logger.cfg` en la carpeta «Log».
5. Implemente la configuración de prevención de pérdida de datos y Control de dispositivos desde la consola Web para empezar a recopilar registros.

Nota

Para desactivar los registros de depuración del módulo de protección de datos, elimine `debugcfg` de la clave de registro y reinicie el endpoint.

Capítulo 12

Uso de Web Reputation

En este capítulo se describen las amenazas basadas en Web y el uso de OfficeScan para proteger la red y los equipos ante ellas.

Los temas que se incluyen son:

- *Acerca de las amenazas Web en la página 12-2*
- *Servicios de Command & Control Contact Alert en la página 12-2*
- *Reputación Web en la página 12-4*
- *Políticas de reputación Web en la página 12-5*
- *Notificaciones de amenazas Web para usuarios del agente en la página 12-14*
- *Notificaciones de rellamadas de C&C para administradores en la página 12-15*
- *Epidemias de rellamada de C&C en la página 12-20*
- *Registros de amenazas Web en la página 12-22*

Acerca de las amenazas Web

Las amenazas Web abarcan una amplia gama de amenazas que se originan en Internet. Las amenazas Web utilizan métodos sofisticados, con una combinación de diversos archivos y técnicas en lugar de un solo archivo o enfoque. Por ejemplo, los creadores de amenazas Web cambian constantemente la versión o variante que utilizan. Dado que la amenaza Web se encuentra en una ubicación fija de un sitio Web y no en un endpoint infectado, el creador de la amenaza Web modifica su código constantemente para evitar ser detectado.

En los últimos años, a los individuos denominados anteriormente hackers, programadores de virus, spammers y desarrolladores de spyware se les conoce ahora como delincuentes informáticos. Las amenazas Web ayudan a estos individuos a conseguir uno de sus dos objetivos. Un objetivo es robar información para venderla posteriormente. La consecuencia resultante es la fuga de información confidencial en forma de pérdida de identidad. El endpoint infectado también puede convertirse en un origen de ataques de phishing u otras actividades de recopilación de información. Entre otros efectos, esta amenaza puede repercutir negativamente en la fiabilidad del comercio por Internet y mermar la confianza que hace falta para realizar transacciones a través de la Web. El segundo objetivo es piratear la CPU de un usuario para utilizarla como instrumento para realizar actividades que les den beneficios. Entre estas actividades se incluye enviar spam o llevar a cabo extorsión mediante ataques distribuidos de negación de servicios o actividades de pago por clic.

Servicios de Command & Control Contact Alert

Los servicios de Command & Control (C&C) Contact Alert de Trend Micro proporcionan funciones mejoradas de detección y alerta para mitigar el daño que causan las amenazas continuas avanzadas y los ataques con destino. Los servicios de C&C Contact Alert se integran con los servicios de reputación Web que determinan la acción que se realizará cuando se detecten direcciones de rellamada, según el nivel de seguridad de la reputación Web.

La lista de IP de C&C mejora las detecciones de rellamadas C&C mediante el motor de inspección del contenido de red para identificar los contactos de C&C mediante cualquier canal de la red.

Para obtener información detallada sobre la configuración del nivel de seguridad de los Servicios de Reputación Web, consulte *Configurar una Política de reputación Web en la página 12-5*.

TABLA 12-1. Características de los servicios de C&C Contact Alert

CARACTERÍSTICA	DESCRIPCIÓN
Lista Global Intelligence	Trend Micro Smart Protection Network recopila la lista de Inteligencia global de orígenes procedentes de todo el mundo, y prueba y evalúa el nivel de riesgo de cada dirección de rellamada de C&C. Los Servicios de Reputación Web utilizan la lista Global Intelligence junto con las puntuaciones de reputación sobre sitios Web con contenido malicioso para proporcionar seguridad mejorada ante las amenazas avanzadas. El nivel de seguridad de la reputación Web determina la acción que se realizará cuando se encuentren sitios Web o servidores de C&C con contenido malicioso en función de los niveles de riesgo asignados.
Lista Analizador virtual	Los servidores Smart Protection Server se pueden integrar con Analizador virtual para obtener la lista de servidores de C&C de Analizador virtual. Analizador virtual evalúa los riesgos potenciales en un entorno seguro y, mediante el uso de métodos avanzados de comprobación heurísticos y de comportamiento, asigna un nivel de riesgo a las amenazas analizadas. Analizador virtual rellena la lista Analizador virtual con cualquier amenaza que intente conectarse a un posible servidor de C&C. La lista Analizador virtual está muy enfocada a cada empresa y proporciona una defensa más personalizada ante los ataques con destino. OfficeScan recupera la lista de Analizador virtual y, de este modo, puede comparar todas las posibles amenazas de C&C tanto con la lista de Inteligencia global como con la lista Analizador virtual local. Para obtener información detallada acerca de las listas de objetos sospechosos de Analizador virtual, consulte *Configuración de la lista de objetos sospechosos en la página 14-35*.
Servicio de conexión sospechosa	El servicio de conexión sospechosa gestiona las listas IP de C&C globales y definidas por el usuario, y supervisa el comportamiento de las conexiones que los endpoints establecen con los servidores C&C. Para conocer más detalles, consulte *Servicio de conexión sospechosa en la página 8-5*.

Característica	Descripción
Notificaciones para administradores	Los administradores pueden elegir si desean recibir notificaciones detalladas y personalizables cuando se detecta una rellamada de C&C. Para conocer más detalles, consulte *Configuración de notificaciones de rellamadas de C&C para administradores en la página 12-16*.
Notificaciones del agente	Los administradores pueden elegir si desean enviar notificaciones detalladas y personalizables a los usuarios finales cuando se detecta una rellamada de C&C en un endpoint. Para conocer más detalles, consulte *Notificaciones de C&C Contact Alert para los usuarios del agente en la página 12-19*.
Notificaciones de epidemias	Los administradores pueden personalizar las notificaciones de epidemias que son específicas para sucesos de rellamada de C&C y determinar si la epidemia ocurre en un endpoint único o en toda la red. Para conocer más detalles, consulte *Epidemias de rellamada de C&C en la página 12-20*.
Registros de rellamadas de C&C	Los registros proporcionan información detallada relacionada con todos los sucesos de rellamada de C&C. Para conocer más detalles, consulte *Visualización de los registros de rellamadas de C&C en la página 12-24*.

Reputación Web

La tecnología de reputación Web realiza un seguimiento de la credibilidad de los dominios Web mediante la asignación de un resultado de reputación basado en factores como la antigüedad del sitio Web, los cambios en la ubicación histórica y las indicaciones de actividades sospechosas descubiertas mediante el análisis de comportamientos malintencionados. A continuación seguirá con la exploración de los sitios y el bloqueo del acceso de los usuarios a los sitios infectados.

Los Agentes de OfficeScan envían consultas a los orígenes de Smart Protection para determinar la reputación de los sitios Web a los que los usuarios intentan acceder. La

reputación de los sitios Web se correlaciona con la política de reputación Web específica que se aplica en el endpoint. En función de la política que se utilice, el Agente de OfficeScan bloqueará o permitirá el acceso al sitio Web.

Nota

Para obtener información detallada acerca de las fuentes de Smart Protection, consulte *Lista de fuentes de Smart Protection en la página 4-23*.

Agregue los sitios Web que considere seguros o peligrosos a la lista de elementos permitidos o bloqueados. Cuando el Agente de OfficeScan detecta el acceso a uno de estos sitios Web, permite o bloquea automáticamente el acceso y deja de enviar consultas a los orígenes de Smart Protection.

Políticas de reputación Web

Las políticas de reputación Web establecen si OfficeScan bloqueará o permitirá el acceso a un sitio Web.

Puede configurar políticas para agentes internos y externos. Los administradores de OfficeScan suelen configurar una política más estricta para los agentes externos.

Las políticas constituyen una configuración granular en el árbol de agentes de OfficeScan. Puede aplicar determinadas políticas a grupos de agentes o a agentes individuales. También puede aplicar una única política a todos los agentes.

Después de implementar las políticas, los agentes utilizan los criterios de ubicación que haya definido en la pantalla **Ubicación del Endpoint** (consulte *Ubicación del Endpoint en la página 15-2*) para determinar sus ubicaciones y la política que se va a aplicar. Los agentes cambian de política cada vez que cambia la ubicación.

Configurar una Política de reputación Web

Especifique las credenciales de autenticación del servidor proxy si ha configurado un servidor proxy para administrar la comunicación HTTP en su organización y se requiere autenticación antes de que se permita el acceso Web.

Para obtener instrucciones sobre la configuración del proxy, consulte *Proxy externo para agentes de OfficeScan en la página 15-55*.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. Seleccione los destinos en el árbol de agentes.
   - Para configurar una política para agentes que ejecuten plataformas de escritorio de Windows, seleccione el icono del dominio raíz ( ), los dominios específicos o los agentes.

     Nota

     Cuando seleccione el dominio raíz o los dominios específicos, la configuración solo se aplicará a los agentes que ejecuten plataformas de escritorio de Windows. La configuración no se aplicará a los agentes que ejecuten plataformas de servidor de Windows, aunque formen parte de los dominios.
   - Para configurar una política para agentes que ejecutan plataformas de servidor de Windows, seleccione un agente determinado.
3. Haga clic en **Configuración** > **Configuración de la Reputación Web**.
4. Haga clic en la pestaña **Agentes externos** para configurar una política para agentes externos o en la pestaña **Agentes internos** para configurar una política para agentes internos.

   Consejo

   Defina la configuración de la ubicación del agente en caso de que no lo haya hecho. Los agentes utilizarán está configuración para determinar su ubicación y aplicar la política de reputación Web adecuada. Para conocer más detalles, consulte *Ubicación del Endpoint en la página 15-2*.
5. Seleccione **Activar política de reputación Web en los siguientes sistemas operativos**.

   La lista de sistemas operativos que aparece en la pantalla depende de los destinos seleccionados en el paso 1.

Consejo

Trend Micro recomienda desactivar Web Reputation en los agentes internos si ya utiliza un producto de Trend Micro con la función de Web Reputation, como InterScan Web Security Virtual Appliance.

Cuando se activa una política de reputación Web:

- Los agentes externos envían consultas de reputación Web a la Smart Protection Network.
- Los agentes internos envían las consultas de reputación Web a:
  - Smart Protection Servers si la opción **Enviar consultas a los Servidores de Smart Protection** está activada. Para obtener información detallada sobre esta opción, consulte el paso 7.
  - Red de Smart Protection si la opción **Enviar consultas a la Red de Smart Protection** está activada.

6. Seleccione **Activar el modo de valoración**.

Nota

En el modo de valoración, los agentes permitirán el acceso a todos los sitios Web, pero registrarán el acceso a los sitios Web que se encontrarían bloqueados si la valoración estuviera desactivada. Trend Micro ofrece el modo de valoración para evaluar los sitios Web y, a continuación, realizar las acciones pertinentes en función de su evaluación. Por ejemplo, los sitios Web que considere seguros los puede agregar a la lista de URL permitidas.

7. Seleccione **Comprobar URL de HTTPS**.

La comunicación HTTPS utiliza certificados para identificar servidores Web. Cifra los datos para evitar robos e interceptación. Aunque es más seguro, el acceso a sitios web con HTTPS sigue presentando riesgos. Los sitios comprometidos, incluso aquellos que cuentan con certificados válidos, pueden alojar malware y robar información personal. Además, los certificados son relativamente fáciles de obtener, y por lo tanto resulta sencillo configurar servidores web maliciosos que usen HTTPS.

Active la comprobación de URL de HTTPS para reducir el riesgo de exposición a sitios malintencionados y peligrosos que utilizan HTTPS. OfficeScan puede supervisar el tráfico HTTPS en los siguientes exploradores:

TABLA 12-2. Exploradores compatibles con el tráfico HTTPS

EXPLORADOR	VERSIÓN
Microsoft Internet Explorer	• 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 o posterior

Importante

- La exploración HTTP solamente admite plataformas de Windows 8, Windows 8.1, Windows 10 o Windows 2012 que funcionan en modo de escritorio.
- Después de habilitar la exploración HTTPS por primera vez en Agentes de OfficeScan, los usuarios deben activar el complemento necesario antes de que la exploración HTTPS esté operativa.
  - Firefox

    Agentes de OfficeScan que ejecuten Windows 7, 8, 8.1, 10, Server 2008 R2 o Server 2012: los usuarios deberán habilitar el complemento `Trend Micro Osprey Firefox Extension 2.0.0.1077` en la ventana emergente del explorador (o en la pantalla **Complementos** > **Extensiones**).

    Agentes de OfficeScan que ejecuten Windows XP, Vista, Server 2003 o Server 2008: los usuarios deberán habilitar el complemento `Trend Micro NSC Firefox Extension 5.82.0.1092` en la ventana emergente del explorador (o en la pantalla **Complementos** > **Extensiones**).
  - Internet Explorer 9, 10 y 11

    Agentes de OfficeScan que ejecuten Windows 7, 8, 8.1, 10, Server 2008 R2 o Server 2012: los usuarios deberán habilitar el complemento `Trend Micro Osprey Plugin Class` en la ventana emergente del explorador.

    Agentes de OfficeScan que ejecuten Windows XP, Vista, Server 2003 o Server 2008: los usuarios deberán habilitar el complemento `TmIEPlugInBHO Class` en la ventana emergente del explorador.

  Para obtener más información sobre cómo establecer los parámetros de configuración de Internet Explorer para reputación Web, consulte los siguientes artículos de la base de conocimientos:

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1095350.aspx

8. Seleccione **Explorar solo los puertos HTTP habituales** para restringir la exploración de reputación Web al tráfico que atraviesa los puertos 80, 81 y 8080. OfficeScan examina de forma predeterminada todo el tráfico de todos los puertos.

Nota

No compatible con Windows 7, 8, 8.1, 10 o Windows Server 2008 R2, 2012 o plataformas posteriores.

9. Seleccione **Enviar consultas a los servidores de Smart Protection Server** si desea que los agentes internos envíen consultas de reputación Web a los servidores Smart Protection Server.

   - Si activa esta opción:

     - Los agentes consultan la lista de fuentes de Smart Protection para determinar los servidores de Smart Protection Server a los que envían las consultas.

       Para obtener información acerca de la lista de fuentes de Smart Protection, consulte *Lista de fuentes de Smart Protection en la página 4-23*.

     - asegúrese de que haya servidores Smart Protection Servers disponibles. En caso de que no haya ninguno disponible, los agentes no enviarán consultas a la Smart Protection Network. Las únicas fuentes de datos de reputación Web de las que dispondrán los agentes serán las listas de direcciones URL permitidas y bloqueadas (configuradas en el paso 10).

     - Si desea que los agentes se conecten a los servidores de Smart Protection Server mediante un servidor proxy, especifique la configuración del proxy en **Administración** > **Configuración** > **Proxy > Proxy interno (pestaña)**.

     - Asegúrese de actualizar con regularidad los servidores Smart Protection Servers para que la protección se mantenga vigente.

     - Los agentes no bloquearán los sitios Web sin comprobar. Los servidores de Smart Protection Servers no almacenan datos de reputación Web de estos sitios Web.

   - Si desactiva esta opción:

     - El agente envía consultas de reputación Web a la Smart Protection Network. Los endpoints del agente deben disponer estar conectados a Internet para enviar consultas correctamente.

- Si la conexión a Smart Protection Network requiere una autenticación de servidor proxy, especifique las credenciales de autenticación en **Administración** > **Configuración** > **Proxy > Proxy externo (pestaña)** > **Conexión del agente de OfficeScan con servidores de Trend Micro**.

- Los agentes bloquearán los sitios Web sin comprobar si selecciona **Bloquear páginas que no han sido comprobadas por Trend Micro** en el paso 11.

10. Seleccione uno de los niveles de seguridad disponibles para la reputación Web: **Alto**, **Medio** o **Bajo**.

Nota

Los niveles de seguridad determinan si OfficeScan permitirá o bloqueará el acceso a una URL. Por ejemplo, si define un nivel de seguridad Bajo, OfficeScan solo bloquea las URL que son amenazas Web conocidas. Cuanto mayor sea el nivel de seguridad que configure, mayor será la tasa de detección de amenazas Web, pero también la posibilidad de falsos positivos.

11. Si ha desactivado la opción **Enviar consultas a los servidores Smart Protection Server** en el paso 9, puede seleccionar **Bloquear páginas que no han sido comprobadas por Trend Micro**.

Nota

Mientras que Trend Micro comprueba de forma activa la seguridad de las páginas Web, los usuarios pueden encontrarse con páginas sin comprobar cuando visitan sitios Web nuevos o menos conocidos. Si se bloquea el acceso a las páginas sin comprobar se aumenta la seguridad, pero también se puede impedir el acceso a páginas seguras.

12. Seleccione **Bloquear páginas que contienen secuencias de comandos maliciosas** para identificar explotaciones del explorador Web y secuencias de comandos maliciosas, y evitar que estas amenazas afecten al explorador Web.

OfficeScan utiliza el patrón de prevención de explotación del explorador y el patrón del analizador de secuencias de comando para identificar y bloquear páginas Web antes de exponer el sistema.

TABLA 12-3. Exploradores Web compatibles con la prevención de explotación del explorador

EXPLORADOR	VERSIÓN
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x

Importante

La característica de prevención de explotación del explorador requiere que active el Servicio de protección avanzada.

Para activar el servicio de protección avanzada, vaya a **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Configuración de servicios adicionales**.

Tras habilitar la característica Prevención de explotación del explorador por primera vez en los Agentes de OfficeScan, los usuarios deberán habilitar el complemento necesario en el explorador antes de que dicha característica esté operativa. En el caso de los Agentes de OfficeScan que ejecuten Internet Explorer 9, 10 u 11, los usuarios deberán habilitar el complemento `Protección de Trend Micro para IE` en la ventana emergente del explorador.

13. Configure las listas de elementos permitidos y bloqueados.

Nota

La lista de permitidos tiene preferencia sobre la lista de bloqueados. Cuando una URL coincide con una entrada de la lista de URL permitidas, los agentes siempre permiten el acceso a dicha URL, incluso si está también en la lista de URL bloqueadas.

a. Seleccione **Activar lista de permitidas/bloqueadas**.

b. Escriba una URL.

Puede agregar un carácter comodín (*) en cualquier posición de la URL.

Por ejemplo:

- Si escribe `www.trendmicro.com/*`, todas las páginas del sitio Web de Trend Micro estarán permitidas.
- Si escribe `*.trendmicro.com/*`, todas las páginas de todos los subdominios de `trendmicro.com` estarán permitidas.

Puede escribir URL que contengan direcciones IP. Si una URL contiene una dirección IPv6, escríbala entre paréntesis.

c. Haga clic en **Agregar a la lista de permitidos** o **Agregar a lista de bloqueados**.

d. Para exportar la lista a un archivo `.dat`, haga clic en **Exportar** y, a continuación, en **Guardar**.

e. Si ha exportado una lista desde otro servidor y desea importarla a esta pantalla, haga clic en **Importar** y busque el archivo `.dat`. La lista se cargará en la pantalla.

Importante

La reputación Web no realiza ninguna exploración en direcciones que aparezcan en las listas de URL permitidas y bloqueadas.

14. Para enviar comentarios sobre la reputación Web, haga clic en el proveedor de la URL en **Volver a valorar URL**. El sistema de consultas de reputación Web de Trend Micro se abre en una ventana del explorador.

15. Seleccione esta opción para permitir que el Agente de OfficeScan envíe registros de reputación Web al servidor. Debe permitir que los agentes envíen registros para poder analizar las URL que OfficeScan bloquea y tomar la acción apropiada en las URL que considera seguras.

16. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

- **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los

futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Notificaciones de amenazas Web para usuarios del agente

OfficeScan puede mostrar un mensaje de notificación en el endpoint del Agente de OfficeScan inmediatamente después de que bloquee una URL que infrinja la política de reputación Web. Es necesario que active el mensaje de notificación y que de forma opcional modifique su contenido.

Activar el mensaje de notificación de amenazas Web

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones**.
5. En la sección **Configuración de la reputación Web**, seleccione **Mostrar una notificación cuando se bloquea un sitio Web**.
6. En la sección **Configuración de rellamadas de C&C**, seleccione **Mostrar una notificación cuando se detecte una rellamada de C&C**.
7. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

- **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Modificar las notificaciones de amenazas Web

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. En la lista desplegable **Tipo**, seleccione el tipo de notificación de amenaza Web para modificarla:
   - **Infracciones de la reputación Web**
   - **Rellamadas de C&C**
3. Modifique el mensaje predeterminado en el cuadro de texto que aparece.
4. Haga clic en **Guardar**.

Notificaciones de rellamadas de C&C para administradores

OfficeScan incluye un conjunto de mensajes de notificación predeterminados para informarle a usted y a los administradores de OfficeScan de las detecciones de rellamadas de C&C. Puede modificar las notificaciones y definir la configuración de notificaciones adicionales según sus necesidades.

Configuración de notificaciones de rellamadas de C&C para administradores

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Administrador**.
2. En la pestaña **Criterios**:
   a. Vaya a la sección **Rellamadas de C&C**.
   b. Especifique si las notificaciones se enviarán cuando OfficeScan detecte una rellamada de C&C (la acción se puede bloquear u registrar) o solo cuando el nivel de riesgo de la dirección de rellamada sea Alto.
3. En la pestaña **Correo electrónico**:
   a. Vaya a la sección **Rellamadas de C&C**.
   b. Seleccione **Activar la notificación por correo electrónico**.
   c. Seleccione **Enviar notificaciones a los usuarios con permisos de dominio del árbol de agentes**.

      Utilice la administración basada en funciones para conceder a los usuarios permisos de dominio del árbol de agentes. Si se produce una transmisión en un agente que pertenezca a un dominio específico, se enviará un correo electrónico a las direcciones de correo electrónico de los usuarios con permisos de dominio. Consulte los ejemplos de la siguiente tabla:

TABLA 12-4. Dominios y permisos del árbol de agentes

DOMINIO DEL ÁRBOL DE AGENTES	FUNCIONES CON PERMISOS DE DOMINIO	CUENTA DE USUARIO CON LA FUNCIÓN	DIRECCIÓN DE CORREO ELECTRÓNICO PARA LA CUENTA DE USUARIO
Dominio A	Administrador (integrado)	raíz	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Dominio B	Administrador (integrado)	raíz	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un Agente de OfficeScan que pertenece al dominio A detecta una rellamada de C&C, el correo electrónico se enviará a mary@xyz.com, john@xyz.com y chris@xyz.com.

Si el Agente de OfficeScan que pertenece al dominio B detecta la rellamada de C&C, el mensaje de correo electrónico se enviará a las direcciones mary@xyz.com y jane@xyz.com.

Nota

Si se activa esta opción, todos los usuarios con permisos de dominio deben tener una dirección de correo electrónico correspondiente. El correo electrónico de notificación no se enviará a los usuarios sin dirección de correo electrónico. Los usuarios y las direcciones de correo electrónico se configuran en **Administración** > **Administración de cuentas** > **Cuentas de usuario**.

d. Seleccione **Enviar notificaciones a la(s) siguiente(s) dirección(es) de correo electrónico** y, después, escriba las direcciones de correo electrónico.

e. Acepte o modifique el asunto y el mensaje predeterminados. Utilice variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 12-5. Variables de símbolo para notificaciones de rellamadas de C&C

VARIABLE	DESCRIPCIÓN
%CLIENTCOMPUTER%	endpoint del destino que envió la rellamada
%IP%	Dirección IP del endpoint de destino
%DOMAIN%	Dominio del equipo
%DATETIME%	Fecha y hora en las que se detectó la transmisión
%CALLBACKADDRESS%	Dirección de rellamada del servidor C&C
%CNCRISKLEVEL%	Nivel de riesgo del servidor C&C
%CNCLISTSOURCE%	Indica la lista de orígenes de C&C
%ACTION%	Acción ejecutada

4. En la pestaña **Captura SNMP**:
   a. Vaya a la sección **Rellamadas de C&C**.
   b. Seleccione **Activar la notificación por captura SNMP**.
   c. Acepte o modifique el mensaje predeterminado. Utilice variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 12-5: Variables de símbolo para notificaciones de rellamadas de C&C en la página 12-18* para obtener más información.
5. En la pestaña **Registro de sucesos de NT**:
   a. Vaya a la sección **Rellamadas de C&C**.
   b. Seleccione **Activar la notificación por el registro de sucesos de NT**.
   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 12-5: Variables de símbolo para notificaciones de rellamadas de C&C en la página 12-18* para obtener más información.

6. Haga clic en **Guardar**.

Notificaciones de C&C Contact Alert para los usuarios del agente

OfficeScan puede mostrar un mensaje de notificación en equipos del Agente de OfficeScan inmediatamente después de bloquear una URL de servidor C&C. Es necesario que active el mensaje de notificación y que de forma opcional modifique su contenido

Activar el mensaje de notificación de rellamada de C&C

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones**.
5. En la sección **Configuración de rellamadas de C&C**, seleccione **Mostrar una notificación cuando se detecte una rellamada de C&C**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Modificar las notificaciones de rellamadas de C&C

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. En el menú desplegable **Tipo**, seleccione **Rellamadas de C&C**.
3. Modifique el mensaje predeterminado en el cuadro de texto que aparece.
4. Haga clic en **Guardar**.

Epidemias de rellamada de C&C

Defina una epidemia de rellamada de C&C por el número, el origen y el nivel de riesgo de las rellamadas.

OfficeScan incluye un mensaje de notificación predeterminado que le informa a usted y a los demás administradores de OfficeScan en caso de que se produzca una epidemia. Puede modificar el mensaje de notificación según sus necesidades.

Nota

OfficeScan puede enviar notificaciones de epidemias de rellamada de C&C mediante correo electrónico. Defina la configuración del correo electrónico para permitir que OfficeScan envíe mensajes de correo electrónico correctamente. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

Configuración de los criterios y las notificaciones de las epidemias de rellamadas de C&C

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Epidemia**.
2. En la pestaña **Criterios**, configure las siguientes opciones:

Opción	Descripción
El mismo host comprometido	Selecciónela para definir una epidemia en función de las detecciones de rellamadas por endpoint
Nivel de riesgo de C&C	Especifique si va a activar una epidemia en todas las rellamadas de C&C o solo en los orígenes de riesgo elevado.
Acción	Seleccione de entre las opciones **Cualquier acción**, **Conectado** o **Bloqueado**
Detecciones	Indique el número necesario de detecciones que defina una epidemia
Periodo de tiempo	Indique el número de horas necesario durante las que el número de detecciones debe producirse

Consejo

Trend Micro recomienda aceptar los valores predeterminados de esta pantalla.

3. En la pestaña **Correo electrónico**:
   a. Vaya a la sección **Rellamadas de C&C**.
   b. Seleccione **Activar la notificación por correo electrónico**.
   c. Especifique los destinatarios del correo electrónico.
   d. Acepte o modifique el asunto y el mensaje predeterminados del correo electrónico. Puede utilizar variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 12-6. Variables de símbolo para notificaciones de epidemias de rellamadas de C&C

VARIABLE	DESCRIPCIÓN
%C	Número de registros de rellamadas de C&C
%T	Periodo de tiempo durante el cual se acumulan registros de rellamadas de C&C

e. Seleccione de entre la información adicional de rellamadas de C&C que esté disponible para incluirla en el correo electrónico.

4. En la pestaña **Captura SNMP**:

   a. Vaya a la sección **Rellamadas de C&C**.

   b. Seleccione **Activar la notificación por captura SNMP**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 12-6: Variables de símbolo para notificaciones de epidemias de rellamadas de C&C en la página 12-22* para obtener más información.

5. En la pestaña **Registro de sucesos de NT**:

   a. Vaya a la sección **Rellamadas de C&C**.

   b. Seleccione **Activar la notificación por el registro de sucesos de NT**.

   c. Acepte o modifique el mensaje predeterminado. Puede utilizar variables de símbolo para representar los datos en el campo **Mensaje**. Consulte *Tabla 12-6: Variables de símbolo para notificaciones de epidemias de rellamadas de C&C en la página 12-22* para obtener más información.

6. Haga clic en **Guardar**.

Registros de amenazas Web

Configure los agentes tanto internos como externos para enviar los registros de reputación Web al servidor. Permítalo si desea analizar las direcciones URL que

OfficeScan bloquea y tomar las medidas oportunas en las direcciones URL que considera seguras.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Ver registros de reputación Web

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Ver registros** > **Registros de reputación Web** o **Registros** > **Registros de reputación Web**.
4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
5. Visualice los registros. Los registros contienen la siguiente información:

EVENTO	DESCRIPCIÓN
Fecha/hora	La hora a la que se produjo la detección
Endpoint	El endpoint en el que tuvo lugar la detección
Dominio	El dominio del endpoint en el que tuvo lugar la detección
URL	La URL bloqueada por los servicios de reputación Web
El nivel de riesgo	El nivel de riesgo de la URL
Descripción	Una descripción de la amenaza de seguridad

Evento	Descripción
Proceso	El proceso mediante el cual se produjo el contacto (path\application_name)
Acción	La acción realizada tras la detección

6. Si hay URL que no deberían estar bloqueadas, haga clic en el botón **Agregar a la lista de permitidos** para agregar el sitio Web a la lista de URL permitidas.

7. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar todo a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Visualización de los registros de rellamadas de C&C

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.

3. Haga clic en **Ver registros** > **Registros de rellamadas de C&C** o **Logs** > **Registros de rellamadas de C&C**.

4. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.

5. Visualice los registros. Los registros contienen la siguiente información:

Evento	Descripción
Fecha/hora	La hora a la que se produjo la detección
Usuario	El usuario conectado en el momento de la detección
Host comprometido	El endpoint desde el que se originó la rellamada
Dirección IP	La dirección IP del host comprometido

EVENTO	DESCRIPCIÓN
Dominio	El dominio del endpoint en el que tuvo lugar la detección
Dirección de rellamada	La dirección de rellamada a la que el endpoint envió la rellamada
Origen de lista de C&C	Origen de lista de C&C que identificó el servidor C&C
Nivel de riesgo de C&C	Nivel de riesgo del servidor C&C
Protocolo	El protocolo de Internet que se usó para la transmisión
Proceso	El proceso que inició la transmisión (path \application_name)
Acción	La acción realizada sobre la rellamada

6. Si la reputación Web bloqueó una URL que no desea que se bloquee, haga clic en el botón **Agregar a lista de permitidas de la reputación Web** para agregar la dirección a lista de permitidas de la reputación Web.

Nota

OfficeScan solo puede agregar URL a la lista de permitidas de la reputación Web. En las detecciones realizadas por la lista IP de C&C global o la lista de C&C de Analizador virtual (IP), agregue manualmente estas direcciones IP a la lista IP de C&C permitidas definida por el usuario.

Para conocer más detalles, consulte *Configurar los ajustes de las listas de IP generales definidas por el usuario en la página 8-6*.

7. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar todo a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Capítulo 13

Uso de OfficeScan Firewall

En este capítulo se describen las características y la configuración de OfficeScan Firewall.

Los temas que se incluyen son:

- *Acerca de OfficeScan Firewall en la página 13-2*
- *Activar o desactivar OfficeScan Firewall en la página 13-6*
- *Perfiles y políticas del cortafuegos en la página 13-8*
- *Derechos del cortafuegos en la página 13-24*
- *Configuración general del cortafuegos en la página 13-26*
- *Notificaciones de infracciones del cortafuegos para los usuarios del agente de OfficeScan en la página 13-29*
- *Registros del cortafuegos en la página 13-30*
- *Epidemias de infracciones del cortafuegos en la página 13-32*
- *Comprobar OfficeScan Firewall en la página 13-34*

Acerca de OfficeScan Firewall

El cortafuegos de OfficeScan protege los agentes y servidores de la red mediante la inspección de estados y la exploración de virus de red de alto rendimiento. A través de la consola de administración central se pueden crear reglas para filtrar las conexiones por aplicación, dirección IP, número de puerto o protocolo, y aplicarlas a continuación a diferentes grupos de usuarios.

Nota

Puede activar, configurar y utilizar el cortafuegos de OfficeScan en endpoints Windows XP en los que también se ha activado Firewall de Windows. No obstante, administre las políticas con sumo cuidado para no crear políticas de cortafuegos que entren en conflicto ni obtener resultados inesperados. Consulte la documentación de Microsoft para obtener más información sobre Firewall de Windows.

OfficeScan Firewall incluye las siguientes ventajas y funciones clave:

- *Filtrado de tráfico en la página 13-2*
- *Filtro de aplicaciones en la página 13-3*
- *Lista de software seguro certificado en la página 13-3*
- *Buscar virus de red en la página 13-3*
- *Perfiles y políticas personalizables en la página 13-4*
- *Inspección de estado en la página 13-4*
- *Sistema de detección de intrusiones en la página 13-4*
- *Supervisor de epidemias de infracciones del cortafuegos en la página 13-6*
- *Derechos del cortafuegos del agente de OfficeScan en la página 13-6*

Filtrado de tráfico

El cortafuegos de OfficeScan filtra todo el tráfico de entrada y de salida, lo que le permite bloquear determinados tipos de tráfico según los criterios que se indican a continuación:

- Dirección (entrada/salida)
- Protocolo (TCP/UDP/ICMP/ICMPv6)
- Puertos de destino
- Endpoints de origen y destino

Filtro de aplicaciones

El cortafuegos de OfficeScan filtra el tráfico entrante y saliente para aplicaciones específicas, de forma que permite que estas aplicaciones accedan a la red. Sin embargo, las conexiones de red dependerán de las políticas definidas por el administrador.

Lista de software seguro certificado

La Lista de software seguro certificado ofrece una lista de aplicaciones que pueden omitir los niveles de seguridad de la política del cortafuegos. En caso de que el nivel de seguridad esté establecido en Medio o Alto, OfficeScan aún permitirá que se ejecuten aplicaciones y que éstas accedan a la red.

Active las consultas de la lista de software seguro certificado de carácter global que le ofrece una lista más completa. Se trata de una lista que Trend Micro actualiza de forma dinámica.

Nota

Esta opción funciona con la Supervisión de comportamiento. Asegúrese de que activa el Servicio de prevención de cambios no autorizados y el Servicio de software seguro certificado antes de activar la Lista de software seguro certificado global.

Buscar virus de red

El cortafuegos de OfficeScan también examina cada paquete en busca de virus de red. Para conocer más detalles, consulte *Virus y malware en la página 7-2*.

Perfiles y políticas personalizables

El cortafuegos de OfficeScan permite configurar políticas para bloquear o permitir determinados tipos de tráfico de red. Las políticas se pueden asignar a uno o más perfiles, que a su vez pueden implementarse en los Agentes de OfficeScan que se desee. Es un método con un nivel de personalización elevado para organizar y definir la configuración del cortafuegos de los agentes.

Inspección de estado

El cortafuegos de OfficeScan es un cortafuegos con funciones de inspección de estado que supervisa todas las conexiones con el Agente de OfficeScan y recuerda todos los estados de conexión. Puede identificar condiciones específicas en cualquier conexión, predice las acciones que pueden suceder a continuación y detecta las interrupciones en una conexión normal. Por tanto, un uso eficaz del cortafuegos no sólo implica crear perfiles y políticas, sino también analizar paquetes de conexiones y filtros que pasen a través del cortafuegos.

Sistema de detección de intrusiones

El cortafuegos de OfficeScan también incluye un sistema de detección de intrusiones (IDS). Cuando está activado, el sistema IDS ayuda a identificar patrones de los paquetes de red que pueden indicar un ataque al Agente de OfficeScan. El cortafuegos de OfficeScan evita que se produzcan las siguientes intrusiones conocidas:

SISTEMA DE	DESCRIPCIÓN
Fragmento demasiado grande	un ataque de denegación de servicio en que un hacker envía un paquete TCP/UDP de gran tamaño al endpoint de destino. Como consecuencia, se produce un desbordamiento del búfer del endpoint que puede colapsar o reiniciar el endpoint.
Ping de la muerte	un ataque de denegación de servicio en el que un hacker envía un paquete ICMP/ICMPv6 de gran tamaño a un endpoint de destino. Como consecuencia, se produce un desbordamiento del búfer del endpoint que puede colapsar o reiniciar el endpoint.

Sistema de	Descripción
ARP en conflicto	un tipo de ataque en el que un hacker envía una solicitud ARP (Protocolo de resolución de direcciones) con la misma dirección IP de origen y de destino al endpoint objetivo. El endpoint de destino se envía a sí mismo ininterrumpidamente una respuesta ARP (la dirección MAC), lo que provoca el colapso o bloqueo de este.
Desbordamiento SYN	un ataque de denegación de servicio en el que un programa envía numerosos paquetes TCP de sincronización (SYN) al endpoint, lo que provoca que el endpoint envíe de forma continua respuestas de confirmación de sincronización (SYN/ACK). Este ataque puede desbordar la memoria del endpoint y, finalmente, llegar a colapsar el endpoint.
Solapamiento de fragmentos	Similar a un ataque Teardrop, este ataque de denegación de servicio envía fragmentos TCP solapados a un endpoint. Sobrescribe la información de encabezado del primer fragmento TCP y puede atravesar un cortafuegos. El cortafuegos permite entonces que los fragmentos posteriores, con contenido malicioso, entren en el endpoint.
Teardrop	Similar a un ataque de solapamiento de fragmentos, este ataque de denegación de servicio utiliza fragmentos IP. Un valor de compensación confuso en el segundo fragmento de IP, o en otro posterior, puede provocar que el sistema operativo del endpoint receptor se bloquee al intentar volver a unir los fragmentos.
Ataque con fragmentos pequeños	Un tipo de ataque en el que un tamaño reducido de un fragmento TCP obliga a introducir la información de encabezamiento del primer paquete TCP en el siguiente fragmento. Esto puede hacer que los enrutadores que filtran el tráfico ignoren los siguientes fragmentos, los cuales pueden contener información maliciosa.
IGMP fragmentado	un ataque de denegación de servicio en el que se envían paquetes IGMP fragmentados al endpoint de destino que no los puede procesar correctamente. Esto puede ocasionar el colapso y la ralentización del endpoint.

SISTEMA DE	DESCRIPCIÓN
Ataque LAND	un tipo de ataque que envía paquetes IP de sincronización (SYN) con la misma dirección de origen y destino al endpoint y que provoca que endpoint se envíe a sí mismo la respuesta de confirmación de sincronización (SYN/ACK). Esto puede ocasionar el colapso y la ralentización del endpoint.

Supervisor de epidemias de infracciones del cortafuegos

El cortafuegos de OfficeScan envía un mensaje de notificación personalizado a los destinatarios especificados cuando las infracciones del cortafuegos superan determinados umbrales, lo que puede ser indicio de un ataque.

Derechos del cortafuegos del agente de OfficeScan

Conceda el derecho de ver la configuración del cortafuegos a los usuarios del Agente de OfficeScan en la consola del agente de Agente de OfficeScan. Concédales también el derecho de activar o desactivar el cortafuegos, el sistema de detección de intrusiones y el mensaje de notificación de infracciones del cortafuegos.

Activar o desactivar OfficeScan Firewall

Durante la instalación del servidor de OfficeScan, se le solicitará que active o desactive OfficeScan Firewall.

Si activó el cortafuegos durante la instalación y ha notado una reducción del rendimiento, sobre todo en las plataformas del servidor (Windows Server 2003, Windows Server 2008 y Windows Server 2012), considere la desactivación de dicho cortafuegos.

Si ha desactivado el cortafuegos durante la instalación, pero ahora desea activarlo para proteger al agente frente a intrusiones, lea primero las directrices e instrucciones de *Servicios del agente de OfficeScan en la página 15-7*.

Puede activar o desactivar el cortafuegos en todos los endpoints del Agente de OfficeScan, o en aquellos que seleccione.

Activación o desactivación del cortafuegos de OfficeScan en todos los endpoints seleccionados

Utilice uno de los siguientes métodos para activar o desactivar el cortafuegos en la consola Web.

MÉTODO	PROCEDIMIENTO
Crear una nueva política y aplicarla a los Agentes de OfficeScan	1. Cree una nueva política que active/desactive el cortafuegos. Para ver los pasos que hay que realizar para crear una política nueva, consulte *Agregar una política de cortafuegos en la página 13-11*. 2. Aplique la política a los Agentes de OfficeScan.
activar/desactivar el servicio del cortafuegos en la consola Web.	Para obtener información detallada acerca de los pasos que se deben seguir, consulte *Servicios del agente de OfficeScan en la página 15-7*. **Nota** Desactivar el servicio de cortafuegos deshabilita automáticamente todas las políticas de cortafuegos de los agentes seleccionados.

Utilice uno de los siguientes métodos para activar o desactivar el cortafuegos en los endpoints seleccionados.

MÉTODO	PROCEDIMIENTO
Activar/desactivar el controlador del cortafuegos	1. Abra **Propiedades de conexión de red de Windows**. 2. Active o desactive la casilla de verificación **Driver del cortafuegos común de Trend Micro** de la tarjeta de red.

MÉTODO	PROCEDIMIENTO
Activar/desactivar el servicio del cortafuegos	1. Abra el símbolo del sistema y escriba `services.msc`. 2. Inicie o detenga el **cortafuegos de OfficeScan NT** en Microsoft Management Console (MMC).

Activación o desactivación del cortafuegos de OfficeScan en todos los endpoints

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Licencia del producto**.
2. Vaya a la sección **Servicios adicionales**.
3. En la sección **Servicios adicionales**, junto a la fila **Cortafuegos para Endpoints en red**, haga clic en **Activado** o **Desactivado**.

Perfiles y políticas del cortafuegos

El cortafuegos de OfficeScan utiliza políticas y perfiles para organizar y personalizar los métodos de protección de los endpoints conectados en red.

Con la integración de Active Directory y la Role-based Administration, cada función de usuario, en función de los permisos con los que cuente, puede crear, configurar o eliminar políticas y perfiles para dominios específicos.

Consejo

Si hay varias instalaciones de cortafuegos en el mismo endpoint, se pueden producir resultados inesperados. Considere la opción de desinstalar otras aplicaciones de cortafuegos basadas en software de los Agentes de OfficeScan antes de implementar y activar el cortafuegos de OfficeScan.

Es necesario seguir estos pasos para utilizar correctamente OfficeScan Firewall:

1. Crear una política: la política le permite seleccionar un nivel de seguridad que bloquea o permite el tráfico en los endpoints conectados en red y activa las funciones del cortafuegos.

2. Añadir excepciones a la política: las excepciones permiten a los Agentes de OfficeScan evitar una política. Gracias a las excepciones se pueden especificar agentes y permitir o bloquear determinados tipos de tráfico, a pesar de la configuración del nivel de seguridad de la política. Por ejemplo, bloquee todo el tráfico de un conjunto de agentes en una política, pero cree una excepción que permita el tráfico HTTP para que los agentes puedan acceder a un servidor Web.

3. Cree y asigne perfiles a los Agentes de OfficeScan. Un perfil de cortafuegos incluye un conjunto de atributos del agente y se asocia a una política. Cuando un agente tiene los atributos especificados en el perfil, se activa la política asociada.

Políticas del cortafuegos

Las políticas del cortafuegos le permiten bloquear o permitir determinados tipos de tráfico de red no especificados en una política de excepciones. Una política también define que funciones del cortafuegos se activan o desactivan. Asigne una política a uno o varios perfiles del cortafuegos.

Con la integración de Active Directory y la Role-based Administration, cada función de usuario, en función de los permisos con los que cuente, puede crear, configurar o eliminar políticas para dominios específicos.

En la siguiente tabla se describen los ajustes disponibles durante la configuración de una política de cortafuegos.

CONFIGURACIÓN	DESCRIPCIÓN
Nivel de seguridad	Una configuración general que bloquea o permite todo el tráfico entrante o saliente en el endpoint del Agente de OfficeScan.
Funciones del cortafuegos	Especifique si desea activar o desactivar el cortafuegos de OfficeScan, el sistema de detección de intrusiones (IDS) y el mensaje de notificación de infracciones del cortafuegos. Para conocer más detalles, consulte *Sistema de detección de intrusiones en la página 13-4*.

Configuración	Descripción
Lista de software seguro certificado	especifique si desea permitir que las aplicaciones certificadas seguras se conecten a la red. Para conocer más detalles, consulte *Lista de software seguro certificado en la página 13-3*.
Lista de excepciones de políticas	una lista de excepciones configurables para bloquear o permitir diversos tipos de tráfico de red.

Nota

Puede conceder a los usuario finales el derecho para modificar el nivel de seguridad y la lista de excepciones de políticas al crear perfiles del cortafuegos.

Para conocer más detalles, consulte *Agregar un perfil del cortafuegos en la página 13-21*.

Políticas predeterminadas del cortafuegos

OfficeScan incluye un conjunto de políticas predeterminadas que puede modificar o eliminar.

Nombre de la política	Nivel de seguridad	Configuración de Agente	Excepciones	Uso recomendado
Acceso total	Bajo	Activar cortafuegos	Ninguna	Utilícela para permitir a los agentes acceder a la red sin restricciones.
Puertos de comunicación para Trend Micro Control Manager	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP/UDP entrante y saliente a través de los puertos 80 y 10319	Utilícela cuando los agentes tengan una instalación del agente MCP.

Nombre de la política	Nivel de seguridad	Configuración de Agente	Excepciones	Uso recomendado
Consola de ScanMail for Microsoft Exchange	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 16372	Utilice esta opción cuando los agentes necesiten acceder a la consola de ScanMail.
Consola de InterScan Messaging Security Suite (IMSS)	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 80	Utilice esta opción cuando los agentes necesiten acceder a la consola de IMSS.

Agregar una política de cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Políticas**.
2. Para añadir una nueva política, haga clic en **Agregar**.

   Si la nueva política que desea crear tiene valores de configuración similares a los de la política existente, seleccione la política existente y haga clic en **Copiar**.
3. Escriba el nombre de la política.
4. Seleccione un nivel de seguridad.

   El nivel de seguridad seleccionado no se aplicará al tráfico que coincida con los criterios de la excepción de política del cortafuegos.
5. Seleccione las funciones del cortafuegos que deben utilizarse para la política.

   - El mensaje de notificación de infracción del cortafuegos se muestra cuando el cortafuegos bloquea un paquete saliente. Para modificar el mensaje, consulte *Modificar el contenido del mensaje de notificación del cortafuegos en la página 13-30*.
   - Si el administrador activa todas las funciones del cortafuegos y concede a los usuarios del Agente de OfficeScan derechos para configurar el cortafuegos,

los usuarios podrán activar/desactivar las funciones y modificar la configuración del cortafuegos en la consola del Agente de OfficeScan.

¡ADVERTENCIA!

No podrá utilizar la consola Web de OfficeScan para sobrescribir la configuración de la consola del Agente de OfficeScan que utilice el usuario.

- Si no activa las funciones, la configuración del cortafuegos que defina desde la consola Web de OfficeScan aparecerá en la **Lista de tarjetas de red** en la consola del Agente de OfficeScan.
- La información que aparece en **Configuración** en la pestaña **Cortafuegos** de la consola del Agente de OfficeScan siempre muestra la configuración establecida desde la consola del Agente de OfficeScan, no desde la consola Web del servidor.

6. Active la lista de software seguro certificado global o local.

Nota

Asegúrese de que el Servicio de prevención de cambios no autorizados y los Servicios de software seguro certificado se han activado antes de activar este servicio.

7. En Excepción, seleccione las excepciones de políticas del cortafuegos. Las excepciones de políticas incluidas se definen según la plantilla de excepción del cortafuegos. Consulte *Editar la plantilla de excepciones del cortafuegos en la página 13-13* para obtener más información.
   - Modifique una excepción de política definida; para ello, haga clic en el nombre de la excepción de política y cambie la configuración en la página que se abre.

Nota

La excepción de política modificada no se aplicará a la política que se crea. Si desea que la modificación de la excepción de la política sea permanente, deberá realizar la misma modificación a la excepción de la política en la plantilla de excepción de cortafuegos.

   - Haga clic en **Agregar** para crear una nueva excepción de política. Especifique la configuración en la página que se abre.

Nota

La excepción de política también se aplicará sólo a la política que se crea. Para aplicar esta excepción de política a otras políticas, debe agregarla primero a la lista de excepciones de políticas en la plantilla de excepción del cortafuegos.

8. Haga clic en **Guardar**.

Modificar una política de cortafuegos existente

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Políticas**.
2. Haga clic en una política.
3. Modifique los siguientes parámetros:
   - Nombre de la política
   - Nivel de seguridad
   - Funciones del cortafuegos que deben utilizarse para la política
   - Estado de la Lista del servicio de software seguro certificado
   - Excepciones de políticas del cortafuegos que deben incluirse en la política
     - Edite una excepción de política existente (haga clic en el nombre de la excepción de política y cambie la configuración en la página que se abre).
     - Haga clic en **Agregar** para crear una nueva excepción de política. Especifique la configuración en la página que se abre.
4. Haga clic en **Guardar** para aplicar las modificaciones a la política existente.

Editar la plantilla de excepciones del cortafuegos

La plantilla de excepciones del cortafuegos contiene las excepciones de políticas que pueden configurarse para permitir o bloquear diferentes tipos de tráfico de red en

función de los números de puerto y las direcciones IP de los endpoint del Agente de OfficeScan. Cuando termine de crear una excepción de política, edite las políticas a las que se aplicará.

Decida qué tipo de excepción de política desea utilizar. Existen dos tipos:

- **Restrictivas**

  Bloquea solo determinados tipos de tráficos de red y se aplican a las políticas que permiten todo el tráfico de red. Un ejemplo de uso de una excepción de política restrictiva es bloquear los puertos del Agente de OfficeScan vulnerables a ataques, como los puertos que los troyanos utilizan con mayor frecuencia.

- **Permisivas**

  Permiten solo determinados tipos de tráficos de red y se aplican a las políticas que bloquean todo el tráfico de red. Por ejemplo, puede permitir que los Agentes de OfficeScan accedan solo al servidor de OfficeScan y a un servidor Web. Para ello, permita el tráfico desde el puerto de confianza (utilizado para la comunicación con el servidor de OfficeScan) y el puerto que el Agente de OfficeScan utiliza para la comunicación HTTP.

  Puerto de escucha del Agente de OfficeScan: **Agentes** > **Administración de agentes > Estado**. El número de puerto se encuentra bajo **Información básica**.

  Puerto de escucha del servidor: **Administración** > **Configuración** > **Conexión del agente**. El número de puerto se encuentra en **Configuración de conexión del agente**.

  OfficeScan incluye un conjunto de excepciones de políticas de cortafuegos predeterminadas que puede modificar o eliminar.

TABLA 13-1. Excepciones de políticas del cortafuegos predeterminadas

NOMBRE DE LA EXCEPCIÓN	ACCIÓN	PROTOCOLO	PUERTO	DIRECCIÓN
DNS	Permitir	TCP/UDP	53	Entrante y saliente
NetBIOS	Permitir	TCP/UDP	137, 138, 139, 445	Entrante y saliente

Nombre de la excepción	Acción	Protocolo	Puerto	Dirección
HTTPS	Permitir	TCP	443	Entrante y saliente
HTTP	Permitir	TCP	80	Entrante y saliente
Telnet	Permitir	TCP	23	Entrante y saliente
SMTP	Permitir	TCP	25	Entrante y saliente
FTP	Permitir	TCP	21	Entrante y saliente
POP3	Permitir	TCP	110	Entrante y saliente
LDAP	Permitir	TCP/UDP	389	Entrante y saliente

Nota

Las excepciones predeterminadas se aplican a todos los agentes. Si desea aplicar una excepción predeterminada solo a determinados agentes, modifíquela y especifique las direcciones IP de los agentes.

La excepción LDAP no está disponible si actualiza desde una versión anterior de OfficeScan. Agregue esta excepción manualmente si no aparece en la lista de excepciones.

Agregar una excepción de política de cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Políticas**.
2. Haga clic en **Editar la plantilla de excepciones**.
3. Haga clic en **Agregar**.
4. Escriba el nombre de la excepción de política.
5. Seleccione el tipo de aplicación. Puede seleccionar todas las aplicaciones o, por el contrario, especificar las claves de registro o la ruta de aplicación.

Nota

Compruebe el nombre y las rutas completas introducidos. La excepción de la aplicación no admite comodines.

6. Seleccione la acción que va a llevar a cabo OfficeScan en el tráfico de red (bloquear o permitir el tráfico que cumple con los criterios de excepción) y la dirección del tráfico (el tráfico de red entrante o saliente del endpoint del Agente de OfficeScan).
7. Seleccione el tipo de protocolo de red: TCP, UDP, ICMP o ICMPv6.
8. Especifique los puertos del endpoint del Agente de OfficeScan en los que se va a realizar la acción.
9. Seleccione las direcciones IP de los endpoint del Agente de OfficeScan que desee incluir en la excepción. Por ejemplo, si decide denegar todo el tráfico de red (entrante y saliente) y escribe la dirección IP de un único endpoint de la red, cualquier Agente de OfficeScan que tenga esta excepción en su política no podrá enviar ni recibir datos a través de dicha dirección IP.
   - **Todas las direcciones IP**: incluye todas las direcciones IP.
   - **Dirección IP única**: escriba una dirección IPv4 o IPv6 o un nombre de host.
   - **Intervalo (para IPv4 o IPv6)**: escriba un intervalo de direcciones IPv4 o IPv6.
   - **Intervalo (para IPv6)**: escriba un prefijo y una longitud de dirección IPv6.
   - **Máscara de subred**: escriba una dirección IPv4 y su máscara de subred.
10. Haga clic en **Guardar**.

Modificar una excepción de política de cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Políticas**.
2. Haga clic en **Editar la plantilla de excepciones**.

3. Haga clic en una excepción de política
4. Modifique los siguientes parámetros:
   - Nombre de la excepción de política
   - Ruta, nombre y tipo de aplicación
   - Acción que emprenderá OfficeScan en el tráfico de red y en la dirección del tráfico
   - Tipo de protocolo de red
   - Números de puertos para la excepción de política
   - Agente de OfficeScan Direcciones IP del agente de OfficeScan
5. Haga clic en **Guardar**.

Guardar la configuración de la lista de excepciones de políticas

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Políticas**.
2. Haga clic en **Editar la plantilla de excepciones**.
3. Haga clic en una de las siguientes opciones de guardado:
   - **Guardar los cambios de plantillas**: guarda la plantilla de excepción con las excepciones y la configuración de política actuales. Esta opción aplica la plantilla únicamente a las políticas creadas en el futuro, no a las actuales.
   - **Guardar y aplicar las políticas existentes**: guarda la plantilla de excepción con las excepciones y la configuración de política actuales. Esta opción aplica la plantilla a las políticas futuras y actuales.

Perfiles del cortafuegos

Los perfiles del cortafuegos ofrecen gran flexibilidad al permitir seleccionar los atributos que debe tener un agente individual o un grupo de agentes para poder aplicar una

política. Cree funciones para usuario que puedan crear, configurar o eliminar perfiles para dominios específicos.

Los usuarios que utilicen la cuenta de administrador integrada o los que tengan todos los permisos de administración también pueden activar la opción **Sobrescribir lista de excepciones/nivel de seguridad del agente** para sustituir la configuración del perfil del Agente de OfficeScan por la del servidor.

A continuación se indican los perfiles disponibles:

- **Política asociada**: cada perfil utiliza una única política.
- **Atributos del agente**: los Agentes de OfficeScan con uno o varios atributos de entre los que se indican a continuación aplican la política asociada:
    - **Dirección IP**: cualquier Agente de OfficeScan con una dirección IP específica, una dirección IP incluida en un intervalo de direcciones IP o una dirección IP perteneciente a una subred especificada.
    - **Dominio**: cualquier Agente de OfficeScan que pertenezca a un determinado dominio de OfficeScan.
    - **Endpoint**: el Agente de OfficeScan con un nombre de endpoint específico.
    - **Plataforma**: cualquier Agente de OfficeScan que ejecute una plataforma concreta.
    - **Nombre de inicio de sesión**: endpoints del Agente de OfficeScan en los que usuarios especificados hayan iniciado una sesión.
    - **Descripción de NIC**: cualquier endpoint del Agente de OfficeScan con una descripción de NIC coincidente.
    - **Estado de conexión del agente**: determina si el Agente de OfficeScan está conectado o desconectado.

Nota

El Agente de OfficeScan está conectado si se puede conectar al servidor de OfficeScan o a alguno de los servidores de referencia, y está desconectado si no se puede conectar a ningún servidor.

OfficeScan incluye un perfil predeterminado llamado "Perfil de todos los agentes", que utiliza la política "Acceso total". Puede modificar o eliminar este perfil predeterminado. También puede crear nuevos perfiles. Todos los perfiles del cortafuegos predeterminados y creados por el usuario, incluidos la política asociada a cada perfil y el estado del perfil actual, aparecen en la lista de perfiles del cortafuegos en la consola Web. Administre la lista de perfiles e implemente todos los perfiles en los Agentes de OfficeScan. Los Agentes de OfficeScan almacenan todos los perfiles del cortafuegos en el endpoint del agente.

Configurar la lista de perfiles del cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Perfiles**.
2. Para los usuarios que utilizan la cuenta de administrador integrada o los que tienen todos los permisos de administración, puede activar la opción **Sobrescribir el nivel de seguridad del agente/la lista de excepciones** para sustituir la configuración del perfil del Agente de OfficeScan por la del servidor.
3. Para añadir un perfil nuevo, haga clic en **Agregar**. Para editar un perfil existente, seleccione el nombre del perfil.

   Aparecerá una pantalla para realizar la configuración del perfil. Consulte *Agregar y editar un perfil del cortafuegos en la página 13-21* para obtener más información.
4. Para eliminar un perfil existente, active la casilla de verificación que aparece junto a la política y haga clic en **Eliminar**.
5. Para cambiar el orden de los perfiles de la lista, active la casilla de verificación junto al perfil que desea mover y, a continuación, haga clic en **Subir** o **Bajar**.

   OfficeScan aplica los perfiles del cortafuegos a los Agentes de OfficeScan en el orden en el que los perfiles aparecen en la lista. Por ejemplo, si el agente coincide con el primer perfil, OfficeScan aplicará al agente las acciones configuradas para ese perfil. OfficeScan omite los demás perfiles que se han configurado para ese agente.

Consejo

Cuanto más exclusiva es una política, más conveniente es colocarla al principio de la lista. Por ejemplo, mueva una política que haya creado para un único agente al principio de la lista y, a continuación, las políticas aplicables a un intervalo de agentes, a un dominio de red y a todos los agentes.

6. Para administrar los servidores de referencia, haga clic en **Editar la lista de servidores de referencia**. Los servidores de referencia son endpoints que actúan como sustitutos del servidor de OfficeScan cuando aplica perfiles del cortafuegos. Un servidor de referencia puede ser cualquier endpoint de la red (consulte *Servidores de referencia en la página 14-36* para obtener más información). OfficeScan asume lo siguiente cuando activa los servidores de referencia:

   - Que los Agentes de OfficeScan conectados a los servidores de referencia estén en línea, incluso si los agentes no pueden comunicarse con el servidor de OfficeScan.
   - Que los perfiles del cortafuegos aplicados a los Agentes de OfficeScan conectados también se apliquen a los Agentes de OfficeScan conectados a los servidores de referencia.

Nota

Sólo los usuarios que utilicen la cuenta de administrador integrado o aquellos que tienen todos los derechos de administración pueden ver y configurar la lista de servidores de referencia.

7. Para guardar la configuración actual y asignar los perfiles a los Agentes de OfficeScan:

   a. Seleccione si desea **Sobrescribir el nivel de seguridad del agente/la lista de excepciones**. Esta opción sobrescribe la configuración del cortafuegos definida por el usuario.

   b. Haga clic en **Asignar perfil a los agentes**. OfficeScan asignará todos los perfiles de la lista a todos los Agentes de OfficeScan.

8. Para comprobar que ha asignado correctamente los perfiles a los Agentes de OfficeScan:

a. Vaya a **Agentes** > **Administración de agentes**. En el cuadro desplegable de la vista del árbol de agentes, seleccione **Vista del cortafuegos**.

b. Cerciórese de que aparece una marca de verificación verde en la columna **Cortafuegos** del árbol de agentes. Si la política asociada con el perfil activa el Sistema de detección de intrusiones, también aparecerá una marca de verificación verde en la columna **IDS**.

c. Compruebe que el agente haya aplicado la política de cortafuegos correcta. La política aparece en la columna **Política del cortafuegos** en el árbol de agentes.

Agregar y editar un perfil del cortafuegos

Los endpoints requieren diferentes niveles de protección. Los perfiles del cortafuegos le permiten especificar los endpoints del agente a los que se aplicará una política asociada. Por lo general, se necesita un perfil para cada política en uso.

Agregar un perfil del cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Perfiles**.
2. Haga clic en **Agregar**.
3. Haga clic en **Activar este perfil** para que OfficeScan pueda implementar el perfil en los Agentes de OfficeScan.
4. Escriba un nombre para identificar el perfil y, si lo desea, una descripción.
5. Seleccione una política pare este perfil.
6. Especifique los endpoints del agente a los que OfficeScan aplicará la política. Seleccione los endpoints según los siguientes criterios:
   - Dirección IP
   - Dominio: Haga clic en el botón para abrir y seleccionar dominios en el árbol de agentes.

Nota

Sólo pueden seleccionar dominios aquellos usuarios que tengan todos los permisos sobre los dominios.

- Nombre del Endpoint: haga clic en el botón para abrir y seleccione los endpoints del Agente de OfficeScan del árbol de agentes.
- Plataforma
- Nombre de inicio de sesión
- Descripción de NIC: escriba una descripción parcial o completa, sin comodines.

Consejo

Trend Micro recomienda escribir el fabricante de la tarjeta NIC debido a que las descripciones de NIC suelen empezar con el nombre del fabricante. Por ejemplo, si escribe "Intel", todos los NIC fabricados por Intel cumplirán los criterios. Si escribe un modelo concreto de NIC, como por ejemplo "Inter(R) Pro/100", sólo cumplirán los criterios las descripciones de NIC que empiecen por "Intel(R) Pro/100".

- Estado de conexión del agente

7. Seleccione si desea conceder a los usuarios el derecho de cambiar el nivel de seguridad del cortafuegos o de editar una lista configurable de excepciones para permitir determinados tipos de tráfico.

   Para conocer más detalles, consulte *Políticas del cortafuegos en la página 13-9*.

8. Haga clic en **Guardar**.

Modificar un perfil del cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Perfiles**.

2. Haga clic en un perfil.

3. Haga clic en **Activar este perfil** para que OfficeScan pueda implementar este perfil en los Agentes de OfficeScan. Modifique los siguientes parámetros:

   - Nombre y descripción del perfil
   - Política asignada al perfil
   - endpoints del Agente de OfficeScan del perfil, según los siguientes criterios:
     - Dirección IP
     - Dominio: haga clic en el botón para abrir el árbol de agentes y seleccionar dominios en este.
     - Nombre del endpoint: haga clic en el botón para abrir el árbol de agentes y seleccionar los endpoints del agente en este.
     - Plataforma
     - Nombre de inicio de sesión
     - Descripción de NIC: escriba una descripción parcial o completa, sin comodines.

       Consejo

       Trend Micro recomienda escribir el fabricante de la tarjeta NIC debido a que las descripciones de NIC suelen empezar con el nombre del fabricante. Por ejemplo, si escribe "Intel", todos los NIC fabricados por Intel cumplirán los criterios. Si escribe un modelo concreto de NIC, como por ejemplo "Inter(R) Pro/100", sólo cumplirán los criterios las descripciones de NIC que empiecen por "Intel(R) Pro/100".

     - Estado de la conexión del agente

4. Haga clic en **Guardar**.

Derechos del cortafuegos

Permite que los usuarios puedan definir su propia configuración del cortafuegos. Todos los valores configurados por el usuario no pueden sustituirse por los valores de configuración implementados desde el servidor de OfficeScan. Por ejemplo, si el usuario desactiva el sistema de detección de intrusiones (IDS) y activa dicho sistema en el servidor de OfficeScan, el sistema en cuestión permanecerá desactivado en el endpoint del Agente de OfficeScan.

Active la siguiente configuración para permitir que los usuarios configuren el cortafuegos.

TABLA 13-2. Derechos del cortafuegos

DERECHOS	DESCRIPCIÓN
Mostrar la configuración del cortafuegos en la consola del agente de OfficeScan	La opción **Cortafuegos** muestra toda la configuración del cortafuegos en el Agente de OfficeScan.
Permitir que los usuarios activen/desactiven el cortafuegos, el sistema de detección de intrusiones y el mensaje de notificaciones de infracción del cortafuegos	El cortafuegos de OfficeScan protege los agentes y servidores de la red mediante funciones de inspección de estado, exploración y eliminación de virus de red de alto rendimiento. Si concede a los usuarios los derechos necesarios para activar o desactivar el cortafuegos y sus funciones, adviértales que no lo desactiven durante un largo periodo de tiempo a fin de evitar que el endpoint quede expuesto a intrusiones o ataques de hackers. Si no concede a los usuarios dichos derechos, la configuración del cortafuegos que defina desde la consola Web del servidor de OfficeScan aparecerá en la lista de tarjetas de red de la consola del Agente de OfficeScan.

Derechos	Descripción
Permitir que los agentes envíen los registros del cortafuegos al servidor de OfficeScan	Seleccione esta opción para analizar el tráfico que bloquea y permite OfficeScan Firewall. Para obtener información detallada acerca de los registros del cortafuegos, consulte *Registros del cortafuegos en la página 13-30*. Si selecciona esta opción, configure el programa de envío de registros en **Agentes** > **Configuración global para los agentes** en la pestaña **Configuración de seguridad**. Vaya a la sección **Configuración del cortafuegos**. El programa solo se aplica a los agentes con derechos de envío de registros del cortafuegos. Para obtener instrucciones, consulte *Configuración general del cortafuegos en la página 13-26*.

Conceder derechos del cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Derechos del cortafuegos**.
5. Seleccione las siguientes opciones:
   - *Mostrar la pestaña del cortafuegos en la consola del agente de OfficeScan en la página 13-24*
   - *Permitir que los usuarios activen/desactiven el cortafuegos, el sistema de detección de intrusiones y el mensaje de notificaciones de infracción del cortafuegos en la página 13-24*
   - *Permitir que los agentes de OfficeScan envíen registros del cortafuegos al servidor de OfficeScan en la página 13-25*

6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración general del cortafuegos

La configuración general del cortafuegos se aplica a los Agentes de OfficeScan de varias formas.

- Se puede aplicar una configuración del cortafuegos específica a todos los agentes que administre el servidor.
- Se puede aplicar una configuración solo a los Agentes de OfficeScan que cuenten con determinados derechos del cortafuegos. Por ejemplo, el programa de envío de registros del cortafuegos solo se aplica a los Agentes de OfficeScan con derecho a enviar registros al servidor.

Active las siguientes opciones generales si es necesario:

- **Enviar registros del cortafuegos al servidor**

  Puede conceder el derecho a enviar registros del cortafuegos al servidor de OfficeScan a determinados Agentes de OfficeScan. Configure el programa de envío de registros en esta sección. Solo los agentes que tengan configurado el derecho a enviar registros del cortafuegos podrán usar el programa.

  Consulte *Derechos del cortafuegos en la página 13-24* para obtener información sobre los derechos del cortafuegos disponibles para los agentes seleccionados.

- **Actualizar el controlador del cortafuegos de OfficeScan sólo después de reiniciar el sistema**

  Active el Agente de OfficeScan para que actualice el driver del Cortafuegos común solo una vez reiniciado el endpoint del Agente de OfficeScan. Active esta opción para impedir posibles interrupciones en el endpoint del agente (como la desconexión temporal de la red) cuando se actualice el driver del Cortafuegos común durante la actualización del agente.

- **Enviar información de registro del cortafuegos al servidor de OfficeScan cada hora para determinar la posibilidad de una epidemia del cortafuegos**

  Si activa esta opción, los Agentes de OfficeScan enviarán recuentos de registro del cortafuegos al servidor de OfficeScan cada hora. Para obtener información detallada acerca de los registros del cortafuegos, consulte *Registros del cortafuegos en la página 13-30*.

  OfficeScan utiliza recuentos de registros y criterios de epidemias de infracciones del cortafuegos para determinar la posibilidad de una epidemia de infracciones del cortafuegos. OfficeScan envía notificaciones por correo electrónico a los administradores de OfficeScan en caso de que se produzca una epidemia.

- Vaya a la sección **Configuración del servicio de software seguro certificado** y active el servicio de software seguro certificado cuando se le solicite.

  El servicio de software seguro certificado realiza consultas a los centros de datos de Trend Micro para comprobar la seguridad de un programa detectado por el bloqueador de comportamientos malintencionados, la supervisión de eventos, el cortafuegos o las exploraciones antivirus. Active el Servicio de software seguro certificado para reducir la probabilidad de detecciones de falsos positivos.

Nota

Asegúrese de que los Agentes de OfficeScan tengan la configuración del proxy correcta (para obtener más información, consulte *Configuración del proxy del agente de OfficeScan en la página 15-54*) antes de activar el servicio de software seguro certificado. Una configuración incorrecta del proxy, junto con una conexión intermitente a Internet, puede acarrear atrasos o fallos en la respuesta de los centros de datos de Trend Micro, lo que puede hacer que los programas que se supervisen no respondan.

Además, los Agentes de OfficeScan que solo utilizan IPv6 no podrán realizar consultas directas a los centros de datos de Trend Micro. Con el fin de permitir que los Agentes de OfficeScan se conecten a los centros de datos de Trend Micro, se necesita un servidor proxy de doble pila que pueda convertir direcciones IP, como puede ser DeleGate.

Definir la configuración general del cortafuegos

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. En la pestaña **Configuración de seguridad**, vaya a la sección **Configuración del cortafuegos** y configure las siguientes opciones:
   - *Enviar registros del cortafuegos al servidor en la página 13-26*
   - *Actualizar el controlador del cortafuegos de OfficeScan sólo después de reiniciar el sistema en la página 13-27*
   - *Enviar información de registro del cortafuegos al servidor de OfficeScan cada hora para determinar la posibilidad de una epidemia del cortafuegos en la página 13-27*
3. En la pestaña **Sistema**, vaya a la sección **Configuración del servicio de software seguro certificado** y configure las siguientes opciones:
   - *Activar el servicio de software seguro certificado para la supervisión de comportamiento, el cortafuegos y las exploraciones antivirus en la página 13-27*
4. Haga clic en **Guardar**.

Notificaciones de infracciones del cortafuegos para los usuarios del agente de OfficeScan

OfficeScan puede mostrar un mensaje de notificación en los endpoints inmediatamente después de que el cortafuegos de OfficeScan bloquea el tráfico saliente que ha infringido las políticas del cortafuegos. Conceda a los usuarios el derecho a activar/desactivar el mensaje de notificación:

Nota

También puede activar la notificación al configurar una política específica del cortafuegos. Para configurar una política del cortafuegos, consulte *Agregar una política de cortafuegos en la página 13-11*.

Conceder a los usuarios el derecho para activar/desactivar el mensaje de notificación

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Derechos del cortafuegos**.
5. Seleccione **Permitir que los usuarios activen/desactiven el cortafuegos, el sistema de detección de intrusiones y el mensaje de notificaciones de infracción del cortafuegos**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los

futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Modificar el contenido del mensaje de notificación del cortafuegos

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Agentes**.
2. Seleccione **Infracciones del cortafuegos** en el menú desplegable **Tipo**.
3. Modifique los mensajes predeterminados en el cuadro de texto habilitado para ello.
4. Haga clic en **Guardar**.

Registros del cortafuegos

Los Agentes de OfficeScan con los derechos necesarios envían los registros del cortafuegos disponibles en el servidor. Conceda este derecho a determinados agentes para que supervisen y analicen el tráfico en los endpoints que el cortafuegos de OfficeScan está bloqueando.

Para obtener más información sobre los derechos del cortafuegos, consulte *Derechos del cortafuegos en la página 13-24*.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Ver registros del cortafuegos

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Registros** > **Registros del cortafuegos** o **Ver registros** > **Registros del cortafuegos**.
4. Para asegurarse de que tiene a su disposición los registros más actualizados, haga clic en **Notificar a los agentes**. Deje que transcurra algún tiempo para que los agentes envíen registros del cortafuegos antes de continuar con el siguiente paso.
5. Especifique los criterios de los registros y, después, haga clic en **Mostrar registros**.
6. Visualice los registros. Los registros contienen la siguiente información:
   - Fecha y hora en que se detectó la violación del cortafuegos
   - Endpoint en el que se ha producido la infracción del cortafuegos
   - Dominio del endpoint en el que se ha producido la infracción del cortafuegos
   - Dirección IP del host remoto
   - Dirección IP del host local
   - Protocolo
   - Número de puerto
   - Dirección: si el tráfico entrante (recibido) o saliente (enviado) ha violado la política del cortafuegos.
   - Proceso: el programa ejecutable o servicio que se ejecuta en el endpoint que ha provocado la violación del cortafuegos.
   - Descripción: especifica el riesgo de seguridad real (p. ej. virus de red o ataque IDS) o la violación de la política del cortafuegos.

7. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Epidemias de infracciones del cortafuegos

Defina una epidemia de infracciones del cortafuegos mediante el número de infracciones del cortafuegos y el periodo de detección.

OfficeScan incluye un mensaje de notificación predeterminado que le informa a usted y a los demás administradores de OfficeScan en caso de que se produzca una epidemia. Puede modificar el mensaje de notificación según sus necesidades.

Nota

OfficeScan puede enviar notificaciones de epidemias de infracciones mediante correo electrónico. Defina la configuración del correo electrónico para permitir que OfficeScan envíe mensajes de correo electrónico correctamente. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

Configurar los criterios de epidemias de infracciones del cortafuegos y las notificaciones

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Epidemia**.
2. En la pestaña **Criterios**:
   a. Vaya a la sección **Infracciones del cortafuegos**.
   b. Seleccione **Supervisar las infracciones del cortafuegos en los agentes de OfficeScan**.
   c. Especifique el número de registros de IDS, del cortafuegos y de virus de red.

d. Especifique el periodo de detección.

Consejo

Trend Micro recomienda aceptar los valores predeterminados de esta pantalla.

OfficeScan envía un mensaje de notificación cuando se supera el número de registros especificado. Si, por ejemplo, especifica 100 registros de IDS, 100 del cortafuegos, 100 de registros de virus de red y un periodo de 3 horas, OfficeScan envía la notificación cuando el servidor recibe 301 registros en un periodo de 3 horas.

3. En la pestaña **Correo electrónico**:

   a. Vaya a la sección **Epidemias de infracciones del cortafuegos**.

   b. Seleccione **Activar la notificación por correo electrónico**.

   c. Especifique los destinatarios del correo electrónico.

   d. Acepte o modifique el asunto y el mensaje predeterminados del correo electrónico. Puede utilizar variables de símbolo para representar los datos en los campos **Asunto** y **Mensaje**.

TABLA 13-3. Variables de símbolo para notificaciones de epidemias de infracciones del cortafuegos

VARIABLE	DESCRIPCIÓN
%A	Tipo de registro excedido
%C	Número de registros de violaciones del cortafuegos
%T	Periodo de tiempo durante el cual se acumulan registros de infracciones del cortafuegos

4. Haga clic en **Guardar**.

Comprobar OfficeScan Firewall

Para garantizar que el cortafuegos de OfficeScan funciona correctamente, realice una prueba en un Agente de OfficeScan individual o en un grupo de Agentes de OfficeScan.

¡ADVERTENCIA!

Pruebe la configuración del programa del Agente de OfficeScan solo en entornos controlados. No realice pruebas en endpoints conectados a la red o a Internet. Si lo hace, puede exponer a los endpoints del Agente de OfficeScan a virus, ataques de hackers y otros riesgos.

Procedimiento

1. Cree una política de prueba y guárdela. Establezca los parámetros de configuración para bloquear los tipos de tráfico que desee probar. Por ejemplo, para evitar que el Agente de OfficeScan acceda a Internet, realice lo siguiente:
   a. Establezca el nivel de seguridad en **Bajo** (permitir todo el tráfico entrante y saliente).
   b. Seleccione **Activar el cortafuegos y Notificar a los usuarios cuando se produce una infracción en el cortafuegos**.
   c. Cree una excepción que bloquee el tráfico HTTP (o HTTPS).
2. Cree y guarde un perfil de prueba y seleccione los agentes con los que desea probar las funciones del cortafuegos. Asocie la política de prueba con el perfil de prueba.
3. Haga clic en **Asignar perfil a los agentes**.
4. Compruebe la implementación.
   a. Haga clic en **Agentes** > **Administración de agentes**.
   b. Seleccione el dominio al que pertenece el agente.
   c. Seleccione **Vista del cortafuegos** en la vista del árbol de agentes.
   d. Compruebe si hay una marca de verificación de color verde en la columna **Cortafuegos** del árbol de agentes. Si ha activado el sistema de detección de

intrusiones para ese agente, asegúrese de que también aparezca una marca de verificación verde en la columna **IDS**.

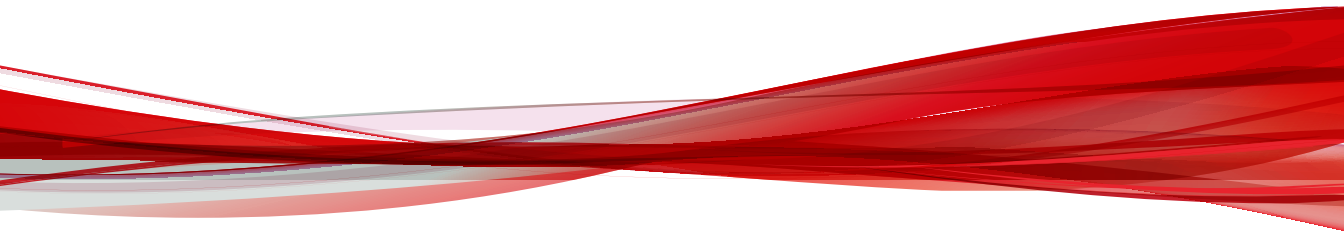
e. Compruebe que el agente haya aplicado la política de cortafuegos correcta. La política aparece en la columna **Política de cortafuegos** en el árbol de agentes.

5. Compruebe el cortafuegos en el endpoint del agente. Para hacerlo, intente enviar o recibir el tipo de tráfico que ha configurado en la política.

6. Si desea probar una política configurada para evitar que el agente acceda a Internet, abra un explorador Web en el endpoint del agente. Si ha configurado OfficeScan para que muestre un mensaje de notificación cuando se produzcan infracciones del cortafuegos, el mensaje aparecerá en el endpoint del agente al ocurrir una infracción de tráfico saliente.

Parte III

Administración del servidor y los agentes de OfficeScan



Capítulo 14

Administrar el servidor de OfficeScan

En este capítulo se describen la administración y la configuración del servidor de OfficeScan.

Los temas que se incluyen son:

- *Role-based Administration en la página 14-3*
- *Trend Micro Control Manager en la página 14-26*
- *Configuración de la lista de objetos sospechosos en la página 14-34*
- *Servidores de referencia en la página 14-36*
- *Configuración de las notificaciones del administrador en la página 14-39*
- *Registros de sucesos del sistema en la página 14-41*
- *Administración de registros en la página 14-43*
- *Licencias en la página 14-47*
- *Copia de seguridad de la base de datos de OfficeScan en la página 14-50*
- *Herramienta de migración de SQL Server en la página 14-52*
- *Configuración de la conexión del servidor Web y el agente de OfficeScan en la página 14-56*
- *Comunicación entre servidor y agente en la página 14-57*

- *Contraseña de la consola Web en la página 14-64*
- *Configuración de la Consola Web en la página 14-64*
- *Administrador de cuarentena en la página 14-65*
- *Server Tuner en la página 14-66*
- *Smart Feedback en la página 14-69*

Role-based Administration

Utilice Role-based Administration para conceder y controlar los derechos de acceso a la consola OfficeScan Web. Si hay varios administradores de OfficeScan en su organización, puede utilizar esta característica para asignarles derechos específicos de la consola Web y concederles solo las herramientas y permisos necesarios para realizar tareas específicas. También puede controlar el acceso al árbol de agentes mediante la asignación de uno o varios dominios para administrar. Además, puede conceder a los que no sean administradores acceso de "solo visualización" a la consola Web.

A cada usuario (administrador o no administrador) se le asigna una función concreta. La función define el nivel de acceso a la consola Web. Los usuarios inician sesión en la consola Web mediante una cuenta de usuario personalizada o una cuenta de Active Directory.

La role-based administration está formada por las siguientes tareas:

1. Defina las funciones de usuario. Para obtener información detallada, consulte *Funciones de usuario en la página 14-3*.

2. Configure las cuentas de usuario y asigne una función concreta a cada una de ellas. Para obtener información detallada, consulte *Cuentas de usuario en la página 14-14*.

Vea las actividades de la consola Web de todos los usuarios en los registros de sucesos del sistema. Las siguientes actividades están registradas:

- Inicio de sesión en la consola
- Modificación de la contraseña
- Cierre de sesión de la consola
- Tiempo de espera de la sesión excedido (el usuario se desconecta automáticamente)

Funciones de usuario

Una función de usuario hace accesibles para el usuario las opciones del menú de la consola Web. Se asigna un permiso a la función para cada opción del menú.

Asigne permisos para las siguientes funciones:

- *Permisos de las opciones del menú en la página 14-4*
- *Tipos de opción de menú en la página 14-4*
- *Opciones de menú para servidores y agentes en la página 14-5*
- *Opciones de menú de los dominios gestionados en la página 14-8*

Permisos de las opciones del menú

Los permisos determinan el nivel de acceso a cada opción del menú. El permiso de una opción de menú puede ser:

- **Configurar**: permite el acceso total a una opción de menú. Los usuarios pueden configurar todos los parámetros, realizar todas las tareas y ver los datos de la opción de menú.
- **Mostrar**: solo permite a los usuarios ver las configuraciones, las tareas y los datos de la opción de menú.
- **Sin acceso**: oculta la opción de menú e impide su visualización.

Tipos de opción de menú

Existen dos tipos configurables de opciones de menú para las funciones de usuario de OfficeScan.

TABLA 14-1. Tipos de opción de menú

TIPO	ALCANCE
Elementos de menú para servidores/ agentes	• Configuración, tareas y datos del servidor • Configuración general, tareas y datos del agente Para consultar una lista completa de las opciones de menú disponibles, consulte *Opciones de menú para servidores y agentes en la página 14-5*.

TIPO	ALCANCE
Opciones de menú de los dominios gestionados	La configuración, las tareas y los datos del agente granular se encuentran disponibles fuera del árbol de agentes Para consultar una lista completa de las opciones de menú disponibles, consulte *Opciones de menú de los dominios gestionados en la página 14-8*.

Opciones de menú para servidores y agentes

En las siguientes tablas se muestran las opciones de menú disponibles para los servidores y agentes.

Nota

Las opciones de menú solo se muestran tras la activación de su programa de complemento correspondiente. Por ejemplo, si el módulo de prevención de pérdida de datos no está activado, ninguna de las opciones de menú de la prevención de pérdida de datos aparecerá en la lista. Cualquier programa de complemento adicional aparece en la opción de menú Complementos.

Solo los usuarios con la función «Administrador (integrado)» pueden acceder a la opción de menú Complementos.

TABLA 14-2. Opciones del menú Agentes

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ
Agentes	• Administración de agentes • Agrupación de agentes • Configuración global para los agentes • Ubicación del Endpoint • Prevención de pérdida de datos • Comprobación de la conexión • Prevención de epidemias

TABLA 14-3. Opciones del menú Registros

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ

Registros	• Agentes
	  • Riesgos de seguridad
	  • Actualización de componentes del agente
	• Actualizaciones del servidor
	• Sucesos del sistema
	• Mantenimiento de los registros

TABLA 14-4. Opciones del menú Actualizaciones

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Actualizaciones	Servidor	• Actualización programada • Actualización manual • Origen de actualización
	Agentes	• Actualización automática • Origen de actualización
	Recuperar	N/D

TABLA 14-5. Opciones del menú Administración

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Administración	Administración de cuentas	• Cuentas de usuario • Funciones de usuario

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
		Nota Solo los usuarios que utilicen cuentas de administradores integrados pueden acceder a las Cuentas de usuario y a las Funciones de usuario.
	Smart Protection	• Fuentes de Protección Inteligente • Servidor integrado • Smart Feedback
	Active Directory	• Integración con Active Directory • Sincronización programada
	Notificaciones	• Configuración general • Epidemia • Agente
	Configuración	• Proxy • Conexión del agente • Agentes inactivos • Administrador de cuarentena • Licencia del producto • Control Manager • Consola Web • Copia de seguridad de la base de datos

Opción de menú del nivel superior	Opción de menú	Opción de submenú
		• Lista de objetos sospechosos • Edge Relay

Opciones de menú de los dominios gestionados

En la siguiente tabla se muestran las opciones de menú disponibles para los dominios gestionados:

Tabla 14-6. Opción del menú Panel

Opciones de menú principales	Opción de menú
Panel **Nota** Cualquier usuario puede acceder a esta página, independientemente del permiso que tenga.	N/D

Tabla 14-7. Opciones del menú Valoración

Opción de menú del nivel superior	Opción de menú	Opción de submenú
Valoración	Conformidad con las normas de seguridad	• Informe manual • Informe programado
	Endpoints no administrados	N/D

TABLA 14-8. Opciones del menú Agentes

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Agentes	Cortafuegos	• Políticas • Perfiles
	Instalación de agentes	• Basada en explorador • Remoto

TABLA 14-9. Opciones del menú Registros

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Registros	Agentes	• Comprobación de la conexión • Central Quarantine Restore • Restauración de spyware/ grayware

TABLA 14-10. Opciones del menú Actualizaciones

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Actualizaciones	Resumen	N/D
	Agentes	Actualización manual

TABLA 14-11. Opciones del menú Administración

OPCIÓN DE MENÚ DEL NIVEL SUPERIOR	OPCIÓN DE MENÚ	OPCIÓN DE SUBMENÚ
Administración	Notificaciones	Administrador

Funciones de usuario integradas

OfficeScan incorpora un conjunto de funciones de usuario integradas que no se pueden modificar ni eliminar. Las funciones integradas son:

TABLA 14-12. Funciones de usuario integradas

NOMBRE DE LA FUNCIÓN	DESCRIPCIÓN
Administrador	Delegue esta función en otros administradores o usuarios de OfficeScan que posean suficientes conocimientos de OfficeScan. Los usuarios con esta función tienen el permiso "Configurar" en todas las opciones de menú. **Nota** Solo los usuarios con la función «Administrador (integrado)» pueden acceder a la opción de menú Complementos.

Nombre de la función	Descripción

Usuario invitado	Delegue esta función en usuarios que deseen ver la consola Web como referencia.
	• Los usuarios con esta función no tienen acceso a las siguientes opciones de menú:
	  • Complementos
	  • **Administración** > **Administración de cuentas** > **Funciones de usuario**
	  • **Administración** > **Administración de cuentas** > **Cuentas de usuario**
	• Los usuarios tiene el permiso "Ver" para el resto de elementos de menú.

Usuario avanzado de Trend (solo actualizar función)	Esta función solo está disponible si se actualiza desde OfficeScan 10. Esta función reúne los permisos de la función "Usuario avanzado" de OfficeScan 10. Los usuarios con esta función tienen el permiso "Configurar" en todos los dominios del árbol de agentes, pero no podrán acceder a las nuevas funciones de esta versión.

Funciones personalizadas

Tiene la posibilidad de crear funciones personalizadas si ninguna de las que incorpora OfficeScan satisface sus necesidades.

Únicamente los usuarios que tienen la función de administrador integrada y aquellos que utilizan la cuenta raíz que se ha creado durante la instalación de OfficeScan pueden crear funciones de usuario personalizadas y asignarlas a las cuentas de usuario.

Añadir una función personalizada

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Funciones de usuario**.
2. Haga clic en **Agregar**. Si la función que desea crear tiene valores de configuración similares a los de una función existente, seleccione esta última y haga clic en **Copiar**.

   Aparecerá una nueva pantalla.
3. Especifique un nombre para la función y, de forma opcional, una descripción.
4. Haga clic en **Opciones de menú para servidores/agentes** y especifique el permiso para cada opción de menú disponible. Para consultar una lista completa de las opciones de menú disponibles, consulte *Opciones de menú para servidores y agentes en la página 14-5*.
5. Haga clic en **Opciones de menú para los dominios gestionados** y especifique el permiso para cada opción de menú disponible. Para consultar una lista completa de las opciones de menú disponibles, consulte *Opciones de menú de los dominios gestionados en la página 14-8*.
6. Haga clic en **Guardar**.

   La nueva función se muestra en la lista de funciones del usuario.

Modificar una función personalizada

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Funciones de usuario**.
2. Haga clic en el nombre de la función.

   Aparecerá una nueva pantalla.
3. Modifique alguno de los siguientes elementos:

- Descripción
- Permisos de función
  - **Elementos de menú para servidores/agentes**
  - **Opciones de menú de los dominios gestionados**

4. Haga clic en **Guardar**.

Eliminar una función personalizada

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Funciones de usuario**.
2. Active la casilla de verificación que aparece junto a la función.
3. Haga clic en **Eliminar**.

Nota

No se puede eliminar una función si se encuentra asignada a al menos una cuenta.

Importar o exportar funciones personalizadas

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Funciones de usuario**.
2. Para exportar las funciones personalizadas a un archivo `.dat`:
   a. Seleccione las funciones y haga clic en **Exportar**.
   b. Guarde el archivo `.dat`. Si está administrando otro servidor de OfficeScan, utilice el archivo `.dat` para importar las funciones personalizadas a dicho servidor.

Nota

La exportación de funciones solo es posible entre servidores con la misma versión.

3. Para exportar las funciones personalizadas a un archivo `.csv`:

   a. Seleccione las funciones y haga clic en **Exportar Parámetros relacionados con Roles**.

   b. Guarde el archivo `.csv`. Utilice este archivo para comprobar la información y los permisos de las funciones seleccionadas.

4. Si ha guardado las funciones personalizadas desde un servidor de OfficeScan diferente y desea importarlas al servidor de OfficeScan actual, haga clic en **Importar** y localice el archivo `.dat` que contiene las funciones personalizadas.

   - Las funciones de la pantalla Funciones de usuario se sobrescriben si se importa una función con el mismo nombre.
   - La importación de funciones solo es posible entre servidores con la misma versión.
   - Una función importada de otro servidor de OfficeScan:
     - Conserva los permisos de las opciones de menú para servidores y agentes, y para los dominios gestionados.
     - Aplica los permisos predeterminados a las opciones disponibles de menú de administración de agentes. En el otro servidor, registre los permisos de la función para las opciones del menú de administración de agentes y, a continuación, vuelva a aplicarlos en la función importada.

Cuentas de usuario

Configure las cuentas de usuario y asigne una función concreta a cada usuario. La función de usuario determina los elementos de menú de la consola Web que un usuario puede ver o configurar.

Durante la instalación del servidor de OfficeScan, el programa de instalación crea automáticamente un cuenta integrada llamada "raíz". Los usuarios que inician sesión con

la cuenta raíz pueden acceder a todos los elementos de menú. No es posible eliminar la cuenta raíz, pero sí modificar sus detalles, como la contraseña y nombre completo o la descripción de la cuenta. Si olvida la contraseña de la cuenta raíz, póngase en contacto con su proveedor de servicios para que le ayude a restablecerla.

Agregue cuentas personalizadas o cuentas de Active Directory. Todas las cuentas de usuario se muestran en la lista de cuentas de usuario de la consola Web.

Asigne a las cuentas de usuario el derecho para ver o configurar la configuración granular de los agentes, las tareas y los datos disponibles en el árbol de agentes. Para consultar una lista completa de las opciones de menú del árbol de agentes disponibles, consulte *Elementos del menú de administración de agentes en la página 14-15*.

Nota

Después de actualizar el servidor de OfficeScan, debe editar las cuentas personalizadas y activar manualmente todas las funciones nuevas en la pantalla **Paso 3 Defina el menú del árbol de agentes** de las cuentas personalizadas que se añadieron previamente. Para obtener información detallada acerca de los permisos, consulte *Definición de permisos para dominios en la página 14-21*.

Las cuentas de usuario de OfficeScan se pueden utilizar para llevar a cabo un "inicio de sesión único". El inicio de sesión único permite a los usuarios acceder a la consola Web OfficeScan desde la consola de Trend Micro Control Manager. Consulte el procedimiento que se detalla a continuación para obtener más información.

Elementos del menú de administración de agentes

En la siguiente tabla se muestran las opciones disponibles del menú de administración de agentes.

Nota

Las opciones de menú solo se muestran tras la activación de su programa de complemento correspondiente. Por ejemplo, si el módulo de prevención de pérdida de datos no está activado, ninguna de las opciones de menú de la prevención de pérdida de datos aparecerá en la lista.

TABLA 14-13. Elementos del menú de administración de agentes

OPCIONES DE MENÚ PRINCIPALES	SUBMENÚS
Estado	N/D
Tareas	• Explorar ahora • Desinstalación del agente • Central Quarantine Restore • Restauración de spyware y grayware

OPCIONES DE MENÚ PRINCIPALES	SUBMENÚS

Configuración	• Configuración de la exploración
	  • Métodos de exploración
	  • Configuración de la exploración manual
	  • Configuración de la exploración en tiempo real
	  • Configuración de la exploración programada
	  • Configuración de Explorar ahora
	• Configuración de la Reputación Web
	• Configuración de conexión sospechosa
	• Configuración de la supervisión de comportamiento
	• Configuración de Control de dispositivos
	• Configuración de DLP
	• Envío de muestras
	• Configuración del agente de actualización
	• Derechos y otras configuraciones
	• Configuración de servicios adicionales
	• Lista de spyware/grayware permitido
	• Lista de programas de confianza
	• Configuración del aprendizaje automático predictivo
	• Exportar configuración
	• Importar configuración

Opciones de menú principales	Submenús
Registros	• Registros de virus/malware • Registros de spyware/grayware • Registros del cortafuegos • Registros de reputación Web • Registros de conexión sospechosa • Registros de archivos sospechosos • Registros de rellamadas de C&C • Registros de supervisión del comportamiento • Registros del aprendizaje automático predictivo • Registros de control de dispositivos • Registros de prevención de pérdida de datos • Registros de operaciones de exploración • Eliminar registros
Administrar el árbol de agentes	• Agregar un dominio • Cambiar nombre del dominio • Mover agente • Eliminar dominio/agente
Exportar	N/D

Añadir una cuenta personalizada

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Cuentas de usuario**.
2. Haga clic en **Agregar**.

Aparecerá la ventana **Paso 1: información del usuario**.

3. Seleccione **Activar esta cuenta**.

4. En la lista desplegable **Seleccionar función**, seleccione una función previamente configurada.

   Para obtener más información sobre cómo crear funciones de usuario, consulte *Funciones personalizadas en la página 14-11*.

5. Escriba el nombre de usuario, la descripción y la contraseña; a continuación, confirme la contraseña.

   Importante

   No es posible utilizar el nombre de usuario como contraseña de la cuenta. Proporcione una contraseña que no sea el nombre de usuario.

6. Escriba una dirección de correo electrónico para la cuenta.

   Nota

   OfficeScan envía notificaciones a esta dirección de correo electrónico. Las notificaciones informan al destinatario acerca de las detecciones de riesgos de seguridad y las transmisiones de activos digitales. Para obtener información detallada acerca de las notificaciones, consulte *Notificaciones de riesgos de seguridad para los administradores en la página 7-87*.

7. Haga clic en **Siguiente**.

   Aparecerá la ventana **Paso 2: control de dominio del agente**.

8. Defina el alcance del árbol de agentes seleccionando el dominio raíz o uno o varios dominios en el árbol de agentes.

   Hasta ahora solo se han definido los dominios. El nivel de acceso para los dominios seleccionados quedará determinado en el paso 10.

9. Haga clic en **Siguiente**.

   Aparecerá la ventana **Paso 3: definir el menú del árbol de agentes**.

10. Haga clic en los controles de **Opciones de menú disponibles** y especifique el permiso para cada opción de menú disponible. Para consultar una lista completa de las opciones de menú disponibles, consulte *Elementos del menú de administración de agentes en la página 14-15*.

    El alcance del árbol de agentes configurado en el paso 8 determina el nivel de permiso en las opciones de menú y define los destinos del permiso. El alcance del árbol de agentes puede ser el dominio raíz (todos los agentes) o dominios específicos del árbol de agentes.

    TABLA 14-14. Opciones del menú Administración de agentes y alcance del árbol de agentes

CRITERIOS	ALCANCE DEL ÁRBOL DE AGENTES	
	DOMINIO RAÍZ	DOMINIOS ESPECÍFICOS
Permiso de las opciones del menú	Configurar, Mostrar o Sin acceso	Configurar, Mostrar o Sin acceso
Destino	Dominio raíz (todos los agentes) o dominios específicos Por ejemplo, puede conceder el permiso "Configurar" a una función en la opción de menú "Tareas" del árbol de agentes. Si el destino es el dominio raíz, el usuario puede iniciar las tareas en todos los agentes. Si los destinos son los dominios A y B, las tareas solo se pueden iniciar en los agentes de los dominios A y B.	Solo los dominios seleccionados Por ejemplo, puede conceder el permiso "Configurar" a una función en la opción de menú "Configuración" del árbol de agentes. Esto implica que el usuario puede implementar la configuración, pero solo para los agentes de los dominios seleccionados.
	El árbol de agentes solo se mostrará si el permiso de la opción de menú Administración de agentes en "Opciones de menú para servidores y agentes" es "Ver".	

- Si selecciona la casilla de verificación que aparece debajo de **Configurar**, se seleccionará automáticamente la casilla **Ver**.

- Si no selecciona ninguna casilla de verificación, el permiso será "Sin acceso".
- Si configura permisos para un dominio específico, puede copiar los permisos a otros dominios haciendo clic en **Copiar la configuración del dominio seleccionado en otros dominios**.

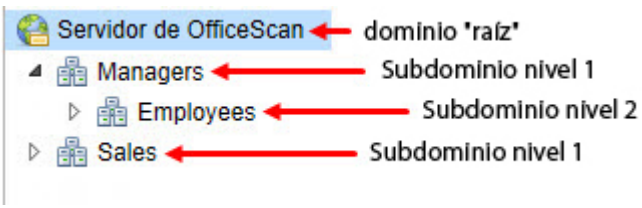
11. Por último, haga clic en **Finalizar**.

12. Envíe los detalles de la cuenta al usuario.

Definición de permisos para dominios

Al definir permisos para dominios, OfficeScan aplica automáticamente los permisos de un dominio principal a todos los subdominios que administra. Un subdominio no puede tener menos permisos que su dominio principal. Por ejemplo, si el administrador del sistema tiene permiso para ver y configurar todos los agentes que administra OfficeScan (el dominio «Servidor de OfficeScan»), los permisos de los subdominios deben permitirle acceder a estas funciones de configuración. Si se quitara un permiso en un subdominio, el administrador del sistema dejaría de tener permisos de configuración completos para todos los agentes.

En el siguiente procedimiento, el árbol de dominios es de la forma siguiente:



Por ejemplo, para conceder a la cuenta de usuario «Luis» permisos para ver y configurar elementos de menú específicos del subdominio «Empleados», y conceder únicamente permisos para ver los registros del dominio principal «Jefes», realice el procedimiento siguiente.

TABLA 14-15. Permisos para la cuenta de usuario «Luis»

DOMINIO	PERMISOS DESEADOS
Servidor de OfficeScan	Sin permisos especiales
Jefes	Ver **Registros**
Empleados	Ver y configurar **Tareas** Ver y configurar **Registros** Ver **Configuración**
Ventas	Sin permisos especiales

Procedimiento

1. Vaya a la pantalla **Cuentas de usuario - Paso 3: definir el menú del árbol de agentes**.
2. Haga clic en el dominio «Servidor de OfficeScan».
3. Quite la marca de todas las casillas de verificación **Ver** y **Configurar**.

   Nota

   El dominio «Servidor de OfficeScan» solo es configurable si ha seleccionado todos sus subdominios en la pantalla **Cuentas de usuario - Paso 2: control de dominio del agente**.

4. Haga clic en el dominio «Ventas».
5. Quite la marca de todas las casillas de verificación **Ver** y **Configurar**.

   Nota

   El dominio «Ventas» solo se muestra si se ha seleccionado en la pantalla **Cuentas de usuario - Paso 2: control de dominio del agente**.

6. Haga clic en el dominio «Jefes».
7. Seleccione «Ver registros» y quite la marca de todas las demás casillas de verificación **Ver** y **Configurar**.

8. Haga clic en el dominio «Empleados».
9. Seleccione los siguientes elementos de menú para Luis:
   - **Tareas**: ver y configurar.
   - **Registros**: ver y configurar.
   - **Configuración**: ver.

   Ahora Luis puede ver y configurar los elementos de menú seleccionados para el dominio «Empleados» y solo puede ver **Registros** para el dominio «Jefes».

Si Luis tiene permiso para ver y configurar el dominio «Jefes», OfficeScan concede automáticamente los mismos permisos al subdominio «Empleados». Esto se debe a que el dominio «Jefes» administra todos sus subdominios.

Modificar una cuenta personalizada

Nota

Después de actualizar el servidor de OfficeScan, debe editar las cuentas personalizadas y activar manualmente todas las funciones nuevas en la pantalla **Paso 3 Defina el menú del árbol de agentes** de las cuentas personalizadas que se añadieron previamente. Para obtener información detallada acerca de los permisos, consulte *Definición de permisos para dominios en la página 14-21*.

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Cuentas de usuario**.
2. Haga clic en la cuenta de usuario.
3. Active o desactive la cuenta mediante la casilla de verificación que se muestra.
4. Modifique los siguientes parámetros:
   - Función
   - Descripción

- Contraseña

  Nota

  No se puede volver a escribir la contraseña que se configuró anteriormente mientras se edita una cuenta. No modifique el campo **Contraseña** para seguir usando la contraseña configurada anteriormente.

- Dirección de correo electrónico

5. Haga clic en **Siguiente**.
6. Defina el alcance del árbol de agentes.
7. Haga clic en **Siguiente**.
8. Haga clic en los controles de **Opciones de menú disponibles** y especifique el permiso para cada opción de menú disponible.

   Para consultar una lista completa de las opciones de menú disponibles, consulte *Elementos del menú de administración de agentes en la página 14-15*.
9. Por último, haga clic en **Finalizar**.
10. Envíe los detalles de la nueva cuenta al usuario.

Añadir cuentas o grupos de Active Directory

Procedimiento

1. Vaya a **Administración** > **Administración de cuentas** > **Cuentas de usuario**.
2. Haga clic en **Agregar**.

   Aparecerá la ventana **Paso 1: información del usuario**.
3. Seleccione **Activar esta cuenta**.
4. En la lista desplegable **Seleccionar función**, seleccione una función previamente configurada.

Para obtener más información sobre cómo crear funciones de usuario, consulte *Funciones personalizadas en la página 14-11*.

5. Seleccione **Usuario o grupo de Active Directory**.

Importante

El servidor de OfficeScan debe unirse al dominio de Active Directory para administrar las cuentas de usuario.

6. Busque una cuenta (nombre de usuario o grupo) especificando el nombre de usuario y el dominio al que pertenece la cuenta.

Nota

Utilice el carácter (*) para buscar varias cuentas. Si no especifica el carácter comodín, incluya el nombre de cuenta completo. OfficeScan no ofrecerá ningún resultado para nombres incompletos de cuentas o si el grupo predeterminado "Usuarios de dominio" se está utilizando.

7. Cuando OfficeScan encuentre una cuenta válida, mostrará el nombre de la cuenta en **Usuarios y grupos**. haga clic en el icono "adelante" (>) para mover la cuenta que aparece en **Usuarios y grupos seleccionados**.

   Si especifica un grupo de Active Directory, a todos los miembros que pertenezcan a él se les asignará la misma función. Si una cuenta determinada pertenece a al menos dos grupos y la función de estos no es la misma:

   - Los permisos de ambos grupos se fusionan. Si un usuario define una configuración determinada y se establece un conflicto de permisos para dicha configuración, se aplica el permiso superior.
   - Todas las funciones de usuario se muestran en los registros de sucesos del sistema. Por ejemplo, "El usuario Luis Cano ha iniciado sesión con las siguientes funciones: administrador, usuario avanzado".

8. Haga clic en **Siguiente**.

   Aparecerá la ventana **Paso 2: control de dominio del agente**.

9. Defina el alcance del árbol de agentes.

10. Haga clic en **Siguiente**.

    Aparecerá la ventana **Paso 3: definir el menú del árbol de agentes**.

11. Haga clic en los controles de **Opciones de menú disponibles** y especifique el permiso para cada opción de menú disponible.

    Para consultar una lista completa de las opciones de menú disponibles, consulte *Elementos del menú de administración de agentes en la página 14-15*.

12. Por último, haga clic en **Finalizar**.

13. Comunique al usuario que inicie sesión en la consola Web con su cuenta de dominio y su contraseña.

Trend Micro Control Manager

Trend Micro™ Control Manager™ es una consola de administración centralizada que gestiona los productos y servicios de Trend Micro en los niveles de gateway, servidor de correo, servidor de archivos y equipos de sobremesa corporativos. La consola de administración basada en Web de Control Manager ofrece un único punto de supervisión de productos y servicios administrados en toda la red.

Control Manager permite a los administradores del sistema supervisar y crear informes sobre actividades tales como infecciones, infracciones de seguridad o puntos de entrada de virus. Los administradores del sistema pueden descargar e implementar componentes en toda la red, con lo que se garantiza que la protección sea uniforme y actualizada. Control Manager permite actualizaciones manuales y programadas previamente, así como la configuración y la administración de los productos como grupos o individuos para una mayor flexibilidad.

Integración de Control Manager en esta versión de OfficeScan

Esta versión de OfficeScan incluye las siguientes características y funciones para la administración de los servidores de OfficeScan desde Control Manager:

- Cree, administre e implemente políticas para la prevención de pérdida de datos, el control de dispositivos y el antivirus de OfficeScan, y asigne derechos a los Agentes de OfficeScan desde la consola de Control Manager.

  En la siguiente tabla se enumeran las configuraciones de políticas disponibles en Control Manager 6.0 SP3 revisión 2.

TABLA 14-16. OfficeScan Tipos de administración de políticas de Control Manager

TIPO DE POLÍTICA	CARACTERÍSTICAS
Configuración del antivirus y el agente de OfficeScan	• Configuración de servicios adicionales • Configuración de la supervisión de comportamiento • Configuración de Control de dispositivos • Configuración de la exploración manual • Derechos y otras configuraciones • Configuración de la exploración en tiempo real • Lista de spyware/grayware permitido • Métodos de exploración • Configuración de Explorar ahora • Configuración de la exploración programada • Configuración de conexión sospechosa • Lista de programas de confianza • Configuración del agente de actualización • Configuración de la reputación Web

TIPO DE POLÍTICA	CARACTERÍSTICAS
Protección de datos	Configuración de las políticas de prevención de pérdida de datos **Nota** Administre los permisos del control de dispositivos para la protección de datos en las políticas del Agente de OfficeScan.

- Copie la siguiente configuración de un servidor de OfficeScan a otro de la consola de Control Manager:
  - *Tipos de identificadores de datos en la página 11-6*
  - *Plantillas de prevención de pérdida de datos en la página 11-21*

Nota

Si esta configuración se copia en servidores de OfficeScan en los que no hay activada una licencia de protección de datos, la configuración solo se aplicará cuando la licencia se active.

Versiones de Control Manager compatibles

Esta versión de OfficeScan admite las siguientes versiones de Control Manager:

- Control Manager 6.0 o posterior

Para obtener información sobre las direcciones IP que el servidor de OfficeScan y los Agentes de OfficeScan notifican a Control Manager, consulte *Pantallas que muestran direcciones IP en la página A-7*.

Aplique las revisiones y los archivos hotfix básicos más recientes de estas versiones de Control Manager para que Control Manager pueda administrar OfficeScan. Para obtener las revisiones y los archivos Hotfix más recientes, póngase en contacto con su proveedor de asistencia o visite el Centro de actualizaciones de Trend Micro en:

http://www.trendmicro.com/download/emea/?lng=es

Después de instalar OfficeScan, regístrelo en Control Manager y establezca la configuración de OfficeScan en la consola de administración de Control Manager. Consulte la *documentación de Control Manager* para obtener información sobre la administración de los servidores de OfficeScan.

Registrar OfficeScan en Control Manager

Importante

Tras actualizar a OfficeScan XG o una versión posterior desde OfficeScan 10.6 SP3 o una versión anterior, debe eliminar el registro de la conexión con el servidor de Control Manager y volver a registrar la conexión si desea usar la autorización con certificado.

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Control Manager**.
2. Especifique el nombre para mostrar de la entidad, que es el nombre del servidor de OfficeScan que se mostrará en Control Manager.

   De forma predeterminada, este nombre incluye el nombre de host del equipo del servidor y el nombre de este producto (por ejemplo, Servidor01_OSCE).

   Nota

   En Control Manager, los servidores de OfficeScan y otros productos que administra Control Manager se conocen como "entidades".

3. Especifique el nombre FQDN del servidor de Control Manager o la dirección IP, así como el número de puerto que debe utilizarse para conectarse al servidor. También puede conectarse con mayor seguridad mediante protocolo HTTPS.

   - En el caso de un servidor de OfficeScan de doble pila, escriba el nombre FQDN o la dirección IP (IPv4 o IPv6, si están disponibles) de Control Manager.
   - En el caso de un servidor de OfficeScan que solo utilice IPv4, escriba el nombre FQDN o la dirección IPv4 de Control Manager.

- En el caso de un servidor de OfficeScan que solo utilice IPv6, escriba el nombre FQDN o la dirección IPv6 de Control Manager.

4. Junto a **Certificado de Control Manager**, haga clic en **Examinar...** y seleccione el archivo del certificado descargado desde el servidor de Control Manager de destino.

   Para obtener el archivo del certificado de Control Manager, vaya al servidor de Control Manager y copie el archivo del certificado al servidor de OfficeScan desde la siguiente ubicación:

   ```
   <Carpeta de instalación de Control Manager>\Certificate\CA
   \TMCM_CA_Cert.pem
   ```

   Importante

   Si su empresa usa un certificado personalizado en el servidor de Control Manager, deberá cargar el certificado de la entidad de certificación raíz durante el registro de Control Manager.

   Para obtener más información, consulte *Autorización con certificado de Control Manager en la página 14-31*.

5. Si el servidor Web IIS de Control Manager requiere autenticación, escriba el nombre de usuario y la contraseña.

6. Si va a utilizar un servidor proxy para conectarse al servidor de Control Manager, especifique la siguiente configuración:

   - Protocolo de proxy
   - Nombre FQDN o dirección IPv4/IPv6 y puerto del servidor
   - ID y contraseña de usuario de autenticación para el servidor proxy

7. Decida si desea utilizar el reenvío por puerto de comunicación unidireccional o bidireccional y, a continuación, especifique la dirección IPv4/IPv6 y el puerto.

8. Para comprobar si OfficeScan se puede conectar al servidor de Control Manager según la configuración especificada, haga clic en **Comprobar la conexión**.

   Haga clic en **Registrar** si una conexión se ha establecido correctamente.

9. Si la versión del servidor de Control Manager es la 6.0 SP1 o posterior, aparecerá un mensaje instándole a que use el servidor de Control Manager como fuente de actualizaciones del Smart Protection Server integrado de OfficeScan. Haga clic en **Aceptar** para usar el servidor de Control Manager como fuente de actualizaciones del Smart Protection Server integrado o en **Cancelar** para continuar usando la fuente de actualizaciones actual (el ActiveUpdate Server, de forma predeterminada).

10. Si modifica cualquiera de los parámetros de esta pantalla tras registrarse, haga clic en **Configuración de la actualización** después de cambiar la configuración para notificar al servidor de Control Manager de los cambios.

Nota

Si el servidor de Control Manager está conectado a Deep Discovery, el proceso de suscripción automática se inicia una vez que se completa el registro. Para obtener más información, consulte *Configuración de la lista de objetos sospechosos en la página 14-34*.

11. Si no desea que el servidor de Control Manager siga administrando OfficeScan, haga clic en **Eliminar registro**.

Autorización con certificado de Control Manager

Antes de registrar OfficeScan en el servidor de Control Manager, debe obtener el archivo del certificado de Control Manager del servidor de Control Manager que se encuentra en la siguiente ubicación:

```
<Carpeta de instalación de Control Manager>\Certificate\CA
\TMCM_CA_Cert.pem
```

OfficeScan y Control Manager usan el certificado y el cifrado de clave pública para garantizar que solo se realizan registros autorizados y comunicaciones de administración de políticas entre los servidores. Si cualquiera de los servidores detecta una comunicación no autorizada, estos rechazarán el registro o la configuración de políticas que reciban.

Importante

Si su empresa usa un certificado personalizado en el servidor de Control Manager, deberá cargar el certificado de la entidad de certificación raíz durante el registro de Control Manager.

Comprobar el estado de OfficeScan en la Consola de administración de Control Manager

Procedimiento

1. Abra la consola de administración de Control Manager.

   Para abrir la consola de Control Manager en cualquier endpoint de la red, abra un explorador de Internet y escriba lo siguiente:

   `https://<nombre del servidor de Control Manager>/Webapp/login.aspx`

   Donde `<Nombre del servidor de Control Manager>` representa la dirección IP o el nombre del host del servidor de Control Manager.

2. En el menú principal, haga clic en **Directorios** > **Productos**.

3. En el árbol que se abre, vaya a **[Servidor de Control Manager]** > **Carpeta local carpeta** > **Nueva entidad**.

4. Compruebe si se abre el icono del servidor de OfficeScan.

Herramienta de exportación de políticas

La Herramienta de exportación de políticas del servidor de Trend Micro OfficeScan ayuda a los administradores a exportar la configuración de políticas de OfficeScan compatible con Control Manager 6.0 o posterior. Los administradores también necesitan Control Manager Import Tool para poder importar las políticas. La Herramienta de exportación de políticas es compatible con OfficeScan 10.6 Service Pack 1 y posterior.

- Configuración de la exploración en tiempo real
- Configuración de la exploración programada
- Configuración de la exploración manual
- Configuración de Explorar ahora
- Configuración del agente de actualización
- Configuración de la reputación Web
- Método de exploración
- Configuración de la supervisión de comportamiento
- Configuración de control de dispositivos
- Configuración de la prevención de pérdida de datos
- Derechos y otras configuraciones
- Configuración de servicios adicionales
- Lista de spyware/grayware permitido
- Configuración de conexión sospechosa

Uso de la Herramienta de exportación de políticas

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a la <*Carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\PolicyExportTool`.
2. Haga doble clic en `PolicyExportTool.exe` para iniciar la Herramienta de exportación de políticas.

   Se abre una pantalla de la interfaz de la línea de comandos y la Herramienta de exportación de políticas empieza a exportar la configuración. La herramienta crea dos carpetas (`PolicyClient` y `PolicyDLP`) en la carpeta `PolicyExportTool` que contienen la configuración exportada.
3. Copie las dos carpetas en la carpeta de instalación de Control Manager.
4. Ejecute la Herramienta de importación de políticas en el servidor de Control Manager.

   Para obtener información detallada sobre la Herramienta de importación de políticas, consulte el *Archivo léame de la Herramienta de importación de políticas* en el

servidor de Control Manager (`TMCM_installation folder\WebUI\WebApp\widget\common\tool\PolicyImport\`).

Nota

La Herramienta de exportación de políticas no exporta identificadores de datos personalizados o plantillas de DLP personalizadas. Para los administradores que necesiten exportar identificadores de datos personalizados y plantillas de DLP, realice una exportación manual desde la consola de OfficeScan y, a continuación, importe de forma manual el archivo mediante la consola de Control Manager.

Configuración de la lista de objetos sospechosos

Los objetos sospechosos son artefactos digitales que se generan al completar un análisis con productos de Trend Micro Deep Discovery u otros orígenes. OfficeScan puede sincronizar objetos sospechosos y recuperar acciones relacionadas con estos objetos desde un servidor de Control Manager 6.0 SP3 o posterior (conectado a Deep Discovery).

Después de suscribirse a Control Manager, seleccione los tipos de objetos sospechosos de manera que supervisen las rellamadas de C&C o los posibles ataques con destino que agentes identifique en la red. Entre los objetos sospechosos se incluyen:

- Lista de URL sospechosas
- Lista de IP sospechosas
- Lista de archivos sospechosos

Nota

En las versiones de la 10.6 a la 11.0 de OfficeScan, el origen principal de objetos sospechosos es Deep Discovery Analyzer. A partir de OfficeScan 11.0 SP1, el origen principal es Control Manager 6.0 SP3, cuyo proceso de gestión de objetos sospechosos es más sólido.

Si OfficeScan se ha suscrito a Deep Discovery Analyzer, solo estará disponible la lista de URL sospechosas. Si anula la suscripción de OfficeScan a Deep Discovery Analyzer, no podrá suscribirlo de nuevo. Es necesario suscribir OfficeScan a Control Manager, que está conectado a Deep Discovery, para sincronizar objetos sospechosos.

Para obtener más información sobre el modo en que Control Manager administra los objetos sospechosos, consulte *Manual del administrador de Control Manager*.

Configuración de la lista de objetos sospechosos

Durante el registro de OfficeScan en Control Manager, Control Manager implementa una clave API en OfficeScan para iniciar el proceso de suscripción. Para activar este proceso de suscripción automático, póngase en contacto con el administrador de Control Manager para asegurarse de que Control Manager está conectado a Deep Discovery y de que la configuración es la correcta.

Para obtener más información sobre cómo registrar un servidor de Control Manager, consulte *Registrar OfficeScan en Control Manager en la página 14-29*.

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Lista de objetos sospechosos**.
2. Seleccione la lista que se activará en los agentes.
   - Lista de URL sospechosas
   - Lista de IP sospechosas (solo disponible cuando se ha suscrito al servidor de Control Manager registrado)
   - Lista de archivos sospechosos (solo disponible cuando se ha suscrito al servidor de Control Manager registrado)

   Los administradores pueden sincronizar manualmente las listas de objetos sospechosos en cualquier momento haciendo clic en el botón **Sincronizar ahora**.

3. En **Actualizar las listas de objetos sospechosos en los agentes de OfficeScan**, especifique cuándo actualizan los agentes las listas de objetos sospechosos.

   - **En función del programa de actualizaciones de los componentes de los agentes de OfficeScan**: los Agentes de OfficeScan actualizan las listas de objetos sospechosos según el programa de actualización actual.
   - **De forma automática tras actualizar las listas de objetos sospechosos en el servidor**: los Agentes de OfficeScan actualizan las listas de objetos sospechosos automáticamente cuando el servidor de OfficeScan recibe las listas actualizadas.

   Nota

   Los Agentes de OfficeScan no están configurados para recibir actualizaciones de agentes de actualización que realicen actualizaciones incrementales de las listas de objetos sospechosos a las que estén suscritos durante la sincronización.

4. Haga clic en **Guardar**.

Servidores de referencia

Una de las maneras en las que el Agente de OfficeScan determina la política o el perfil que debe utilizar consiste en comprobar el estado de conexión con el servidor de OfficeScan. Si un Agente de OfficeScan interno (o un agente de la red empresarial) no se puede conectar al servidor, el estado del agente cambia a desconectado. A continuación, el agente aplica una política o un perfil diseñados para agentes externos. Los servidores de referencia solucionan este problema.

Cualquier Agente de OfficeScan que pierde la conexión con el servidor de OfficeScan se intentará conectar con los servidores de referencia. Si el agente establece correctamente una conexión con un servidor de referencia, se aplica la política o el perfil de agentes internos.

Entre las políticas y los perfiles administrador por servidores de referencia se incluyen los siguientes:

- Perfiles del cortafuegos
- Políticas de reputación Web
- Políticas de protección de datos
- Políticas de Control de dispositivos

Tenga en cuenta lo siguiente:

- Asigne equipos con capacidades de servidor, como un servidor Web, un servidor SQL o un servidor FTP, como servidores de referencia. Puede especificar un máximo de 320 servidores de referencia.
- Los Agentes de OfficeScan se conectan con el primer servidor de referencia de la lista de servidores de referencia. Si no se puede establecer la conexión, el agente intenta conectar con el siguiente servidor de la lista.
- Los Agentes de OfficeScan utilizan los servidores de referencia al determinar la configuración del antivirus (supervisión de comportamiento, control de dispositivos, perfiles del cortafuegos y la política de reputación Web) o de la protección de datos que se va a usar. Los servidores de referencia no administran agentes ni implementan actualizaciones y configuraciones de agente. El servidor de OfficeScan lleva a cabo esas tareas.
- El Agente de OfficeScan no puede enviar registros a servidores de referencia o utilizarlos como orígenes de actualización.

Administrar la lista de servidores de referencia

Procedimiento

1. Vaya a **Agentes** > **Cortafuegos** > **Perfiles** o **Agentes** > **Ubicación del Endpoint**.
2. En función de la pantalla que aparezca, realice lo siguiente:
   - Si se encuentra en la pantalla **Perfiles del cortafuegos para agentes**, haga clic en **Editar la lista de servidores de referencia**.

- Si se encuentra en la pantalla **Ubicación del Endpoint**, haga clic en **Lista de servidores de referencia**.

3. Seleccione **Activar la lista de servidores de referencia**.
4. Para agregar un endpoint a la lista, haga clic en **Agregar**.
   a. Especifique la dirección IPv4/IPv6, el nombre o el nombre del dominio completo (FQDN) del endpoint, por ejemplo:
      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`
   b. Escriba el puerto a través del cual los agentes se comunican con este endpoint. Especifique cualquier puerto de contacto abierto (como los puertos 20, 23 o 80) en el servidor de referencia.

      Nota

      Para especificar otro número de puerto para el mismo servidor de referencia, repita los pasos 2a y 2b. El Agente de OfficeScan utiliza el primer número de puerto de la lista y, si la conexión falla, utiliza el siguiente número de puerto.

   c. Haga clic en **Guardar**.
5. Para editar la configuración de un endpoint de la lista, haga clic en el nombre del endpoint. Modifique el nombre del endpoint o el puerto y, a continuación, haga clic en **Guardar**.
6. Para quitar un endpoint de la lista, seleccione el nombre del endpoint y, a continuación, haga clic en **Eliminar**.
7. Para permitir que los endpoints actúen como servidores de referencia, haga clic en **Asignar a agentes**.

Configuración de las notificaciones del administrador

Defina la configuración de las notificaciones del administrador para permitir a OfficeScan enviar correctamente notificaciones por correo electrónico y captura SNMP. OfficeScan también puede enviar notificaciones a través del registro de sucesos de Windows NT, pero no hay ninguna configuración establecida para este canal de notificación.

OfficeScan puede enviar notificaciones a usted y otros administradores de OfficeScan cuando se detecte lo siguiente:

TABLA 14-17. Detecciones que activan las notificaciones de administrador

DETECCIONES	CANALES DE NOTIFICACIÓN		
	CORREO ELECTRÓNICO	CAPTURA SNMP	REGISTROS DE SUCESOS DE WINDOWS NT
Virus y malware	Sí	Sí	Sí
Spyware y grayware	Sí	Sí	Sí
Transmisiones de activos digitales	Sí	Sí	Sí
Rellamadas de C&C	Sí	Sí	Sí
Epidemias de virus y malware	Sí	Sí	Sí
Epidemias de spyware y grayware	Sí	Sí	Sí
Epidemias de infracciones del cortafuegos	Sí	No	No
Epidemias de sesiones de carpetas compartidas	Sí	No	No

Detecciones	Canales de notificación		
	Correo electrónico	Captura SNMP	Registros de sucesos de Windows NT
Epidemias de rellamada C&C	Sí	Sí	Sí

Configuración de general de las notificaciones

Procedimiento

1. Vaya a **Administración** > **Notificaciones** > **Configuración general**.
2. Defina la configuración de las notificaciones de correo electrónico.
   a. Especifique una dirección IPv4 o IPv6 o un Nombre del Endpoint en el campo **Servidor SMTP**.
   b. Escriba un número de puerto comprendido entre 1 y 65535.
   c. Especifique una dirección de correo electrónico.

      Si desea activar ESMTP en el siguiente paso, especifique una dirección de correo electrónico válida.
   d. Si lo desea, también puede activar **ESMTP**.
   e. Especifique el nombre de usuario y la contraseña de la dirección de correo electrónico que ha introducido en el campo **Desde**.
   f. Seleccione un método de autenticación del agente en el servidor:
      - **Inicio de sesión**: el inicio de sesión es una versión antigua del agente del usuario de correo. Tanto el servidor como el agente utilizan BASE64 para autenticar el nombre de usuario y la contraseña.
      - **Texto sin formato**: el texto sin formato es el método más sencillo, pero también puede resultar inseguro, ya que el nombre de usuario y la contraseña se envían como una cadena y cifrada en BASE64 antes de enviarse por Internet.

- **CRAM-MD5**: CRAM-MD5 combina un mecanismo de autenticación de pregunta-respuesta y un algoritmo criptográfico Message Digest 5 para intercambiar y autenticar información.

3. Defina la configuración de las notificaciones de las capturas SNMP.

   a. Especifique una dirección IPv4 o IPv6 o un Nombre del Endpoint en el campo **Dirección IP del servidor**.

   b. Especifique un nombre de comunidad que sea difícil de adivinar.

   Nota

   Por motivos de seguridad, el nombre de la comunidad se muestra como un valor enmascarado mediante un asterisco (*). El valor predeterminado asignado es: «público».

4. Haga clic en **Guardar**.

Registros de sucesos del sistema

OfficeScan registra los sucesos relacionados con el programa servidor, tales como la desconexión y el inicio. Utilice estos registros para comprobar que el servidor de OfficeScan y los servicios funcionan correctamente.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Ver registros de sucesos del sistema

Procedimiento

1. Vaya a **Registros** > **Sucesos del sistema**.

2. En **Suceso**, busque los registros que precisan alguna acción más. OfficeScan registra los sucesos siguientes:

TABLA 14-18. Registros de sucesos del sistema

TIPO DE REGISTRO	SUCESOS
Master Service y servidor de base de datos de OfficeScan	• El servicio maestro se ha iniciado • El servicio maestro se ha detenido correctamente • El servicio maestro no se ha detenido correctamente
Prevención de epidemias	• Se ha activado la prevención de epidemias • Se ha desactivado la prevención de epidemias • Número de sesiones de carpetas compartidas en los últimos <número de minutos>
Copia de seguridad de la base de datos	• Copia de seguridad de la base de datos realizada con éxito • Copia de seguridad de la base de datos no realizada
Acceso a la consola Web basado en funciones	• Inicio de sesión en la consola • Modificación de la contraseña • Cierre de sesión de la consola • Tiempo de espera de la sesión excedido (el usuario se desconecta automáticamente)
Autenticación del servidor	• El Agente de OfficeScan ha recibido comandos no válidos del servidor • El certificado de autenticación no es válido o ha caducado

3. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Administración de registros

OfficeScan guarda registros completos sobre las detecciones de riesgos de seguridad, sucesos y actualizaciones. Puede utilizar estos registros para valorar las políticas de protección de la organización e identificar los Agentes de OfficeScan que tienen un mayor riesgo de sufrir una infección o un ataque. Utilice también estos registros para comprobar la conexión agente-servidor y ver si las actualizaciones de los componentes se realizaron correctamente.

OfficeScan también utiliza un mecanismo de verificación de tiempo central para garantizar la consistencia de tiempo entre el servidor y los agentes de OfficeScan. Esta función evita que las inconsistencias provocadas por las zonas horarias, el horario de verano y las diferencias horarias puedan dar lugar a confusiones al visualizar los registros.

Nota

OfficeScan lleva a cabo una comprobación de la hora de todos los registros excepto de los registros de actualización del servidor y de sucesos del sistema.

El servidor de OfficeScan recibe los siguientes registros de Agentes de OfficeScan:

- *Visualización de los registros de virus/malware en la página 7-98*
- *Visualización de los registros de spyware/grayware en la página 7-107*
- *Visualización de los registros de restauración de spyware y grayware en la página 7-111*
- *Ver registros del cortafuegos en la página 13-31*
- *Ver registros de reputación Web en la página 12-23*
- *Ver los registros de conexión sospechosa en la página 8-15*
- *Ver los registros de archivos sospechosos en la página 7-111*
- *Visualización de los registros de rellamadas de C&C en la página 12-24*
- *Visualización de registros de supervisión del comportamiento en la página 9-18*

- *Visualización de los registros de Control de dispositivos en la página 10-20*
- *Visualización de los registros de operaciones de exploración en la página 7-113*
- *Visualización de los registros de prevención de pérdida de datos en la página 11-61*
- *Visualizar los registros de actualización de agentes de OfficeScan en la página 6-55*
- *Ver los registros de comprobación de la conexión en la página 15-49*

El servidor de OfficeScan crea los registros siguientes:

- *Registros de actualización del servidor de OfficeScan en la página 6-29*
- *Registros de sucesos del sistema en la página 14-41*

Los siguientes registros también se encuentran disponibles en el servidor de OfficeScan y los Agentes de OfficeScan:

- *Registros de sucesos de Windows en la página 18-26*
- *Registros del servidor de OfficeScan en la página 18-3*
- *Registros de agentes de OfficeScan en la página 18-15*

Mantenimiento de los registros

Para evitar que los registros ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros desde la consola Web.

Eliminar registros según un programa

Procedimiento

1. Vaya a **Registros** > **Mantenimiento de los registros**.
2. Seleccione **Activar la eliminación programada de registros**.
3. Seleccione los tipos de registros que deben eliminarse. Todos los registros generados por OfficeScan, excepto los de depuración, se pueden eliminar en

función de un programa. Para el caso de los registros de depuración, desactive la creación de registros de depuración para detener la recopilación de registros.

Nota

En el caso de los registros de virus y malware, se pueden eliminar los registros generados a partir de determinados tipos de exploración y de Damage Cleanup Services. En el caso de los registros de spyware y grayware, puede eliminar los registros de determinados tipos de exploración. Para obtener información detallada acerca de los tipos de exploración, consulte *Tipos de exploración en la página 7-15*.

4. Seleccione si deben eliminarse los registros de todos los tipos de archivos seleccionados o sólo los que superan un determinado número de días.
5. Especifique la frecuencia y la hora de la eliminación de registros.
6. Haga clic en **Guardar**.

Eliminar manualmente los registros

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Riesgos de seguridad** o **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Siga uno de los pasos siguientes:
   - Si accede a la pantalla **Registros de riesgos de seguridad**, haga clic en **Eliminar registros** .
   - Si accede a la pantalla **Administración de agentes**, haga clic en **Registros** > **Eliminar registros**.
4. Seleccione los tipos de registros que deben eliminarse. Solo se pueden eliminar de forma manual los siguientes registros:

- Registros de supervisión del comportamiento
- Registros de rellamadas de C&C
- Registros de prevención de pérdida de datos
- Registros de control de dispositivos
- Registros del cortafuegos
- Registros del aprendizaje automático predictivo
- Registros de spyware/grayware
- Registros de operaciones de exploración
- Registros de conexión sospechosa
- Registros de archivos sospechosos
- Registros de virus/malware
- Registros de reputación Web

Nota

En el caso de los registros de virus y malware, se pueden eliminar los registros generados a partir de determinados tipos de exploración y de Damage Cleanup Services. En el caso de los registros de spyware y grayware, puede eliminar los registros de determinados tipos de exploración.

Para obtener información detallada acerca de los tipos de exploración, consulte *Tipos de exploración en la página 7-15*.

5. Seleccione si deben eliminarse los registros de todos los tipos de archivos seleccionados o sólo los que superan un determinado número de días.
6. Haga clic en **Eliminar**.

Licencias

Vea, active y renueve los servicios de licencias de OfficeScan en la consola Web y active o desactive el cortafuegos de OfficeScan. El cortafuegos de OfficeScan es parte del servicio Antivirus, que también incluye compatibilidad con la prevención de epidemias.

Nota

Algunas características nativas de OfficeScan, como la protección de datos y el soporte para Virtual Desktop tienen sus propias licencias. Las licencias para estas características se activan y administran desde Plug-in Manager. Para obtener más información sobre las licencias de estas características, consulte *Licencia de protección de datos en la página 3-4* y *Licencia del Soporte para Virtual Desktop en la página 15-85*.

Un servidor de OfficeScan que solo utilice IPv6 no se puede conectar al servidor de registro en línea de Trend Micro para activar o renovar la licencia. Es necesario un servidor proxy de doble pila que convierta direcciones IP, como DeleGate, para permitir al servidor de OfficeScan que se conecte al servidor de registro.

Ver información sobre la licencia del producto

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Licencia del producto**.
2. Vea el resumen del estado de la licencia, que aparece en la parte superior de la pantalla. Durante los casos siguientes aparecen recordatorios sobre las licencias:

TABLA 14-19. Recordatorios de licencia

TIPO DE LICENCIA	RECORDATORIO
Versión completa	• Durante el periodo de gracia del producto. La duración del periodo de gracia puede varía entre una zona y otra. Consulte con su representante de Trend Micro para comprobar la duración de su periodo de gracia. • Cuando la licencia caduca y finaliza el periodo de gracia. Durante este tiempo no podrá obtener asistencia técnica ni actualizar componentes. Los motores de exploración seguirán explorando los endpoints, pero utilizarán componentes obsoletos. Es posible que estos componentes obsoletos no puedan protegerle completamente frente a los riesgos de seguridad más recientes.
Versión de prueba	Cuando caduca la licencia. Durante este período, OfficeScan desactiva las actualizaciones de componentes. Los motores de exploración seguirán explorando los endpoints, pero utilizarán componentes obsoletos. Es posible que estos componentes obsoletos no puedan protegerle completamente frente a los riesgos de seguridad más recientes.

3. Ver información sobre la licencia. En el apartado **Información sobre la licencia** se muestra la siguiente información:

   - **Servicios**: incluye todos los servicios de licencias de OfficeScan.
   - **Estado**: muestra "Activada", "No activada", "Caducada" o "En período de gracia". Cuando un servicio dispone de múltiples licencias y al menos una está activa, el estado que aparece es "Activada".
   - **Versión**: muestra si la versión es "Completa" o "De prueba". Si tiene tanto la versión completa, como la de prueba, la versión se mostrará como "Completa".
   - **Fecha de vencimiento**: cuando un servicio tiene múltiples licencias, se muestra la fecha de vencimiento más reciente. Por ejemplo, si las fechas de caducidad son 31/12/2007 y 30/06/2008, aparecerá 30/06/2008.

Nota

La versión y la fecha de caducidad de los servicios de licencia que no se han activado es "N/D".

4. OfficeScan permite activar varias licencias para un servicio de licencias. Haga clic en el nombre del servicio para ver todas las licencias (activas y caducadas) correspondientes a ese servicio.

Activar o renovar una licencia

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Licencia del producto**.
2. Haga clic en el nombre del servicio de licencias.
3. En la pantalla **Detalles de la licencia del producto** que se abre, haga clic en **Nuevo código de activación**.
4. Escriba el código de activación en la pantalla que se abre y haga clic en **Guardar**.

Nota

Antes de activar un servicio es necesario registrarlo. Para más información sobre la clave de registro y el código de activación, póngase en contacto con un representante de Trend Micro.

5. De nuevo en la pantalla **Detalles de la licencia del producto**, haga clic en **Información de la actualización** para actualizar la página con los detalles nuevos de la licencia y el estado del servicio. Esta pantalla también muestra un enlace al sitio Web de Trend Micro en el que puede visualizar información detallada sobre la licencia.

Copia de seguridad de la base de datos de OfficeScan

La base de datos del servidor de OfficeScan contiene toda la configuración de OfficeScan, incluidos los derechos y la configuración de exploración. En caso de que se dañe la base de datos del servidor, podrá recuperarla si ha efectuado una copia de seguridad. Realice en cualquier momento una copia de seguridad de la base datos de forma manual o bien configure un programa de copia de seguridad.

Al realizar la copia de seguridad de la base de datos, OfficeScan contribuye automáticamente a desfragmentar la base de datos y repara los posibles errores del archivo de índice.

Compruebe los registros de sucesos del sistema para determinar el estado de la copia de seguridad. Para obtener más información, consulte *Registros de sucesos del sistema en la página 14-41*.

Consejo

Trend Micro recomienda configurar un programa de copia de seguridad automática. Programe la copia de seguridad en horas de menor actividad en las que el tráfico del servidor es inferior.

¡ADVERTENCIA!

no realice la copia de seguridad con ninguna otra herramienta o software. Configure la copia de seguridad de la base de datos únicamente desde la consola OfficeScan Web.

Crear una copia de seguridad de la base de datos de OfficeScan

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Copia de seguridad de la base de datos**.

2. Escriba la ubicación en donde desea guardar la base de datos. Si la carpeta no existe todavía, seleccione **Crear la carpeta si no existe**. Se debe incluir la unidad y la ruta de acceso completa del directorio (por ejemplo, `C:\OfficeScan\DatabaseBackup`).

   De forma predeterminada, OfficeScan guarda la copia de seguridad en el siguiente directorio: *Carpeta de instalación del servidor*`>\DBBackup`

   Nota

   OfficeScan crea una subcarpeta en la ruta de la copia de seguridad. El nombre de la carpeta indica la hora de la copia de seguridad con el siguiente formato: DDMMAAAA_HHMMSS. OfficeScan conserva las 7 últimas carpetas de copia de seguridad y va eliminando de forma automática las carpetas anteriores.

3. Si la ruta de la copia de seguridad corresponde a un equipo remoto (una ruta UNC), escriba un nombre de cuenta y la contraseña correspondientes. Asegúrese de que la cuenta tiene derechos de escritura en el equipo.

4. Para configurar el programa de copia de seguridad:

   a. Seleccione **Activar la copia de seguridad de la base de datos programada**.

   b. Especifique la frecuencia y la hora de la copia de seguridad.

   c. Para realizar una copia de seguridad de la base de datos y guardar los cambios realizados, haga clic en **Crear copia de seguridad ahora**. Para guardar solo sin realizar la copia de seguridad de la base de datos, haga clic en **Guardar**.

Restaurar los archivos de Database Backup

Procedimiento

1. Detenga el OfficeScan Master Service.

2. Sobrescriba los archivos de la base de datos de <*carpeta de instalación del servidor*>`\PCCSRV\HTTPDB` con los archivos de copia de seguridad.

3. Reinicie el OfficeScan Master Service.

Herramienta de migración de SQL Server

Los administradores pueden migrar la base de datos de OfficeScan existente de su estilo CodeBase nativo a una base de datos SQL Server utilizando la herramienta de migración de SQL Server. La herramienta de migración de SQL Server es compatible con las siguientes migraciones de bases de datos:

- Base de datos CodeBase de OfficeScan a una nueva base de datos SQL Server Express.
- Base de datos CodeBase de OfficeScan a una base de datos SQL Server existente.
- Base de datos SQL de OfficeScan (anteriormente migrada) movida a otra ubicación.

Utilizar la herramienta de migración de SQL Server

La herramienta de migración de SQL migra la base de datos CodeBase existente a una base de datos SQL mediante SQL Server 2014 SP2 Express.

Consejo

Después de migrar la base de datos de OfficeScan, puede mover la base de datos SQL recién migrada a un servidor SQL Server diferente. Vuelva a ejecutar la herramienta de migración de SQL Server y seleccione **Cambiar a una base de datos SQL de OfficeScan existente** para usar el otro servidor SQL Server.

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a <*Carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\SQL`.
2. Haga doble clic en `SQLTxfr.exe` para ejecutar la herramienta.

   Se abre la consola de la **herramienta de migración de SQL Server**.

3. Elija el tipo de migración:

Opción	Descripción
Instalar una nueva instancia de SQL Server 2014 SP2 Express y migrar la base de datos de OfficeScan	Instala SQL Server 2014 SP2 Express automáticamente y migra la base de datos de OfficeScan existente a una base de datos SQL nueva. **Nota** OfficeScan asigna automáticamente el puerto 1433 al servidor SQL Server.
Migrar la base de datos de OfficeScan a un servidor SQL Server existente	Migra la base de datos de OfficeScan existente a una nueva base de datos SQL en un SQL Server existente.
Cambiar a una base de datos SQL de OfficeScan existente	Cambia la configuración de OfficeScan de modo que haga referencia a una base de datos SQL de OfficeScan en un SQL Server existente.

4. Especifique el **Nombre del servidor** de la manera siguiente:

   - Para nuevas instalaciones de SQL: <nombre de host o dirección IP de SQL Server>\<nombre de la instancia>
   - Para migraciones de SQL Server: <nombre de host o dirección IP de SQL Server>,<número del puerto>\<nombre de la instancia>
   - Al cambiar a una base de datos SQL de OfficeScan existente: <nombre de host o dirección IP de SQL Server>,<número del puerto>\<nombre de la instancia>

Importante

OfficeScan crea automáticamente una instancia para la base de datos de OfficeScan cuando se instala SQL Server. Cuando realice la migración a un servidor o una base de datos SQL existente, escriba el nombre de la instancia de OfficeScan existente en el servidor SQL Server.

5. Proporcione las credenciales de autenticación de la base de datos de SQL Server.

- Cuando utilice la **Cuenta de Windows** para iniciar sesión en el servidor, el **Nombre de usuario** debe tener el siguiente formato:

  nombre_de_dominio\nombre_de_usuario o nombre_de_usuario

Importante

La cuenta de usuario debe pertenecer al grupo de administradores locales o al administrador de Active Directory (AD) integrado; debe configurar las siguientes políticas de asignación de derechos del usuario mediante la **Directiva de seguridad local** o la consola de **Administración de directivas de grupo** de Windows:

- Iniciar sesión como un servicio
- Iniciar sesión como un trabajo por lotes
- Permitir inicio de sesión local

La cuenta de usuario debe tener además las siguientes funciones de base de datos:

- dbcreator
- bulkadmin
- db_owner

6. En el caso de instalaciones de SQL Server nuevas, introduzca una contraseña nueva y confírmela.

Nota

Las contraseñas deben cumplir los siguientes requisitos de seguridad mínimos:

a. Longitud mínima: 8 caracteres

b. Deben contener por lo menos tres de los siguientes caracteres:

- Mayúsculas: A - Z
- Minúsculas: a - z
- Números: 0 - 9 0 - 9
- Caracteres especiales: !@#$^*?_~-();.+: !@#$^*?_~-();.+:

7. Especifique el **nombre de la base de datos** de OfficeScan en SQL Server.

   Al realizar la migración de una base de datos CodeBase de OfficeScan a una base de datos SQL nueva, OfficeScan crea automáticamente la base de datos nueva con el nombre proporcionado.

8. También puede realizar las siguientes tareas:

   - Haga clic en **Probar la conexión** para comprobar las credenciales de autenticación de SQL Server o de la base de datos existente.
   - Haga clic en **Alerta de base de datos SQL no disponible…** para configurar las notificaciones de la base de datos SQL.

     Para conocer más detalles, consulte *Configurar la alerta de base de datos SQL no disponible en la página 14-55*.

9. Haga clic en **Inicio** para aplicar los cambios de configuración.

Configurar la alerta de base de datos SQL no disponible

OfficeScan envía automáticamente esta alterca cuando la base de datos SQL no está disponible.

¡ADVERTENCIA!

OfficeScan detiene todos los servicios de manera automática cuando la base de datos no está disponible. OfficeScan no puede registrar información del agente o del suceso, realizar actualizaciones o configurar agentes cuando la base de datos no está disponible.

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a <*Carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\SQL`.

2. Haga doble clic en `SQLTxfr.exe` para ejecutar la herramienta.

   Se abre la consola de la **herramienta de migración de SQL Server**.

3. Haga clic en **Alerta de base de datos SQL no disponible…**

   Aparece la pantalla **Alerta de servidor SQL Server no disponible**.

4. Introduzca las direcciones de correo electrónico de los destinatarios de la alerta.

   Separe las entradas múltiples mediante punto y coma (;).

5. Modifique el **asunto** y el **mensaje** según sea necesario.

   OfficeScan proporciona las siguientes variables de token:

   TABLA 14-20. Tokens de la alerta de base de datos SQL no disponible

VARIABLE	DESCRIPCIÓN
%x	Nombre de la instancia del servidor SQL Server de OfficeScan
%s	Nombre del servidor de OfficeScan afectado

6. Haga clic en **Aceptar**.

Configuración de la conexión del servidor Web y el agente de OfficeScan

Durante la instalación del servidor de OfficeScan, el programa de instalación configura automáticamente un servidor Web que permite la conexión de los equipos en red al servidor de OfficeScan. Configure el servidor Web al que se conectarán los agentes del endpoint conectados en red.

Si modifica la configuración del servidor Web externamente (por ejemplo, desde la consola de administración de IIS), duplique los cambios en OfficeScan. Por ejemplo, si cambia manualmente la dirección IP del servidor para los equipos conectados en red o si le asigna una dirección IP dinámica, tendrá que volver a configurar el servidor de OfficeScan.

¡ADVERTENCIA!

Si se cambia la configuración de la conexión, se podría perder la conexión de forma permanente entre el servidor y los agentes, por lo que sería necesario volver a implementar los Agentes de OfficeScan.

Configurar la conexión

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Conexión del agente**.
2. Escriba el nombre del dominio o la dirección IPv4/IPv6 y el número de puerto del servidor Web.

   Nota

   Este número de puerto es el puerto de confianza que utiliza el servidor de OfficeScan para comunicarse con los Agentes de OfficeScan.

3. Haga clic en **Guardar**.

Comunicación entre servidor y agente

Puede configurar OfficeScan para asegurarse de que la comunicación entre el servidor y los agentes sea válida. OfficeScan utiliza criptografía de claves públicas y características de cifrado avanzadas para proteger todas las comunicaciones entre el servidor y los agentes.

Para obtener más detalles acerca de las características de protección de comunicaciones, consulte lo siguiente:

- *Autenticación de las comunicaciones iniciadas por el servidor en la página 14-58*
- *Cifrado mejorado para la comunicación entre servidor y agente en la página 14-63*

Autenticación de las comunicaciones iniciadas por el servidor

OfficeScan usa la criptografía de claves públicas para autenticar las comunicaciones que el servidor de OfficeScan inicia con los agentes. Con la criptografía de claves públicas, el servidor mantiene una clave privada e implementa una clave pública en todos los agentes. Los agentes usan la clave pública para verificar que las comunicaciones entrantes provienen del servidor y son válidas. Los agentes responden si la verificación se ha realizado correctamente.

Nota

OfficeScan no autentica las comunicaciones que los agentes inician en el servidor.

Las claves públicas y privadas están asociadas a un certificado de Trend Micro. Durante la instalación del servidor de OfficeScan, el certificado se guarda en el almacén de certificados del host. Utilice la herramienta Administrador de certificados de autenticación para administrar los certificados y las claves de Trend Micro.

A la hora de decidir si usar una sola clave de autenticación en todos los servidores de OfficeScan, tenga en cuenta lo siguiente:

- La implementación de una sola clave de certificado es una práctica común en los niveles de seguridad estándar. Este enfoque equilibra el nivel de seguridad de su organización y reduce los gastos generales asociados con el mantenimiento de varias claves.
- La implementación de varias claves de certificado en los servidores de OfficeScan proporciona un nivel de seguridad máximo. Este enfoque aumenta el mantenimiento necesario cuando las claves de certificado caducan y es necesario redistribuirlas entre los servidores.

Importante

Antes de volver a instalar el servidor de OfficeScan, realice una copia de seguridad del certificado existente. Una vez que se complete la nueva instalación, importe el certificado del cual ha realizado la copia de seguridad para que no se interrumpa la autenticación de las comunicaciones entre el servidor de OfficeScan y los Agentes de OfficeScan. Si crea un certificado nuevo durante la instalación del servidor, los Agentes de OfficeScan no pueden autenticar la comunicación del servidor porque continúan utilizando el certificado antiguo (que ya no existe).

Para obtener más información sobre cómo restaurar, exportar e importar certificados, y sobre cómo realizar copias de seguridad de estos, consulte *Utilizar el administrador de certificados de autenticación en la página 14-60*.

Configurar la autenticación de las comunicaciones iniciadas por el servidor

Procedimiento

1. En el servidor de OfficeScan, vaya a `<carpeta_de_instalación_del_servidor>\PCCSRV` y abra `ofcscan.ini` con un editor de texto.

2. Agregue o modifique la cadena de texto `SGNF` en la sección `[configuración global]`.

   Para activar la autenticación: `SGNF=1`

   Para desactivar la autenticación: `SGNF=0`

   Nota

   OfficeScan activa la autenticación de forma predeterminada. Agregue la clave `SGNF` al archivo `ofcscan.ini` únicamente si desea desactivar esta función.

3. En la consola Web, vaya a **Agentes** > **Configuración global para los agentes** y haga clic en **Guardar** para implementar la configuración en los agentes.

Utilizar el administrador de certificados de autenticación

El servidor de OfficeScan conserva los certificados caducados de los agentes con claves públicas que han caducado. Por ejemplo, los agentes que no se han conectado al servidor durante un largo período de tiempo tienen claves públicas caducadas. Cuando los agentes vuelven a conectarse, asocian la clave pública caducada al certificado caducado, lo que les permite reconocer las comunicaciones iniciadas por el servidor. A continuación, el servidor implementa la clave pública más reciente en los agentes.

Al configurar certificados, tenga en cuenta lo siguiente:

- La ruta del certificado admite unidades asignadas y rutas UNC.
- Introduzca una contraseña fuerte y guárdela para referencia futura.

Importante

Al utilizar la herramienta Administrador de certificados de autenticación, tenga en cuenta los siguientes requisitos:

- El usuario debe tener derechos de administrador.
- La herramienta solo puede administrar los certificados ubicados en el endpoint local.

Procedimiento

1. En el servidor de OfficeScan, abra el símbolo del sistema y cambie el directorio a <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\CertificateManager`.
2. Ejecute cualquiera de los comandos siguientes:

COMANDO	EJEMPLO	DESCRIPCIÓN
`CertificateManager.exe -c [contraseña_de_copia_de_seguridad]`	`CertificateManager.exe -c strongpassword`	Genera un nuevo certificado de Trend Micro y reemplaza el existente. Ejecute este comando si el certificado existente está caducado o si se ha filtrado a partes no autorizadas.

COMANDO	EJEMPLO	DESCRIPCIÓN
CertificateManager.exe -b [contraseña] [ruta del certificado] **Nota** El certificado está en formato .zip.	CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip	Realiza una copia de seguridad de todos los certificados de Trend Micro emitidos por el servidor actual de OfficeScan. Ejecute este comando para realizar una copia de seguridad del certificado en el servidor de OfficeScan. **Nota** Hacer una copia de seguridad de los certificados del servidor de OfficeScan le permite usar estos certificados en caso de que deba volver a instalar el servidor de OfficeScan.
CertificateManager.exe -r [contraseña] [ruta del certificado] **Nota** El certificado está en formato .zip.	CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip	Restaura todos los certificados de Trend Micro en el servidor. Ejecute este comando para restaurar el certificado en un servidor de OfficeScan que se ha vuelto a instalar.

COMANDO	EJEMPLO	DESCRIPCIÓN
CertificateManager.exe -e [contraseña] [ruta del certificado]	`CertificateManager.exe -e <carpeta_de_instalación_del_agente>\OfcNTCer.dat`	Exporta la clave pública del Agente de OfficeScan asociada al certificado actualmente en uso. Ejecute este comando si se daña la clave pública que utilizan los agentes. Copie el archivo `.dat` en la carpeta raíz del agente para que se sobrescriba el existente. **Importante** La ruta de archivo del certificado en el Agente de OfficeScan debe ser: `<carpeta_de_instalación_del_agente>\OfcNTCer.dat`
CertificateManager.exe -i [contraseña] [ruta del certificado] **Nota** El nombre de archivo predeterminado del certificado es: `OfcNTCer.pfx`	`CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx`	Importa un certificado de Trend Micro en el almacén de certificados.

COMANDO	EJEMPLO	DESCRIPCIÓN
`CertificateManager.exe -l [ruta de CSV]`	`CertificateManager.exe -l D:\Test\MismatchedAgentList.csv`	Muestra los agentes (en formato CSV) que utilizan actualmente un certificado que no coincide.

Cifrado mejorado para la comunicación entre servidor y agente

OfficeScan proporciona un cifrado mejorado de la comunicación entre el servidor y los agentes mediante el Estándar de cifrado avanzado (AES) 256 para cumplir los estándares de seguridad gubernamentales.

Importante

OfficeScan solo es compatible con el cifrado AES-256 en servidores y agentes que ejecutan OfficeScan 11.0 SP1, o posterior, y Plug-in Manager 2.2, o versiones posteriores.

¡ADVERTENCIA!

Asegúrese de actualizar a la versión 11.0 SP1 todos los Agentes de OfficeScan que administra el servidor antes de activar el cifrado AES-256. Las versiones antiguas del Agente de OfficeScan no podrán descifrar la comunicación cifrada AES-256. Si activa el cifrado AES-256 en versiones antiguas del Agente de OfficeScan, perderá la comunicación con el servidor de OfficeScan por completo cuando utilice un servidor proxy.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Red**.
3. Vaya a la sección **Comunicación entre servidor y agente**.
4. Haga clic en el botón **Cambiar** junto a **Usar cifrado AES-256 para la comunicación entre el servidor y los agentes de OfficeScan**.

Aparecerá un mensaje.

5. Haga clic en **Comprobar versiones** para confirmar que ha actualizado todos los agentes a OfficeScan 11.0 SP1 o posterior.

6. Haga clic en **Aceptar**.

Contraseña de la consola Web

Solo se podrá acceder a la pantalla en la que se gestiona la contraseña de la consola Web (o la contraseña de la cuenta raíz que se crea en la instalación del servidor de OfficeScan) si el equipo servidor no cuenta con los recursos necesarios para poder utilizar Role-based Administration. Por ejemplo, si el equipo servidor funciona con Windows Server 2003 y no tiene instalado Authorization Manager Runtime, se puede acceder a la pantalla. Si los recursos son los adecuados, esta pantalla no aparecerá y la contraseña se podrá gestionar modificando la cuenta raíz desde la pantalla **Cuentas de usuario**.

Si OfficeScan no está registrado en Control Manager, póngase en contacto con su proveedor de asistencia para que le informe sobre cómo acceder a la consola Web.

Configuración de la Consola Web

Utilice la pantalla **Configuración de la Consola Web** para lo siguiente:

- Configure el servidor de OfficeScan para que actualice el panel Resumen de forma periódica. De forma predeterminada, el servidor actualiza el panel cada 30 segundos. El número de segundos debe ser superior a 10 e inferior a 300.

- Especifique la configuración del tiempo de espera de la consola Web. De forma predeterminada, un usuario se desconecta de forma automática de la consola Web pasados 30 minutos de inactividad. El número de minutos debe ser superior a 10 e inferior a 60.

Configurar las opciones de la consola Web

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Consola Web**.
2. Seleccione **Activar la actualización automática** y, a continuación, seleccione el intervalo de actualización.
3. Seleccione **Activar la desconexión automática de la consola Web** y, a continuación, seleccione el intervalo de tiempo de espera.
4. Haga clic en **Guardar**.

Administrador de cuarentena

Cuando el Agente de OfficeScan detecta un riesgo de seguridad y la acción de exploración se establece como Poner en cuarentena, este cifra el archivo infectado y lo mueve a la carpeta de cuarentena actual, la cual se encuentra en <*carpeta de instalación del agente*>\SUSPECT\Backup.

Tras mover el archivo al directorio de cuarentena local, el Agente de OfficeScan lo envía al directorio de cuarentena designado. Especifique el directorio en **Agentes** > **Administración de agentes > Configuración** > **Configuración de {tipo de exploración}** > **Acción (pestaña)**. Los archivos situados en el directorio de cuarentena designado se cifran para evitar que infecten otros archivos. Consulte el apartado *Directorio de cuarentena en la página 7-42* para obtener más información.

Si el directorio de cuarentena designado se encuentra en el equipo servidor de OfficeScan, modifique la configuración del directorio de cuarentena del servidor desde la consola Web. El servidor guarda los archivos en cuarentena en <*Carpeta de instalación del servidor*>\PCCSRV\Virus.

Nota

Si el Agente de OfficeScan no logra enviar el archivo cifrado al servidor de OfficeScan por el motivo que sea (un problema de conexión de red, por ejemplo), se guardará en la carpeta de cuarentena del Agente de OfficeScan. El Agente de OfficeScan intentará volver a enviar el archivo cuando se conecte al servidor de OfficeScan.

Configurar el directorio de cuarentena

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Administrador de cuarentena**.
2. Acepte o modifique la capacidad predeterminada de la carpeta de cuarentena y el tamaño máximo de un archivo infectado que OfficeScan puede almacenar en la carpeta de cuarentena.

   En la pantalla aparecen los valores predeterminados.
3. Haga clic en **Guardar la configuración de cuarentena**.
4. Para eliminar todos los archivos de la carpeta de cuarentena, haga clic en **Eliminar todos los archivos puestos en cuarentena**.

Server Tuner

Utilice Server Tuner para optimizar el rendimiento del servidor de OfficeScan mediante parámetros para los siguientes problemas de rendimiento relacionados con el servidor:

- **descargar**

  Cuando el número de Agentes de OfficeScan (incluidos los agentes de actualización) que requieren actualizaciones del servidor de OfficeScan supera los recursos disponibles del servidor, este pone en cola la solicitud de actualización del agente y procesa las solicitudes cuando los recursos están disponibles. Cuando el agente completa correctamente la actualización de sus componentes desde el servidor de OfficeScan, el cliente envía una notificación al servidor. Defina el

número máximo de minutos que esperará el servidor de OfficeScan para recibir una notificación de actualización del agente. Defina también el número máximo de intentos de notificación del servidor al agente para que realice una actualización y aplique los nuevos parámetros de configuración. El servidor sigue intentándolo solo si no recibe la notificación del agente.

- **Buffer**

  Cuando el servidor de OfficeScan recibe varias solicitudes de Agentes de OfficeScan como, por ejemplo, una solicitud para realizar una actualización, el servidor gestiona todas las solicitudes posibles y coloca en un búfer el resto de las solicitudes. El servidor administra a continuación las solicitudes guardadas en el búfer de una en una cuando dispone de los recursos necesarios. Especifique el tamaño del búfer para sucesos tales como solicitudes de actualizaciones de agente y para crear informes sobre los registros de agente.

- **Tráfico de red**

  La cantidad de tráfico de red varía a lo largo del día. Para controlar el flujo de tráfico de red que llega al servidor de OfficeScan y a otros orígenes de actualización, especifique el número de Agentes de OfficeScan que pueden actualizar simultáneamente los componentes en un momento determinado del día.

Server Tuner requiere el archivo siguiente: `SvrTune.exe`

Ejecutar Server Tuner

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a *carpeta de instalación del servidor*> `\PCCSRV\Admin\Utility\SvrTune`.
2. Haga doble clic en `SvrTune.exe` para iniciar Server Tuner.

   Se abrirá la consola de Server Tuner.
3. En **Download**, modifique los parámetros siguientes:

   - **Tiempo de espera para clientes**: escriba el número de minutos que esperará el servidor de OfficeScan para recibir una respuesta de actualización de los

agentes. Si el agente no responde durante este período, el servidor de OfficeScan no considera que los componentes del agente están actualizados. Cuando se excede el tiempo de espera de un agente notificado, se pasa a otro agente que espera la notificación.

- **Tiempo de espera para agentes de actualización**: escriba el número de minutos que esperará el servidor de OfficeScan para recibir una respuesta de actualización de un agente de actualización. Cuando se excede el tiempo de espera de un agente notificado, se pasa a otro agente que espera la notificación.
- **Número de reintentos**: escriba el número máximo de veces que el servidor de OfficeScan intentará notificar al agente para que realice una actualización o aplique los nuevos parámetros de configuración.
- **Intervalo de reintento**: escriba el número de minutos que esperará el servidor de OfficeScan entre cada intento de notificación.

4. En **Network Traffic**, modifique los parámetros siguientes:

   - **Horas normales**: haga clic en los botones de opción que representan las horas en las considera que el tráfico de red es normal.
   - **Horas de menor actividad**: haga clic en los botones de opción que representan las horas en las que considera que el tráfico de red es el más reducido.
   - **Horas de mayor actividad**: haga clic en los botones de opción que representan las horas en las considera que el tráfico de red es el más grande.
   - **Máximo de conexiones de cliente**: escriba el número máximo de clientes que pueden actualizar componentes de forma simultánea desde "otro origen de actualización" y desde el servidor de OfficeScan. Escriba un número máximo de clientes para cada uno de los períodos de tiempo. Cuando se alcanza el número máximo de conexiones, los Agentes de OfficeScan solo pueden actualizar componentes después de que se finalice la conexión actual del agente (cuando finaliza una actualización o cuando la respuesta de un agente alcanza el límite de tiempo de espera que ha especificado en los campos **Tiempo de espera para clientes** o **Tiempo de espera para agentes de actualización**).

5. Haga clic en **Aceptar**. Aparecerá un mensaje de solicitud para reiniciar el OfficeScan Master Service (OfficeScan Master Service).

Nota

Sólo se reinicia el servicio, no el equipo.

6. Seleccione una de las siguientes opciones de reinicio:
   - Haga clic en **Yes** para guardar la configuración de Server Tuner y reiniciar el servicio. La configuración surtirá efecto después de reiniciar.
   - Haga clic en **No** para guardar la configuración de Server Tuner pero no reiniciar el servicio. Reinicie el OfficeScan Master Service Master o reinicie el Equipo del servidor de OfficeScan para que la nueva configuración surta efecto.

Smart Feedback

Smart Feedback de Trend Micro comparte información anónima sobre amenazas con Smart Protection Network, lo que permite a Trend Micro identificar y combatir rápidamente las nuevas amenazas. Puede desactivar la función de comentarios inteligentes en cualquier momento desde esta consola.

Participar en el programa Smart Feedback

Procedimiento

1. Vaya a **Administración** > **Smart Protection** > **Smart Feedback**.
2. Haga clic en **Activar Smart Feedback de Trend Micro**
3. Para ayudar a Trend Micro a entender su organización, seleccione el tipo **Sector**.
4. Para enviar información sobre potenciales amenazas de seguridad para los archivos de los Agentes de OfficeScan, active la casilla de verificación **Activar evaluación de archivos de programa sospechosos**.

Nota

Los archivos enviados a Smart Feedback no contienen datos de los usuarios y se envían sólo para el análisis de amenazas.

5. Para configurar los criterios de envío de feedback, seleccione el número de detecciones para la cantidad de tiempo específica que provoca el feedback.
6. Especifique el ancho de banda máxima que OfficeScan puede utilizar cuando envía el feedback con el fin de reducir las interrupciones de la red.
7. Haga clic en **Guardar**.

Capítulo 15

Administración del agente de OfficeScan

En este capítulo se describen la administración y la configuración del Agente de OfficeScan.

Los temas que se incluyen son:

- *Ubicación del Endpoint en la página 15-2*
- *Administración del programa del agente de OfficeScan en la página 15-7*
- *Conexión agente-servidor en la página 15-28*
- *Configuración del proxy del agente de OfficeScan en la página 15-54*
- *Visualización de información sobre agentes de OfficeScan en la página 15-60*
- *Importación y exportación de la configuración de los agentes en la página 15-61*
- *Conformidad con las normas de seguridad en la página 15-62*
- *Compatibilidad con Trend Micro Virtual Desktop en la página 15-82*
- *Configuración global para los agentes en la página 15-97*
- *Configuración de derechos y otras configuraciones de los agentes en la página 15-99*

Ubicación del Endpoint

OfficeScan proporciona una función de conocimiento de ubicación que determina si la ubicación del Agente de OfficeScan es interna o externa. La función de conocimiento de ubicación se aprovecha en las siguientes funciones y servicios de OfficeScan:

TABLA 15-1. Funciones y servicios que aprovechan el conocimiento de ubicación

FUNCIÓN/ SERVICIO	DESCRIPCIÓN
Servicios de Reputación Web	La ubicación del Agente de OfficeScan determina la política de reputación Web que el Agente de OfficeScan aplicará. Los administradores suelen aplicar una política más estricta para los agentes externos. Para obtener información detallada acerca de las políticas de reputación Web, consulte *Políticas de reputación Web en la página 12-5*.
Servicios de File Reputation	Para los agentes que utilicen Smart Scan, la ubicación del Agente de OfficeScan determina el origen de Smart Protection al cual los agentes envían consultas de exploración. Los Agentes de OfficeScan externos envían consultas de exploración a la Smart Protection Network mientras que los agentes internos envían las consultas a los orígenes que se hayan definido en la lista de orígenes de Smart Protection. Para obtener información detallada acerca de las fuentes de Smart Protection, consulte *Fuentes de Smart Protection en la página 4-6*.
Prevención de pérdida de datos	La ubicación del Agente de OfficeScan determina la política de prevención de pérdida de datos que el agente aplicará. Los administradores suelen aplicar una política más estricta para los agentes externos. Para obtener información detallada acerca de las políticas de Prevención de pérdida de datos, consulte *Políticas de prevención de pérdida de datos en la página 11-3*.

FUNCIÓN/ SERVICIO	DESCRIPCIÓN
Control de dispositivos	La ubicación del Agente de OfficeScan determina la política de control de dispositivos que el agente aplicará. Los administradores suelen aplicar una política más estricta para los agentes externos. Para obtener información detallada acerca de las políticas de Control de dispositivos, consulte *Control de dispositivos en la página 10-2*.

Criterios de ubicación

Especifique si la ubicación se basa en la dirección IP del gateway del endpoint del Agente de OfficeScan, el estado de la conexión del Agente de OfficeScan con el servidor de OfficeScan o cualquier servidor de referencia.

- **Estado de conexión del agente**: si el Agente de OfficeScan puede conectarse al servidor de OfficeScan o a cualquiera de los servidores de referencia asignados en la intranet, la ubicación del endpoint será interna. Asimismo, si un endpoint ubicado fuera de la red de la empresa puede establecer conexión con el servidor de OfficeScan o algún servidor de referencia, su ubicación también será interna. Si ninguna de estas condiciones es aplicable, la ubicación del endpoint será externa.
- **Direcciones IP y MAC del gateway**: si la dirección IP del gateway del endpoint del Agente de OfficeScan coincide con las direcciones IP del gateway que se han especificado en la pantalla **Ubicación del Endpoint**, la ubicación del endpoint será interna. De lo contrario, la ubicación del endpoint será externa.

Definir la configuración de ubicación

Procedimiento

1. Vaya a **Agentes** > **Ubicación del Endpoint**.
2. Elija si la ubicación está basada en el **estado de la conexión del agente** o en la **dirección MAC e IP del gateway**.

3. Si selecciona **Estado de la conexión del agente**, decida si desea utilizar algún servidor de referencia.

   Consulte *Servidores de referencia en la página 14-36* para obtener más información.

   a. Si no especificó un servidor de referencia, el Agente de OfficeScan comprobará el estado de conexión con el servidor de OfficeScan cuando se produzcan los siguientes sucesos:

      - El Agente de OfficeScan cambia del modo independiente al normal (conectado o desconectado).
      - El Agente de OfficeScan cambia de un método de exploración a otro.

        Consulte *Tipos de métodos de exploración en la página 7-9* para obtener más información.

      - El Agente de OfficeScan detecta un cambio de dirección IP en el endpoint.
      - El Agente de OfficeScan se reinicia.
      - El servidor inicia la comprobación de la conexión.

        Consulte *Iconos del agente de OfficeScan en la página 15-28* para obtener más información.

      - El criterio de ubicación de la reputación Web cambia mientras se aplica la configuración global.
      - La política de prevención de epidemias ya no se aplica y se restaura la configuración previa a la epidemia.

   b. Si ha especificado un servidor de referencia, el Agente de OfficeScan comprobará el estado de conexión con el servidor de OfficeScan primero y, a continuación, con el servidor de referencia si la conexión con el servidor de OfficeScan no se ha realizado correctamente. El Agente de OfficeScan comprueba el estado de conexión cada hora y cuando se produce alguno de los sucesos mencionados anteriormente.

4. Si selecciona la **dirección MAC y la dirección IP del gateway**:

a. Escriba la dirección IPv4/IPv6 del gateway en el cuadro de texto.

b. Escriba la dirección MAC.

c. Haga clic en **Agregar**.

   Si no escribe la dirección MAC, OfficeScan incluirá todas las direcciones MAC pertenecientes a la dirección IP especificada.

d. Repita los pasos A a C hasta agregar todas las direcciones IP del gateway que desea.

e. Use la herramienta Gateway Settings Importer para importar una lista de valores de configuración del gateway.

   Consulte *Gateway Settings Importer en la página 15-5* para obtener más información.

5. Haga clic en **Guardar**.

Gateway Settings Importer

OfficeScan comprueba la ubicación de un endpoint para determinar la política de reputación Web que hay que utilizar y el origen de Smart Protection al que hay que conectarse. Una de las formas que tiene OfficeScan de identificar la ubicación es comprobar la dirección IP del gateway y la dirección MAC del endpoint.

Configure los ajustes del gateway en la pantalla **Ubicación del Endpoint** o utilice la herramienta Gateway Settings Importer para importar una lista de los valores de configuración del gateway en la pantalla **Ubicación del Endpoint**.

Usar Gateway Settings Importer

Procedimiento

1. Prepare un archivo de texto (`.txt`) que contenga la lista de valores de configuración del gateway. En cada línea, escriba una dirección IPv4 o IPv6 y, de forma opcional, una dirección MAC.

Separe las direcciones IP y las direcciones MAC con una coma. El número máximo de entradas es 4096.

Por ejemplo:

```
10.1.111.222,00:17:31:06:e6:e7

2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. En el equipo servidor, vaya a <*Carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\GatewaySettingsImporter`.

3. Haga clic con el botón derecho en `GSImporter.exe` y seleccione **Ejecutar como administrador**.

Nota

No puede ejecutar la herramienta Gateway Settings Importer desde Terminal Services.

---

4. En la pantalla **Gateway Settings Importer**, desplácese al archivo creado en el paso 1 y haga clic en **Importar**.

5. Haga clic en **Aceptar**.

   Se mostrará la configuración del gateway en la pantalla **Ubicación del Endpoint** y el servidor de OfficeScan implementará la configuración en los Agentes de OfficeScan.

6. Para eliminar todas las entradas, haga clic en **Borrar todo**.

   Si solo necesita eliminar una entrada determinada, quítela de la pantalla **Ubicación del Endpoint**.

7. Para exportar la configuración a un archivo, haga clic en **Exportar todo** y, a continuación, especifique el tipo y el nombre del archivo.

Administración del programa del agente de OfficeScan

En los temas siguientes se tratan formas de administrar y proteger el programa del Agente de OfficeScan:

- *Servicios del agente de OfficeScan en la página 15-7*
- *Reinicio del servicio Agente de OfficeScan en la página 15-12*
- *Autoprotección del agente de OfficeScan en la página 15-13*
- *Restricción de acceso del agente de OfficeScan en la página 15-18*
- *Descarga y desbloqueo del agente de OfficeScan en la página 15-19*
- *Derecho del modo independiente del Agente de OfficeScan en la página 15-20*
- *Agent Mover en la página 15-24*
- *Agentes de OfficeScan inactivos en la página 15-27*

Servicios del agente de OfficeScan

El Agente de OfficeScan ejecuta los servicios que se muestran en la siguiente tabla. Puede ver el estado de estos servicios en Microsoft Management Console.

TABLA 15-2. Servicios del agente de OfficeScan

SERVICIO	FUNCIONES CONTROLADAS
Servicio de prevención de cambios no autorizados de Trend Micro (`TMBMSRV.exe`)	• Supervisión del comportamiento • Control de dispositivos • Servicio de software seguro certificado
Cortafuegos de OfficeScan NT (`TmPfw.exe`)	Cortafuegos de OfficeScan

SERVICIO	FUNCIONES CONTROLADAS
Servicio de protección de datos de OfficeScan (`dsagent.exe`)	• Prevención de pérdida de datos • Control de dispositivos
OfficeScan NT Listener (`tmlisten.exe`)	Comunicación entre el Agente de OfficeScan y el servidor de OfficeScan
Servicio proxy de OfficeScan NT (`TmProxy.exe`)	• Reputación Web • POP3 mail scan
OfficeScan NT RealTime Scan (`ntrtscan.exe`)	• Exploración en tiempo real • Exploración programada • Exploración manual/Explorar ahora
OfficeScan Common Client Solution Framework (`TmCCSF.exe`)	Servicio de protección avanzada • Prevención de explotación en explorador • Exploración de memoria

Los siguientes servicios proporcionan una sólida protección, pero sus mecanismos de supervisión pueden forzar los recursos del sistema, sobre todo, en servidores que estén ejecutando aplicaciones de uso intensivo del sistema:

- Servicio de prevención de cambios no autorizados de Trend Micro (`TMBMSRV.exe`)
- Cortafuegos de OfficeScan NT (`TmPfw.exe`)
- Servicio de protección de datos de OfficeScan (`dsagent.exe`)

Por ello, estos servicios están desactivados de forma predeterminada en plataformas del servidor (Windows Server 2003, Windows Server 2008 y Windows Server 2012). Si desea activar estos servicios:

- Supervise el rendimiento del sistema de forma constante y realice la acción necesaria cuando perciba una caída de dicho rendimiento.
- Para `TMBMSRV.exe`, puede activar el servicio si excluye las aplicaciones de uso intensivo del sistema desde las políticas de supervisión del comportamiento. Puede

utilizar una herramienta de ajuste del rendimiento para identificar las aplicaciones de uso intensivo del sistema. Para conocer más detalles, consulte *Usar la Herramienta de ajuste del rendimiento de Trend Micro en la página 15-10*.

Para plataformas de escritorio, desactive los servicios solo si percibe una caída del rendimiento.

Activar o desactivar los servicios del agente desde la consola Web

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. Para Agentes de OfficeScan que ejecuten Windows XP, Vista 7, 8, 8.1 o 10:
   a. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.

      Nota

      Cuando seleccione el dominio raíz o dominios específicos, la configuración solo se aplicará a agentes que estén ejecutando plataformas de escritorio de Windows. La configuración no se aplicará a agentes que estén ejecutando plataformas de Windows Server aunque formen parte de los dominios.

   b. Haga clic en **Configuración** > **Configuración de servicios adicionales**.
   c. Active o desactive la casilla de verificación en las siguientes secciones:
      - **Servicio de prevención de cambios no autorizados**
      - **Servicio de cortafuegos**
      - **Servicio de conexión sospechosa**
      - **Servicio de protección de datos**
      - **Servicio de protección avanzada**

d. Haga clic en **Guardar** para aplicar la configuración a los dominios. En caso de que haya seleccionado el icono del dominio raíz, elija alguna de las siguientes opciones:

- **Aplicar a todos los agentes**: aplica la configuración a todos los agentes de escritorio de Windows existentes y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento de realizar la configuración.
- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes de escritorio de Windows que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

3. Para los Agentes de OfficeScan que ejecutan plataformas de Windows Server:

a. Seleccione un agente en el árbol de agentes.

b. Haga clic en **Configuración** > **Configuración de servicios adicionales**.

c. Active o desactive la casilla de verificación en las siguientes secciones:

- **Servicio de prevención de cambios no autorizados**
- **Servicio de cortafuegos**
- **Servicio de conexión sospechosa**
- **Servicio de protección de datos**
- **Servicio de protección avanzada**

d. Haga clic en **Guardar**.

Usar la Herramienta de ajuste del rendimiento de Trend Micro

Procedimiento

1. Descargue la Herramienta de ajuste del rendimiento de Trend Micro desde:

http://esupport.trendmicro.com/solution/en-us/1056425.aspx

2. Descomprima `TMPerfTool.zip` para extraer `TMPerfTool.exe`.

3. Coloque `TMPerfTool.exe` en <*carpeta de instalación del agente*> o en la misma carpeta como `TMBMCLI.dll`.

4. Haga clic con el botón derecho en `TMPerfTool.exe` y seleccione **Ejecutar como administrador**.

5. Lea y acepte el contrato de licencia de usuario final y, después, haga clic en **Aceptar**.

6. Haga clic en **Analizar**.

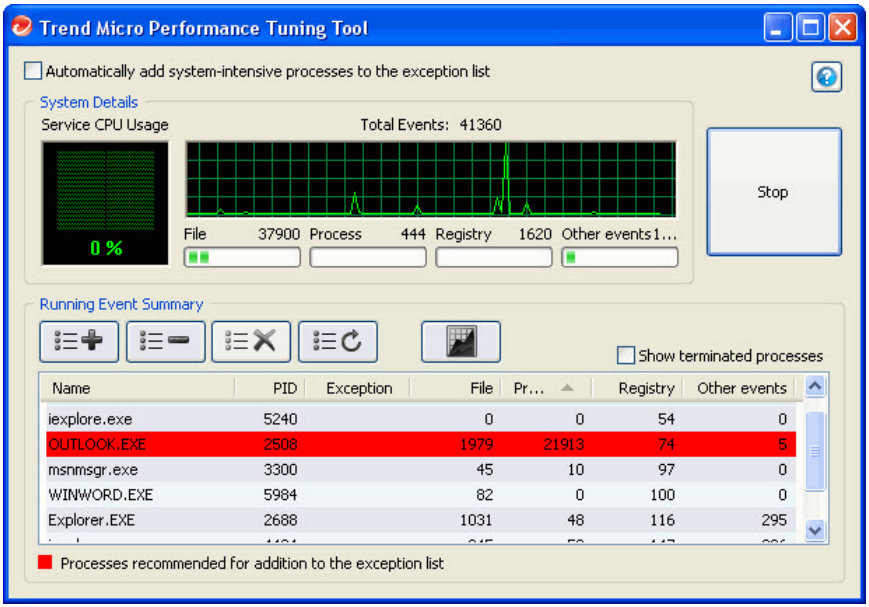


FIGURA 15-1. Procesos de uso intensivo del sistema resaltados

La herramienta comenzará a supervisar el uso de la CPU y la carga de sucesos. Un proceso de uso intensivo del sistema se resalta en rojo.

7. Seleccione un proceso de uso intensivo del sistema y haga clic en el botón **Añadir a la lista de excepciones (permitir)** ( ).
8. Compruebe que haya una mejora en el rendimiento del sistema o de la aplicación.
9. Si se produce dicha mejora, seleccione el proceso de nuevo y haga clic en el botón **Eliminar de la lista de excepciones** ( ).
10. Si el rendimiento cae de nuevo, siga los pasos siguientes:
    a. Apunte el nombre de la aplicación.
    b. Haga clic en **Detener**.
    c. Haga clic en el botón **Generar informe** ( ) y, a continuación, guarde el archivo `.xml`.
    d. Revise las aplicaciones que se hayan identificado como conflictivas y añádalas a la lista de excepciones de Supervisión del comportamiento.

       Para conocer más detalles, consulte *Lista de excepción de supervisión del comportamiento en la página 9-10*.

Reinicio del servicio Agente de OfficeScan

OfficeScan reinicia los servicios del Agente de OfficeScan que han dejado de responder de forma inesperada y que no se han detenido mediante un proceso normal del sistema. Para obtener más información sobre los servicios del agente, consulte *Servicios del agente de OfficeScan en la página 15-7*.

Defina la configuración necesaria para activar el reinicio de los servicios del Agente de OfficeScan.

Definir la configuración de reinicio del sistema

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.

2. Haga clic en la pestaña **Sistema**.
3. Desplácese a la sección **Reinicio de los servicios**.
4. Seleccione **Reiniciar automáticamente un servicio del agente de OfficeScan si el servicio termina de forma inesperada**.
5. Configure la siguiente información:
   - **Reiniciar el servicio después de __ minutos**: especifique el tiempo (en minutos) que debe transcurrir antes de que OfficeScan reinicie un servicio.
   - **Si da error el primer intento de reinicio del servicio, reintentar __ veces**: Especifique el número máximo de reintentos para reiniciar un servicio. Reinicie el servicio manualmente en caso de que siga detenido después de haber probado con el número máximo de intentos.
   - **Restablecer el recuento de errores de reinicio después de _ hora(s)**: si un servicio sigue detenido después de haber agotado el número máximo de intentos, OfficeScan espera un número determinado horas para restablecer el recuento del error. Si un servicio sigue detenido después de que hayan transcurrido las horas establecidas, OfficeScan reinicia el servicio.

Autoprotección del agente de OfficeScan

La función Autoprotección del Agente de OfficeScan ofrece formas para que el Agente de OfficeScan proteja los procesos y otros recursos necesarios para contar con un funcionamiento adecuado. Esta función ayuda a impedir que los programas o los usuarios reales intenten desactivar la protección antimalware.

La función de autoprotección del Agente de OfficeScan proporciona las siguientes opciones:

- *Protección de los servicios del agente de OfficeScan en la página 15-15*
- *Protección de archivos de la carpeta de instalación del agente de OfficeScan en la página 15-15*
- *Proteger las claves de registro del agente de OfficeScan en la página 15-17*
- *Protección de procesos del agente de OfficeScan en la página 15-17*

Configuración de la autoprotección del agente de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Autoprotección del agente de OfficeScan**.
5. Active las siguientes opciones:
   - *Protección de los servicios del agente de OfficeScan en la página 15-15*
   - *Protección de archivos de la carpeta de instalación del agente de OfficeScan en la página 15-15*
   - *Proteger las claves de registro del agente de OfficeScan en la página 15-17*
   - *Protección de procesos del agente de OfficeScan en la página 15-17*
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Protección de los servicios del agente de OfficeScan

OfficeScan bloquea todos los intentos destinados a finalizar los siguientes servicios del Agente de OfficeScan:

- OfficeScan NT Listener (`TmListen.exe`)
- OfficeScan NT RealTime Scan (`NTRtScan.exe`)
- OfficeScan NT Proxy Service (`TmProxy.exe`)
- OfficeScan NT Firewall (`TmPfw.exe`)
- OfficeScan Data Protection Service (`dsagent.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

Nota

Si esta opción está activada, OfficeScan puede impedir que se instalen correctamente productos de terceros en Endpoints. Si se produce este problema, puede desactivar esta opción de forma temporal y volver a activarla después de haber instalado el producto de terceros.

- Marco de soluciones del cliente habitual de Trend Micro (`TmCCSF.exe`)

Protección de archivos de la carpeta de instalación del agente de OfficeScan

Para impedir que otros programas o los usuarios modifiquen o eliminen los archivos del Agente de OfficeScan, OfficeScan ofrece varias características de protección mejoradas.

Tras habilitar **Proteger archivos de la carpeta de instalación del agente de OfficeScan**, OfficeScan bloquea los siguientes archivos en la carpeta raíz <*Carpeta de instalación del agente*>:

- Todos los archivos firmados digitalmente con extensiones `.exe`, `.dll` y `.sys`
- Existen algunos archivos sin firmas digitales, entre los que se incluyen:

- `bspatch.exe`
- `bzip2.exe`
- `INETWH32.dll`
- `libcurl.dll`
- `libeay32.dll`
- `libMsgUtilExt.mt.dll`
- `msvcm80.dll`
- `MSVCP60.DLL`
- `msvcp80.dll`
- `msvcr80.dll`
- `OfceSCV.dll`
- `OFCESCVPack.exe`
- `patchbld.dll`
- `patchw32.dll`
- `patchw64.dll`
- `PiReg.exe`
- `ssleay32.dll`
- `Tmeng.dll`
- `TMNotify.dll`
- `zlibwapi.dll`

Tras habilitar **Proteger archivos de la carpeta de instalación del agente de OfficeScan** y la Exploración en tiempo real de amenazas de virus/malware, OfficeScan realiza las siguientes acciones:

- Comprobación de la integridad de los archivos antes de ejecutar archivos `.exe` en la carpeta de instalación

  Durante las actualizaciones de ActiveUpdate, OfficeScan comprueba que el emisor del archivo que activa la actualización es Trend Micro. Si el emisor no se reconoce como Trend Micro y ActiveUpdate no puede reemplazar el archivo incorrecto, OfficeScan registra el incidente en los registros de sucesos de Windows y bloquea la actualización.

- Prevención del secuestro de la DLL

  Algunos autores de malware copian los archivos de biblioteca de vínculos dinámicos en la carpeta de instalación del Agente de OfficeScan o de la carpeta de supervisión del comportamiento para cargarlos antes de que el agente cargue. Estos archivos intentan interrumpir la protección que ofrece OfficeScan. Para evitar que se copien archivos secuestrados en las carpetas del Agente de OfficeScan, OfficeScan no permite que se copien archivos en la carpeta de instalación ni en la carpeta de supervisión del comportamiento.

- Prevención del bloqueo de archivos mediante la configuración «SHARE:NONE» de Windows

Proteger las claves de registro del agente de OfficeScan

OfficeScan bloquea todos los intentos destinados a modificar, eliminar o añadir nuevas entradas en las siguientes claves y subclaves de registro:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Protección de procesos del agente de OfficeScan

OfficeScan bloquea todos los intentos destinados a finalizar los procesos de la siguiente tabla.

Proceso	Descripción
`TmListen.exe`	Recibe comandos y notificaciones del servidor de OfficeScan y facilita la comunicación entre el Agente de OfficeScan y el servidor.
`NTRtScan.exe`	Ejecuta exploraciones en tiempo real, programadas y manuales en los Agentes de OfficeScan.
`TmProxy.exe`	Explora el tráfico de red antes de que llegue a la aplicación de destino.
`TmPfw.exe`	ofrece un cortafuegos para paquetes, exploración de virus de red y detección de intrusiones.
`TMBMSRV.exe`	regula el acceso a dispositivos externos de almacenamiento e impide los cambios no autorizados de los procesos y claves de registro

PROCESO	DESCRIPCIÓN
`DSAgent.exe`	supervisa la transmisión de datos confidenciales y controla el acceso a los dispositivos
`PccNTMon.exe`	Este proceso es el responsable de iniciar la consola del Agente de OfficeScan
`TmCCSF.exe`	lleva a cabo la prevención de explotación del explorador y exploraciones de memoria.

OfficeScan también puede ofrecer protección contra la inclusión de procesos en las políticas de restricción de software (SRP) de Microsoft. Las políticas de restricción de software impiden que las aplicaciones que contiene se ejecuten en el endpoint. Para impedir que se incluyan procesos de OfficeScan en la lista de políticas de restricción de software:

1. Active **Proteger los procesos del agente de OfficeScan**.
2. Active el **servicio de prevención de cambios no autorizados**.

   Para conocer más detalles, consulte *Activar o desactivar los servicios del agente desde la consola Web en la página 15-9*.

Restricción de acceso del agente de OfficeScan

Esta configuración desactiva el acceso a la consola del Agente de OfficeScan desde la bandeja del sistema o el menú Inicio de Windows. Los usuarios solo pueden acceder a la consola del Agente de OfficeScan si hacen doble clic en `PccNTMon.exe` en la <*Carpeta de instalación del agente*>. Tras definir esta configuración, vuelva a cargar el Agente de OfficeScan para aplicarla.

Este valor de configuración no desactiva el Agente de OfficeScan. El Agente de OfficeScan se ejecuta en segundo plano y sigue ofreciendo protección frente a los riesgos de seguridad.

Restricción del acceso a la consola del agente de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. Haga clic en la pestaña **Otras configuraciones** y vaya a la sección **Restricción de acceso del agente de OfficeScan**.
5. Seleccione **Impedir el acceso de los usuarios a la consola del agente de OfficeScan desde la bandeja del sistema o el menú Inicio de Windows**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Descarga y desbloqueo del agente de OfficeScan

El derecho de descarga y desbloqueo del Agente de OfficeScan permite a los usuarios detener el Agente de OfficeScan de manera temporal o acceder a las funciones avanzadas de la consola Web con o sin contraseña.

Concesión del derecho de descarga y desbloqueo al agente

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Descarga y desbloqueo**.
5. Para permitir que el Agente de OfficeScan descargue sin contraseña, seleccione **No necesita una contraseña**.
   - Si se necesita una contraseña, seleccione **Necesita una contraseña**, introdúzcala y, a continuación, confírmela.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Derecho del modo independiente del Agente de OfficeScan

Otorgue a ciertos usuarios el derecho del modo independiente del Agente de OfficeScan si los sucesos de agente-servidor están interfiriendo en las tareas de los usuarios. Por ejemplo, un usuario que hace presentaciones con frecuencia puede activar el modo independiente antes de comenzar una presentación para evitar que el servidor de

OfficeScan implemente la configuración del Agente de OfficeScan e inicie exploraciones en el Agente de OfficeScan.

Cuando los Agentes de OfficeScan están en el modo independiente:

- Aunque exista una conexión operativa entre el servidor y los Agentes de OfficeScan, estos últimos no envían registros al servidor de OfficeScan.
- Aunque exista una conexión operativa entre el servidor y los agentes, el servidor de OfficeScan no inicia tareas ni implementa la configuración del Agente de OfficeScan en los agentes.
- Los Agentes de OfficeScan actualizan los componentes si no pueden conectarse a ninguno de sus orígenes de actualización. Las fuentes incluyen el servidor de OfficeScan, los agentes de actualización o una fuente de actualización personalizada.

  Los siguientes sucesos dan lugar a una actualización en los agentes independientes:

  - El usuario lleva a cabo una actualización manual.
  - Se ejecuta una actualización manual del agente. Puede desactivar la actualización automática del agente en los agentes independientes.

    Para conocer más detalles, consulte *Desactivación de la actualización automática de agentes para los agentes independientes en la página 15-22*.
  - Se ejecuta la actualización programada. Solo los agentes con los derechos necesarios pueden ejecutar actualizaciones programadas. Puede revocar este derecho en cualquier momento.

    Para conocer más detalles, consulte *Revocación del derecho de actualización programada en los agentes independientes en la página 15-23*.

Concesión del derecho de modo independiente del Agente

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Modo independiente**.
5. Seleccione **Activar modo independiente**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:
   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Desactivación de la actualización automática de agentes para los agentes independientes

Procedimiento

1. Vaya a **Actualizaciones** > **Agentes** > **Actualización automática**.
2. Vaya a la sección **Actualización activada por suceso**.
3. Desactive **Incluir agentes independientes y sin conexión**.

Nota

Esta opción se desactiva de forma automática si desactiva **Iniciar la actualización de los componentes en los agentes inmediatamente después de que el servidor de OfficeScan descargue un componente nuevo**.

Revocación del derecho de actualización programada en los agentes independientes

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz o seleccione dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Actualizaciones de los componentes**.
5. Desactive la opción **Activar/Desactivar la actualización programada**.
6. Haga clic en **Guardar**.

Configuración de idioma del agente de OfficeScan

Puede configurar todos los Agentes de OfficeScan de manera que utilicen la configuración de idioma del servidor de OfficeScan o la configuración de idioma del usuario local actual. Tras instalar o actualizar el programa del Agente de OfficeScan, el agente aplica la configuración de idioma en la pantalla **Configuración global**

De manera predeterminada, si el Agente de OfficeScan no es compatible con la configuración de idioma del usuario actual, la configuración de idioma establece el idioma del servidor de OfficeScan y, luego, utiliza el inglés.

Configuración de idioma del agente de OfficeScan

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Control de agentes**.

3. Vaya a la sección **Configuración de idioma de agente**.
4. Especifique cómo aplica la configuración de idioma el Agente de OfficeScan:
   - **Configuración de idioma local en el endpoint**: El Agente de OfficeScan se muestra con la configuración de idioma del usuario que ha iniciado sesión.

     Nota

     Si el Agente de OfficeScan no es compatible con la configuración de idioma del usuario que ha iniciado sesión, aplicará el idioma del servidor de OfficeScan. Si el endpoint no es compatible con el idioma del servidor de OfficeScan, se mostrará en inglés.

   - **Idioma del servidor de OfficeScan**: El Agente de OfficeScan se muestra con el idioma del servidor de OfficeScan.

     Nota

     Si el endpoint no es compatible con el idioma del servidor de OfficeScan, se mostrará en inglés.
5. Haga clic en **Guardar**.

Agent Mover

Si tiene más de un servidor de OfficeScan en la red, utilice la herramienta Agent Mover para transferir los Agentes de OfficeScan de un servidor de OfficeScan a otro. Resulta especialmente útil tras añadir un servidor de OfficeScan nuevo a la red y cuando se desean transferir los Agentes de OfficeScan existentes a un servidor nuevo.

Nota

Ambos servidores deben ser de la misma versión de idioma. Si utiliza Agent Mover para transferir cualquier Agente de OfficeScan en el que se ejecute una versión anterior a un servidor de la versión actual, el Agente de OfficeScan se actualizará automáticamente.

Asegúrese de que la cuenta que utiliza dispone de derechos de administrador antes de utilizar esta herramienta.

Ejecución de Agent Mover

Procedimiento

1. En el servidor de OfficeScan, vaya a <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Copie `IpXfer.exe` en el endpoint del Agente de OfficeScan. En caso de que el endpoint del Agente de OfficeScan ejecute una plataforma del tipo x64, copie `IpXfer_x64.exe` en su lugar.
3. En el endpoint del Agente de OfficeScan, abra el símbolo del sistema y vaya a la carpeta en la que ha copiado el archivo ejecutable.
4. Ejecute Agent Mover con la siguiente sintaxis:

```
<nombre del archivo ejecutable> -s <nombre del servidor> -p
<puerto de escucha del servidor> -c <puerto de escucha del
agente> -d <dominio o jerarquía de dominio> -e <ubicación
del certificado y nombre de archivo> -pwd <contraseña del
derecho de descarga y desbloqueo del agente>
```

TABLA 15-3. Parámetros de Agent Mover

PARÁMETRO	EXPLICACIÓN
`<nombre del archivo ejecutable>`	`IpXfer.exe` o `IpXfer_x64.exe`
`-s <nombre del servidor>`	El nombre del servidor de OfficeScan de destino (el servidor al que el Agente de OfficeScan realizará transferencias).
`-p <puerto de escucha del servidor>`	El puerto de escucha (o puerto de confianza) del servidor de OfficeScan de destino. Para ver el puerto de escucha en la consola Web de OfficeScan, en el menú principal, haga clic en **Administración** > **Configuración** > **Conexión del agente**.
`-c <puerto de escucha del agente>`	El número de puerto utilizado por el endpoint del Agente de OfficeScan para comunicarse con el servidor.

PARÁMETRO	EXPLICACIÓN
`-d <dominio o jerarquía de dominio>`	El dominio o el subdominio del árbol de agentes en el cual se agrupará el agente. La jerarquía de dominio debe indicar el subdominio.
`-e <ubicación del certificado y nombre de archivo>`	Importa un nuevo certificado de autenticación del Agente de OfficeScan durante el proceso de movimiento. Si no se utiliza este parámetro, el Agente de OfficeScan recupera automáticamente el certificado de autenticación actual de su nuevo servidor de administración. **Nota** La ubicación predeterminado del certificado en el servidor de OfficeScan es: <*carpeta de instalación del servidor*>`\PCCSRV\Pccnt\Common\OfcNTCer.dat`. Al utilizar un certificado de un origen distinto de OfficeScan, asegúrese de que el certificado esté en el formato DER (Distinguished Encoding Rules).
`-pwd <contraseña del derecho de descarga y desbloqueo del agente>`	La contraseña del derecho de descarga y desbloqueo configurada en Derechos y otras configuraciones. **Nota** Si la contraseña del derecho de descarga y desbloqueo es necesaria, pero no la proporciona, Agent Mover se la pedirá antes de mover los agentes.

Ejemplos:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -pwd
unlock
```

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01 -pwd unlock
```

5. Para confirmar que el Agente de OfficeScan se comunica ahora con otro servidor, lleve a cabo las siguientes acciones:

   a. En el endpoint del Agente de OfficeScan, haga clic con el botón derecho en el icono del programa del Agente de OfficeScan que aparece en la bandeja del sistema.

   b. Seleccione **Versiones de los componentes**.

   c. Compruebe el servidor de OfficeScan al que informa el Agente de OfficeScan en el campo **Nombre del servidor/Puerto**.

   Nota

   Si el Agente de OfficeScan no aparece en el árbol de agentes del nuevo servidor de OfficeScan que lo gestiona, reinicie el servicio maestro del nuevo servidor (`ofservice.exe`).

Agentes de OfficeScan inactivos

Cuando se utiliza el programa de desinstalación del Agente de OfficeScan para eliminar el programa del Agente de OfficeScan de endpoints, el programa envía una notificación automáticamente al servidor. Cuando el servidor recibe esta notificación, elimina el icono del Agente de OfficeScan del árbol de agentes para indicar que el agente ya no existe.

Sin embargo, si el Agente de OfficeScan se elimina mediante otros métodos, como reformatear el disco duro del endpoint o borrar los archivos del Agente de OfficeScan manualmente, OfficeScan no se percata de la eliminación y muestra el Agente de OfficeScan como inactivo. Si un usuario descarga o desactiva el Agente de OfficeScan durante un periodo largo de tiempo, el servidor mostrará también el Agente de OfficeScan como inactivo.

Para asegurarse de que el árbol de agentes muestre solo los agentes activos, configure OfficeScan para que elimine automáticamente los agentes inactivos del árbol de agentes.

Eliminación automática de agentes inactivos

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Agentes inactivos**.
2. Seleccione **Activar eliminación automática de agentes inactivos**.
3. Seleccione el número de días que deben transcurrir antes de que OfficeScan considere que el Agente de OfficeScan está inactivo.
4. Haga clic en **Guardar**.

Conexión agente-servidor

El Agente de OfficeScan debe mantener una conexión continua con el servidor principal para poder actualizar componentes, recibir notificaciones y aplicar cambios en la configuración en el momento apropiado. En los siguientes temas se trata el modo de comprobar el estado de conexión del Agente de OfficeScan y de resolver problemas con la misma:

- *Direcciones IP del agente en la página 5-12*
- *Iconos del agente de OfficeScan en la página 15-28*
- *Comprobación de la conexión agente-servidor en la página 15-47*
- *Registros de comprobación de la conexión en la página 15-48*
- *Agentes no accesibles en la página 15-49*

Iconos del agente de OfficeScan

El icono del Agente de OfficeScan ubicado en la bandeja del sistema ofrece señales visuales que indican el estado actual del Agente de OfficeScan y solicitan a los usuarios que lleven a cabo determinadas acciones. En todo momento, el icono mostrará una combinación de las siguientes señales visuales.

TABLA 15-4. Estado del Agente de OfficeScan según se indica en el icono del Agente de OfficeScan

ESTADO DEL AGENTE	DESCRIPCIÓN	SEÑAL VISUAL
Conexión del agente con el servidor de OfficeScan	Los agentes en línea están conectados con el servidor de OfficeScan. El servidor puede iniciar tareas e implementar configuraciones en esos agentes.	El icono contiene un símbolo que se asemeja a un corazón latiendo. El color de fondo es de un tono azul o rojo en función del estado del servicio de exploración en tiempo real.
	Los agentes sin conexión no están conectados con el servidor de OfficeScan. El servidor no puede administrar estos agentes.	El icono contiene un símbolo que se asemeja a un corazón que no late. El color de fondo es de un tono azul o rojo en función del estado del servicio de exploración en tiempo real. El agente puede desconectarse, aunque se encuentre conectado a la red. Para obtener información detallada sobre este problema, consulte *Soluciones a los problemas que se indican en los iconos del agente de OfficeScan en la página 15-44*.
	Los agentes independientes pueden comunicarse o no con el servidor de OfficeScan.	El icono contiene los símbolos del escritorio y la señal. El color de fondo es de un tono azul o rojo en función del estado del servicio de exploración en tiempo real. Si desea obtener información detallada acerca de los agentes en modo independiente, consulte *Derecho del modo independiente del Agente de OfficeScan en la página 15-20*.

Estado del agente	Descripción	Señal visual
Disponibilidad de las fuentes de Smart Protection	Las fuentes de Smart Protection incluyen los Smart Protection Servers y la Red de Smart Protection de Trend Micro. Los agentes de exploración convencional se conectan a las fuentes de Smart Protection para realizar consultas de reputación Web. Los agentes de Smart Scan se conectan a las fuentes de Smart Protection para realizar consultas de exploración y de reputación Web.	El icono incluye una marca de verificación si hay alguna fuente de Smart Protection disponible.
		El icono incluye una barra de progreso si no hay ninguna fuente de Smart Protection disponible y el agente intenta establecer conexión con las fuentes. Para obtener información detallada sobre este problema, consulte *Soluciones a los problemas que se indican en los iconos del agente de OfficeScan en la página 15-44*.
		Para los agentes de exploración convencionales no aparece ninguna marca de verificación o barra de progreso si se ha desactivado la reputación Web en el agente.

Estado del agente	Descripción	Señal visual
Estado del servicio de exploración en tiempo real	OfficeScan utiliza el servicio de exploración en tiempo real para llevar a cabo tanto la exploración en tiempo real como la exploración manual y programada. El servicio debe funcionar o el agente quedará vulnerable a los riesgos de seguridad.	Todo el icono aparecerá en un tono azul si el servicio de exploración en tiempo real se encuentra operativo. Para indicar el método de exploración del agente, se utilizan dos tonos de azul. • Para la exploración convencional: • Para smart scan:
		Todo el icono aparecerá en un tono rojo si el servicio de exploración en tiempo real se ha desactivado o no se encuentra operativo. Para indicar el método de exploración del agente, se utilizan dos tonos de rojo. • Para la exploración convencional: • Para smart scan: Para obtener información detallada sobre este problema, consulte *Soluciones a los problemas que se indican en los iconos del agente de OfficeScan en la página 15-44*.

Estado del agente	Descripción	Señal visual
Estado de la exploración en tiempo real	La exploración en tiempo real proporciona protección proactiva mediante la exploración de archivos en busca de riesgos de seguridad cuando se crean, modifican o recuperan.	No existen señales visuales que indiquen si la exploración en tiempo real se encuentra activada.
		Todo el icono se encuentra rodeado por un círculo rojo y presenta una línea roja diagonal si la exploración en tiempo real se encuentra desactivada. Para obtener información detallada sobre este problema, consulte *Soluciones a los problemas que se indican en los iconos del agente de OfficeScan en la página 15-44*.
Estado de actualización del patrón	Los agentes deben actualizar el patrón de forma regular para proteger el agente de las amenazas más recientes.	No existen señales visuales que indiquen si el patrón se encuentra actualizado o ligeramente desactualizado.
		El icono muestra un signo de exclamación si el patrón se encuentra muy desactualizado. Esto quiere decir que el patrón no se ha actualizado en mucho tiempo. Para obtener más información sobre la actualización de los agentes, consulte *Actualizaciones del agente de OfficeScan en la página 6-30*.

Estado del agente	Descripción	Señal visual
Estado de la licencia de prueba para servidores de OfficeScan	Los agentes en línea están conectados con un servidor de OfficeScan que está usando una licencia de prueba caducada.	Este icono indica que la licencia de prueba del servidor de OfficeScan está caducada.

Iconos de smart scan

Cuando los Agentes de OfficeScan utilizan Smart Scan, se muestra uno de los siguientes iconos.

Tabla 15-5. Iconos de smart scan

Icono	Conexión con el servidor de OfficeScan	Disponibilidad de las fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real
	Conectado	Disponible	Funcional	Activada
	Conectado	Disponible	Funcional	Desactivada
	Conectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado

Icono	Conexión con el servidor de OfficeScan	Disponibilidad de las fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real
	Conectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional
	Desconectado	Disponible	Funcional	Activada
	Desconectado	Disponible	Funcional	Desactivado
	Desconectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado
	Desconectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional
	Independiente	Disponible	Funcional	Activada
	Independiente	Disponible	Funcional	Desactivado
	Independiente	Disponible	Desactivado o no es funcional	Desactivado o no es funcional
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Activada

Icono	Conexión con el servidor de OfficeScan	Disponibilidad de las fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado
	Independiente	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional

Iconos de la exploración convencional

Cuando los Agentes de OfficeScan realizan una exploración convencional, aparece alguno de los siguientes iconos.

Tabla 15-6. Iconos de la exploración convencional

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Conectado	Disponible	Funcional	Activada	Actualizado o ligeramente desactualizado
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Actualizado o ligeramente desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Conectado	Disponible	Funcional	Activada	Muy desactualizado
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Muy desactualizado
	Conectado	Disponible	Funcional	Desactivada	Actualizado o ligeramente desactualizado
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Conectado	Disponible	Funcional	Desactivado	Muy desactualizado
	Conectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Muy desactualizado
	Conectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Conectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Conectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado
	Conectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado
	Desconectado	Disponible	Funcional	Activada	Actualizado o ligeramente desactualizado
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Actualizado o ligeramente desactualizado
	Desconectado	Disponible	Funcional	Activada	Muy desactualizado
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Muy desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Desconectado	Disponible	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Desconectado	Disponible	Funcional	Desactivado	Muy desactualizado
	Desconectado	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Muy desactualizado
	Desconectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Desconectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Desconectado	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Desconectado	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado
	Independiente	Disponible	Funcional	Activada	Actualizado o ligeramente desactualizado
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Actualizado o ligeramente desactualizado
	Independiente	Disponible	Funcional	Activada	Muy desactualizado
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Activada	Muy desactualizado
	Independiente	Disponible	Funcional	Desactivado	Actualizado o ligeramente desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Independiente	Disponible	Funcional	Desactivado	Muy desactualizado
	Independiente	No disponible, volviendo a conectar a fuentes	Funcional	Desactivado	Muy desactualizado
	Independiente	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Independiente	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Independiente	Disponible	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado
	Independiente	No disponible, volviendo a conectar a fuentes	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Actualizado o ligeramente desactualizado
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Muy desactualizado
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Muy desactualizado
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Conectado	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Actualizado o ligeramente desactualizado
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Muy desactualizado
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Muy desactualizado
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Desconectado	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado

Icono	Conexión con el servidor de OfficeScan	Servicios de reputación Web que proporcionan las Fuentes de Smart Protection	Servicio de exploración en tiempo real	Exploración en tiempo real	Patrón de virus
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Actualizado o ligeramente desactualizado
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Activada	Muy desactualizado
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Actualizado o ligeramente desactualizado
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Funcional	Desactivado	Muy desactualizado
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Actualizado o ligeramente desactualizado
	Independiente	No aplicable (función de reputación Web desactivada en el agente)	Desactivado o no es funcional	Desactivado o no es funcional	Muy desactualizado

Soluciones a los problemas que se indican en los iconos del agente de OfficeScan

Lleve a cabo las acciones necesarias si el icono del Agente de OfficeScan indica cualquiera de las condiciones siguientes:

Condición	Descripción
El archivo de patrones no se ha actualizado durante un tiempo	Los usuarios del Agente de OfficeScan deben actualizar los componentes. En la consola Web, configure las opciones de actualización de componentes en **Actualizaciones** > **Agentes** > **Actualización automática** o conceda derechos de actualización a los usuarios en **Agentes** > **Administración de agentes > Configuración** > **Derechos y otras configuraciones** > **Derechos (pestaña)** > **Actualizaciones de los componentes**.
El servicio de exploración en tiempo real se ha desactivado o no se encuentra operativo	Si el servicio de exploración en tiempo real (OfficeScan NT RealTime Scan) se ha desactivado o no se encuentra operativo, los usuarios deben iniciar el servicio manualmente desde la consola de administración de Microsoft.
Se ha desactivado la exploración en tiempo real	Active la exploración en tiempo real en la consola Web (**Agentes** > **Administración de agentes > Configuración** > **Configuración de la exploración** > **Configuración de la exploración en tiempo real**).
Se ha desactivado la exploración en tiempo real y el Agente de OfficeScan se encuentra en modo independiente	Los usuarios deben desactivar el modo independiente en primer lugar. Tras desactivar el modo independiente, active la exploración en tiempo real en la consola Web.
El Agente de OfficeScan está conectado a la red, pero aparece desconectado	Compruebe la conexión en la consola Web (**Agentes** > **Comprobación de la conexión**) y, a continuación, compruebe los registros de comprobación de la conexión (**Registros** > **Agentes** > **Registros de comprobación de la conexión**). En caso de que el Agente de OfficeScan continúe desconectado tras la comprobación:

Condición	Descripción
	1. Si tanto el servidor como el Agente de OfficeScan no tienen conexión, compruebe la conexión de red. 2. Si el Agente de OfficeScan está desconectado, pero está conectado en el servidor, es posible que el nombre de dominio del servidor se haya cambiado y que el Agente de OfficeScan se conecte con el servidor con el nombre del dominio (si ha seleccionado el nombre del dominio durante la instalación del servidor). Registre el nombre del dominio del servidor de OfficeScan en el servidor DNS o WINS, o bien agregue el nombre del dominio y la información IP al archivo "hosts" de la siguiente carpeta del endpoint del agente: `<carpeta de Windows>\system32\drivers\etc`. 3. Si el Agente de OfficeScan está conectado, pero está desconectado en el servidor, compruebe la configuración del cortafuegos de OfficeScan. El cortafuegos puede bloquear la comunicación de servidor a agente pero permitir la comunicación de agente a servidor. 4. Si el Agente de OfficeScan está conectado, pero está desconectado en el servidor, es posible que se haya cambiado la dirección IP del Agente de OfficeScan, pero que su estado no se refleje en el servidor (p. ej., cuando se vuelve a cargar el agente). Intente volver a implementar el Agente de OfficeScan.
Las fuentes de Smart Protection no están disponibles	Efectúe estas tareas si un agente pierde la conexión con las fuentes de Smart Protection: 1. En la consola Web, vaya a la pantalla **Ubicación del Endpoint** (**Agentes** > **Ubicación del Endpoint**) y compruebe que se ha definido correctamente la siguiente configuración del endpoint: • Números de puerto y servidores de referencia • Direcciones IP del gateway 2. En la consola Web, vaya a la pantalla Fuente de Smart Protection (**Administración** > **Smart Protection** > **Fuentes de Protección Inteligente**) y, a continuación, realice las siguientes tareas:

CONDICIÓN	DESCRIPCIÓN
	a. Compruebe que la configuración del Smart Protection Server de la lista estándar o personalizada de fuentes sea correcta. b. Pruebe que se pueda establecer conexión con los servidores. c. Haga clic en **Notificar a todos los agentes** después de configurar la lista de fuentes. 3. Determine si los siguientes archivos de configuración del servidor de Smart Protection Server y del Agente de OfficeScan están sincronizados: • `sscfg.ini` • `ssnotify.ini` 4. Abra el editor del Registro y compruebe que el agente esté conectado a la red de empresa. Clave: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • Si aparece el valor `LocationProfile=1`, significa que el Agente de OfficeScan está conectado a la red y que se puede conectar al servidor de Smart Protection Server. • En cambio, si aparece el valor `LocationProfile=2`, significa que el Agente de OfficeScan no está conectado a la red y que se debe conectar a Smart Protection Network. En Internet Explorer, compruebe que el endpoint del Agente de OfficeScan puede explorar páginas Web de Internet. 5. Compruebe la configuración del proxy interno y externo que se utiliza para conectarse a la Red de Smart Protection y a los Smart Protection Servers. Para conocer más detalles, consulte *Proxy interno para agentes de OfficeScan en la página 15-54* y *Proxy externo para agentes de OfficeScan en la página 15-55*. 6. Para agentes de exploración convencional que ejecuten Windows XP, Vista, Server 2003 y Server 2008, compruebe

CONDICIÓN	DESCRIPCIÓN
	que se esté ejecutando OfficeScan NT Proxy Service (`TmProxy.exe`). Si este servicio se detiene, los agentes no se pueden conectar a las fuentes de Smart Protection para realizar consultas de reputación Web. Para agentes de exploración convencional que ejecuten Windows 7, Server 2012 y versiones posteriores, compruebe que se esté ejecutando el controlador tmusa. Si este controlador se detiene, los agentes no se podrán conectar a los orígenes de Smart Protection para realizar consultas de Web Reputation.

Comprobación de la conexión agente-servidor

El estado de conexión del agente con el servidor de OfficeScan aparece en el árbol de agentes de la consola Web de OfficeScan.

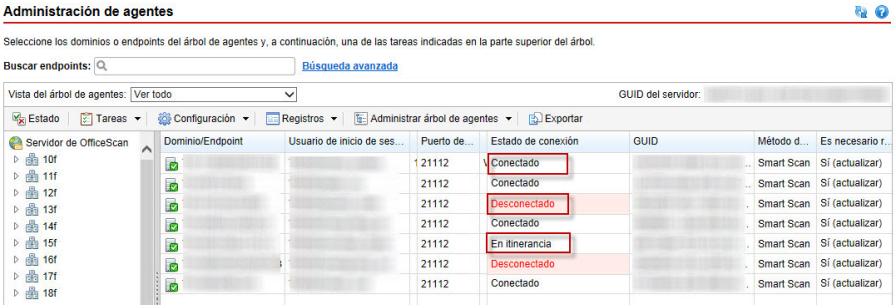


FIGURA 15-2. Árbol de agentes en que el aparece el estado de conexión del agente con el servidor de OfficeScan

Determinadas circunstancias pueden impedir que el árbol de agentes muestre el estado de conexión correcto del agente. Por ejemplo, si se desconecta por accidente el cable de red de un endpoint del agente, el agente no podrá notificar al servidor de que está desconectado. El agente seguirá apareciendo como conectado en el árbol de agentes.

Compruebe la conexión agente-servidor manualmente o deje que OfficeScan realice una comprobación programada. No puede seleccionar dominios o agentes específicos y

comprobar a continuación su estado de conexión. OfficeScan comprueba el estado de conexión de todos sus agentes registrados.

Comprobar conexiones entre agente y servidor

Procedimiento

1. Vaya a **Agentes** > **Comprobación de la conexión**.
2. Para comprobar la conexión entre el agente y el servidor de forma manual, vaya a la pestaña **Comprobación manual** y haga clic en **Comprobar ahora**.
3. Para comprobar la conexión entre el agente y el servidor de manera automática, vaya a la pestaña **Comprobación programada**.
   a. Seleccione **Activar la comprobación programada**.
   b. Seleccione la frecuencia y hora de inicio de la comprobación.
   c. Haga clic en **Guardar** para guardar el programa de comprobación.
4. Compruebe el árbol de agentes para verificar el estado o consultar los registros de comprobación de la conexión.

Registros de comprobación de la conexión

OfficeScan conserva registros de comprobación de la conexión que permiten determinar si el servidor de OfficeScan puede comunicarse o no con todos sus agentes registrados. OfficeScan crea una entrada del registro cada vez que se comprueba la conexión agente-servidor desde la consola Web.

A fin de que el tamaño de los registros no ocupen demasiado espacio en el disco duro, elimínelos manualmente o configure un programa de eliminación de registros. Para obtener más información acerca de la administración de registros, consulte *Administración de registros en la página 14-43*.

Ver los registros de comprobación de la conexión

Procedimiento

1. Vaya a **Registros** > **Agentes** > **Registros de comprobación de la conexión**.
2. Consulte la columna **Estado** para ver los resultados de comprobación de la conexión.
3. Para guardar los registros como un archivo de valores separados por comas (CSV), haga clic en **Exportar a CSV**. Abra el archivo o guárdelo en una ubicación específica.

Agentes no accesibles

Los Agentes de OfficeScan en redes no accesibles, como los de segmentos de red situados detrás de un gateway de NAT, casi nunca tienen conexión porque el servidor no puede establecer conexión directa con los agentes. Como resultado, el servidor no puede notificar a los agentes que:

- Descarguen los componentes más recientes.
- Apliquen la configuración del agente establecida en la consola Web. Por ejemplo, si cambia la frecuencia de la exploración programada en la consola Web, el servidor notificará automáticamente a los agentes que apliquen la nueva configuración.

Por ello, los agentes no accesibles no pueden llevar a cabo estas tareas en el momento apropiado. Sólo las realizan cuando inician la conexión con el servidor, cosa que ocurre cuando:

- Se registran en el servidor tras la instalación.
- Reinician o recargan. Esto no es frecuente, por lo que suele ser necesaria la intervención del usuario.
- La actualización manual o programada se activa en el agente. Este suceso tampoco es frecuente.

El servidor solo "se percata" de la conectividad de los agentes y los trata como si estuvieran conectados durante el registro, el reinicio o la recarga. Sin embargo, dado que

el servidor todavía no es capaz de establecer conexión con los agentes, inmediatamente cambia el estado a desconectados.

OfficeScan ofrece el "latido" y las funciones de sondeo del servidor para resolver problemas relacionados con los agentes no accesibles. Con estas funciones, el servidor deja de notificar a los agentes sobre actualizaciones de los componentes y cambios en la configuración. En lugar de ello, el servidor adopta una función pasiva, a la espera siempre de que los agentes le envíen latidos o que se inicien sondeos. Si el servidor detecta alguno de estos sucesos, empieza a tratar a los agentes como conectados.

Nota

Los sucesos iniciados en el agente que no están relacionados con latidos y sondeos del servidor, como actualizaciones manuales del agente y envíos de registros, no hacen que el servidor actualice el estado de los agentes no accesibles.

Transición

Los Agentes de OfficeScan envían mensajes de transición para notificar al servidor que la conexión desde el agente sigue en funcionamiento. Tras recibir el mensaje de transición, el servidor trata al agente como conectado. En el árbol de agentes, el estado del agente puede ser:

- **Conectado**: para agentes normales conectados.
- **No accesible/Conectado**: para agentes conectados en la red no accesible.

Nota

Los Agentes de OfficeScan no actualizan componentes ni aplican nuevos ajustes de configuración cuando envían mensajes de transición. Los agentes normales efectúan estas tareas durante las rutinas de actualización (consulte *Actualizaciones del agente de OfficeScan en la página 6-30*). Los agentes de la red no accesible las efectúan durante el sondeo del servidor.

La función de transición se ocupa del problema de los Agentes de OfficeScan en redes no accesibles que aparecen siempre como desconectados, aunque sean capaces de conectarse con el servidor.

Un parámetro de la consola Web controla la frecuencia con la que los agentes envían los mensajes de transición. Si el servidor no recibe una transición, empieza inmediatamente

a tratar al agente como desconectado. Otro parámetro controla cuánto tiempo debe transcurrir sin recibir transiciones para que el estado del agente cambie a:

- **Desconectado**: para Agentes de OfficeScan normales desconectados.
- **No accesible/Desconectado**: para Agentes de OfficeScan desconectados en la red no accesible.

Para elegir una configuración de transición de control, hay que buscar un punto de equilibrio entre la necesidad de mostrar la información más reciente sobre el estado del agente y la necesidad de administrar los recursos del sistema. La configuración predeterminada es válida en la mayoría de las situaciones. Sin embargo, hay que tener en cuenta lo siguiente al personalizar la configuración la transición de control:

TABLA 15-7. Recomendaciones sobre la transición

FRECUENCIA DE LA TRANSICIÓN DE CONTROL	RECOMENDACIÓN
Transiciones de control en intervalos largos (más de 60 minutos)	Cuanto mayor sea el intervalo entre transiciones de control, mayor será el número de sucesos que pueden ocurrir antes de que el servidor refleje el estado del agente en la consola Web.
Transiciones de control en intervalos cortos (menos de 60 minutos)	Los intervalos cortos presentan un estado del agente más actualizado, pero es posible que consuman mucho ancho de banda.

Sondeo del servidor

La función de sondeo del servidor resuelve el problema que les ocurre a los Agentes de OfficeScan no accesibles cuando no reciben notificaciones puntuales sobre actualizaciones de componentes y cambios en la configuración del agente. Esta función es independiente de la de transición.

Con la función de sondeo del servidor:

- Los Agentes de OfficeScan inician automáticamente la conexión con el servidor de OfficeScan a intervalos regulares. Cuando el servidor detecta que se ha producido un sondeo, trata al agente como "No accesible/Conectado".

- Los Agentes de OfficeScan se conectan a uno o varios orígenes de actualización para descargar cualquier componente actualizado y aplicar la nueva configuración del agente. Si el origen de actualización principal es el servidor de OfficeScan o un agente de actualización, los agentes obtienen tanto los componentes como la nueva configuración. Si el origen no es el servidor de OfficeScan o un agente de actualización, los agentes obtienen solo los componentes actualizados y, a continuación, se conectan al servidor de OfficeScan o al agente de actualización para obtener la nueva configuración.

Configurar las funciones de transición y de sondeo del servidor

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Red**.
3. Vaya a la sección **Red no accesible**.
4. Defina la configuración del sondeo del servidor.

   Para obtener información detallada acerca del sondeo del servidor, consulte *Sondeo del servidor en la página 15-51*.

   a. Si el servidor de OfficeScan cuenta tanto con dirección IPv4 como IPv6, puede escribir un intervalo de direcciones IPv4 y un prefijo y longitud de IPv6.

      Escriba un intervalo de direcciones IPv4 si el servidor solo utiliza IPv4, o un prefijo y longitud de IPv6 si el servidor solo utiliza IPv6.

      Cuando la dirección IP de cualquier agente coincide con una dirección IP del intervalo, el agente aplica la configuración de transición y de sondeo del servidor y este empieza a tratar al agente como parte de la red no accesible.

Nota

Los agentes con una dirección IPv4 pueden conectarse a un servidor de OfficeScan de doble pila o que solo utiliza IPv4.

Los agentes con una dirección IPv6 pueden conectarse a un servidor de OfficeScan de doble pila o que solo utiliza IPv6.

Los agentes de doble pila pueden conectarse a un servidor de OfficeScan de doble pila, o que solo utiliza IPv4 o IPv6.

b. Especifique la frecuencia de sondeo del servidor en **Los agentes sondean el servidor para los componentes y configuración actualizada cada __ minutos**. Introduzca un valor comprendido entre 1 y 129.600 minutos

Consejo

Trend Micro recomienda que la frecuencia de sondeo del servidor sea de al menos tres veces la de envío de transición.

5. Defina la configuración de transición.

Para obtener información detallada acerca de la función de transición, consulte *Transición en la página 15-50*.

a. Seleccione **Permitir que los agentes envíen transiciones al servidor**.

b. Seleccione **Todos los agentes** o **Solo los agentes de la red no accesible**.

c. Especifique la frecuencia con la que los agentes envían transiciones en **Los agentes envían transiciones cada __ minutos**. Introduzca un valor comprendido entre 1 y 129.600 minutos

d. En **Un agente está desconectado si no hay transiciones pasados __ minutos**, especifique cuánto tiempo debe transcurrir sin recibir transiciones para que el servidor de OfficeScan considere un agente como desconectado. Introduzca un valor comprendido entre 1 y 129.600 minutos

6. Haga clic en **Guardar**.

Configuración del proxy del agente de OfficeScan

Configure los Agentes de OfficeScan para utilizar la configuración del proxy cuando se conecte a servidores internos y externos.

Proxy interno para agentes de OfficeScan

Los Agentes de OfficeScan pueden utilizar la configuración del proxy interno para conectarse a los siguientes servidores en la red:

- Servidor de OfficeScan

  El equipo del servidor aloja el servidor de OfficeScan y el servidor Smart Protection Server integrado. Los Agentes de OfficeScan se conectan al servidor de OfficeScan para actualizar componentes, obtener la configuración y enviar registros. Los Agentes de OfficeScan se conectan al servidor Smart Protection Server integrado para enviar consultas de exploración.

- Smart Protection Servers

  Los servidores de Smart Protection Server engloban todos los servidores de Smart Protection Server independientes y el servidor de Smart Protection Server integrado de otros servidores de OfficeScan. Los Agentes de OfficeScan se conectan a los servidores para enviar consultas de exploración y de Web Reputation.

Definir la configuración del proxy

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Proxy**.
2. Haga clic en la pestaña **Proxy interno**.
3. Vaya a la sección **Conexión del agente con el servidor de OfficeScan**.

a. Seleccione **Utilizar la siguiente configuración del proxy si los agentes se conectan al servidor de OfficeScan**.

b. Especifique el nombre del servidor proxy o la dirección IPv4/IPv6, además del número de puerto.

Nota

Si cuenta con agentes IPv4 e IPv6, especifique un servidor proxy de doble pila identificado mediante el nombre del host. Esto se debe a que la configuración del proxy interno es la configuración general. Si especifica una dirección IPv4, los agentes IPv6 no se podrán conectar al servidor proxy. Lo mismo sucede para los agentes IPv4.

c. Si el servidor proxy requiere autenticación, escriba el nombre de usuario y la contraseña y, después, confirme la contraseña.

4. Vaya a la sección **Conexión del agente con los servidores de Smart Protection Server independientes**.

   a. Seleccione **Utilizar la siguiente configuración del proxy si los agentes se conectan a los servidores de Smart Protection Server independientes**.

   b. Especifique el nombre del servidor proxy o la dirección IPv4/IPv6, además del número de puerto.

   c. Si el servidor proxy requiere autenticación, escriba el nombre de usuario y la contraseña y, después, confirme la contraseña.

5. Haga clic en **Guardar**.

Proxy externo para agentes de OfficeScan

El servidor de OfficeScan y el Agente de OfficeScan pueden utilizar la configuración del proxy externo cuando se conecten a servidores alojados por Trend Micro. En este tema se trata la configuración del proxy externo para agentes. Para obtener información de la configuración del proxy externo para el servidor, consulte *Proxy para las actualizaciones del servidor de OfficeScan en la página 6-20*.

Los Agentes de OfficeScan pueden usar los ajustes del servidor proxy configurados en Internet Explorer o Chrome para conectarse a Trend Micro Smart Protection Network.

En caso de que sea necesaria la autenticación del servidor proxy, los agentes utilizarán las credenciales de autenticación del servidor proxy (contraseña e ID de usuario).

Configurar las credenciales de autenticación del servidor proxy

Procedimiento

1. Vaya a **Administración** > **Configuración** > **Proxy**.
2. Haga clic en la pestaña **Proxy externo**.
3. Vaya a la sección **Conexión del agente de OfficeScan con servidores de Trend Micro**.
4. Escriba el Id de usuario y la contraseña necesarios para la autenticación del servidor proxy. Se admiten los siguientes protocolos de autenticación del servidor proxy:
   - Autenticación de acceso básico
   - Autenticación de acceso de resumen
   - Autenticación de Windows integrada
5. Haga clic en **Guardar**.

Configurar los ajustes de proxy del servicio global de Smart Protection

Los Agentes de OfficeScan usan los ajustes de proxy del servicio de Smart Protection configurados cuando consulta a los orígenes de Smart Protection acerca de las siguientes características:

- Aprendizaje automático predictivo
- Supervisión del comportamiento

Nota

Si el servidor Smart Protection Server integrado no está disponible, los Agentes de OfficeScan se conectan a Trend Micro Smart Protection Network para realizar las consultas.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Sistema**.
3. Vaya a la sección **Proxy del servicio Smart Protection**.
4. Active **Usar los orígenes configurados de Smart Protection para las consultas del servicio**.

   Importante

   El proxy del servicio Smart Protection solo admite el protocolo HTTPS para las consultas de File Reputation. Asegúrese de que todos los servidores Smart Protection Server configurados que proporcionen servicios de File Reputation utilicen el protocolo HTTPS.

   De forma predeterminada, el servidor Smart Protection Server integrado no utiliza la comunicación HTTPS. Para cambiar el método de comunicación, consulte *Configuración de los ajustes de Smart Protection Server integrado en la página 4-22*.

   Para comprobar el método de comunicación utilizado por los servidores Smart Protection Server independientes, consulte *Configuración de listas personalizadas de fuentes de Smart Protection en la página 4-28*.

5. Haga clic en **Guardar**.

Derechos de configuración del proxy para agentes

Puede conceder a los usuarios del agente el derecho de definir la configuración del proxy. Los Agentes de OfficeScan utilizan la configuración del proxy definida por el usuario solo en las situaciones siguientes:

- Cuando los Agentes de OfficeScan ejecutan la función "Actualizar ahora".
- Cuando los usuarios desactivan la configuración automática del proxy o el Agente de OfficeScan no la detecta.

  Consulte el apartado *Configuración automática del proxy del agente de OfficeScan en la página 15-59* para obtener más información.

¡ADVERTENCIA!

Una configuración del proxy definida por el usuario de forma incorrecta puede acarrear problemas de actualización. Proceda con cautela cuando permita que los usuarios definan su propia configuración del proxy.

Conceder derechos de configuración del proxy

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.
4. En la pestaña **Derechos**, vaya a la sección **Configuración del proxy**.
5. Seleccione **Permitir que los usuarios configuren el proxy**.
6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.

- **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Configuración automática del proxy del agente de OfficeScan

La configuración manual del proxy puede ser una tarea complicada para muchos usuarios finales. Utilice la configuración automática del proxy para garantizar la aplicación de la configuración del proxy correcta sin necesidad de que intervenga el usuario.

Cuando se activa, la configuración automática del proxy será la configuración principal del proxy cuando los Agentes de OfficeScan actualicen los componentes de forma automática o mediante la función Actualizar ahora. Para obtener información sobre la actualización automática o la función Actualizar ahora, consulte *Métodos de actualización de los agentes de OfficeScan en la página 6-40*.

Si los Agentes de OfficeScan no pueden conectarse con la configuración automática del proxy, los usuarios de agentes con derechos para definir la configuración del proxy pueden utilizar la configuración del proxy definida por el usuario. De lo contrario, no será posible establecer la conexión con la configuración automática del proxy.

Nota

No se admite la autenticación del proxy.

Definir la configuración automática del proxy

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Haga clic en la pestaña **Red**.
3. Vaya a la sección **Configuración del proxy**.

4. Seleccione **Detectar la configuración automáticamente** si desea que OfficeScan detecte de forma automática, mediante DHCP o DNS, la configuración del proxy definida por el administrador.

5. Si desea que OfficeScan utilice la secuencia de comandos de configuración automática del proxy (PAC, por sus siglas en inglés) definida por el administrador de la red para detectar el servidor proxy apropiado:

   a. Seleccione **Utilizar una secuencia de comandos de configuración automática**.

   b. Escriba la dirección para la secuencia de comandos de la PAC.

6. Haga clic en **Guardar**.

Visualización de información sobre agentes de OfficeScan

La pantalla Ver estado muestra información importante acerca de los Agentes de OfficeScan, incluidos los derechos, detalles sobre el software del agente y sucesos del sistema.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.

2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.

3. Haga clic en **Estado**.

4. Amplíe el nombre del endpoint del agente para ver información de su estado. Si ha seleccionado varios agentes, haga clic en **Expandir todo** para ver la información del estado de los agentes seleccionados.

5. (Opcional) Utilice el botón **Restablecer** para volver a fijar en cero el recuento de riesgos de seguridad.

Importación y exportación de la configuración de los agentes

OfficeScan le permite exportar configuraciones del árbol de agentes que hayan aplicado un Agente de OfficeScan o un dominio concretos a un archivo. Después, puede importar el archivo para aplicar la configuración a otros agentes o dominios o a otro servidor de OfficeScan de la misma versión.

Se exportarán todas las configuraciones del árbol de agentes, excepto la del agente de actualización.

Exportación de la configuración del agente

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Configuración** > **Exportar configuración**.
4. Haga clic en uno de los enlaces para ver la configuración del Agente de OfficeScan o el dominio que haya seleccionado.
5. Haga clic en **Exportar** para guardar la configuración.

   La configuración se guarda en un archivo `.dat`.
6. Haga clic en **Guardar** y, a continuación, especifique la ubicación en la que desee guardar el archivo `.dat`.
7. Haga clic en **Guardar**.

Importación de la configuración del agente

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccione dominios o agentes específicos.
3. Haga clic en **Configuración** > **Importar configuración**.
4. Haga clic en **Examinar** para buscar el archivo `.dat` en el endpoint y haga clic en **Importar**.

   Aparecerá la pantalla **Importar configuración**, que muestra un resumen de la configuración.
5. Haga clic en uno de los enlaces para ver los detalles relacionados con la configuración de exploración o con los derechos que se vayan a importar.
6. Importe la configuración.
   - En caso de que haya hecho clic en el icono del dominio raíz, seleccione **Aplicar a todos dominios** y, después, haga clic en **Aplicar al destino**.
   - Si ha seleccionado los dominios, seleccione **Aplicar a todos los equipos de los dominios seleccionados** y, después, haga clic en **Aplicar al destino**.
   - Si ha seleccionado varios agentes, haga clic en **Aplicar al destino**.

Conformidad con las normas de seguridad

Utilice Conformidad con las normas de seguridad para determinar errores, implementar soluciones y mantener la infraestructura de seguridad. Esta función ayuda a reducir el tiempo necesario para garantizar la seguridad del entorno de la red y equilibrar las necesidades de la organización para garantizar la seguridad y la funcionalidad.

Gestione la conformidad con las normas de seguridad de dos tipos de endpoints:

- **Gestionada**: endpoints con Agentes de OfficeScan que administra el servidor de OfficeScan. Para conocer más detalles, consulte *Conformidad con las normas de seguridad para agentes administrados en la página 15-63*.
- **Sin gestionar**: incluye los elementos que se describen a continuación.
  - Agentes de OfficeScan que el servidor de OfficeScan no administra.
  - Endpoints en los que no se han instalado Agentes de OfficeScan.
  - Endpoints a los que el servidor de OfficeScan no puede acceder.
  - Endpoints cuyo estado de seguridad no se puede comprobar.

    Para conocer más detalles, consulte *Conformidad con las normas de seguridad para Endpoints no administrados en la página 15-76*.

Conformidad con las normas de seguridad para agentes administrados

La función Conformidad con las normas de seguridad genera un informe de conformidad para ayudarle a valorar el estado de seguridad de los Agentes de OfficeScan administrados por el servidor de OfficeScan. Esta función genera el informe bajo petición o según un programa.

La pantalla **Valoración manual** contiene las siguientes pestañas:

- **Servicios**: utilice esta pestaña para comprobar que los servicios del agente funcionan.

  Para conocer más detalles, consulte *Servicios en la página 15-64*.
- **Componentes**: utilice esta pestaña para comprobar que los componentes de los Agentes de OfficeScan están actualizados.

  Para conocer más detalles, consulte *Componentes en la página 15-66*.
- **Conformidad con la exploración**: utilice esta pestaña para comprobar que los Agentes de OfficeScan ejecutan exploraciones de forma regular.

  Para conocer más detalles, consulte *Conformidad con la exploración en la página 15-68*.

- **Configuración**: utilice esta pestaña para comprobar que la configuración del agente coincide con la del servidor.

  Para conocer más detalles, consulte *Configuración en la página 15-70*.

Nota

La pestaña **Componentes** puede mostrar los Agentes de OfficeScan que estén ejecutando la versión actual y anteriores del producto. En las demás pestañas, solo se muestran los Agentes de OfficeScan que estén ejecutando la versión 10.5, 10.6 o superior, o los Agentes de OfficeScan.

Importante

- La función Conformidad con las normas de seguridad consulta el estado de conexión de los Agentes de OfficeScan antes de generar un informe de conformidad. En este informe se incluyen los agentes conectados y sin conexión, pero no los que están en modo independiente.
- Para cuentas de usuario basadas en funciones:
  - Cada cuenta de usuario de la consola Web tiene una configuración del informe de conformidad completamente independiente. Los cambios que se efectúen en la configuración del informe de conformidad de una cuenta de usuario no afectarán a la configuración de las demás cuentas de usuario.
  - El alcance del informe depende de los permisos del dominio del agente para la cuenta de usuario. Si, por ejemplo, concede permisos a una cuenta de usuario para que administre los dominios A y B, los informes de la cuenta de usuario solo mostrarán datos de aquellos agentes que pertenezcan a los dominios A y B.

    Para obtener información detallada acerca de las cuentas de usuario, consulte *Role-based Administration en la página 14-3*.

Servicios

La característica Conformidad con las normas de seguridad comprueba que funcionen los siguientes servicios del Agente de OfficeScan:

- Antivirus

- Antispyware
- Cortafuegos
- Reputación Web
- Supervisión del comportamiento/Control de dispositivos (también conocido como Servicio de prevención de cambios no autorizados de Trend Micro)
- Protección de datos
- Conexión sospechosa

Un agente no compatible se cuenta dos veces como mínimo en el informe de conformidad.

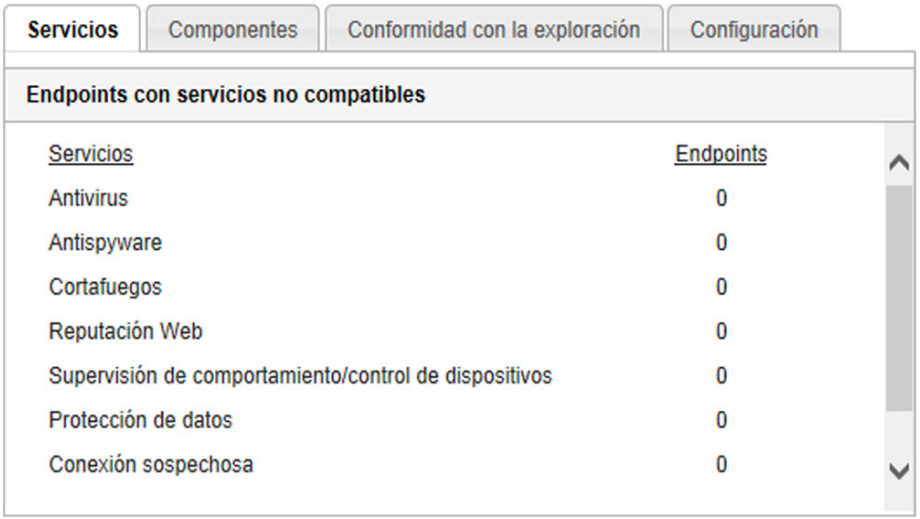


FIGURA 15-3. Informe de conformidad: pestaña Servicios

- En la categoría **Endpoints con servicios no compatibles**.
- En la categoría para la que el Agente de OfficeScan no sea compatible. Por ejemplo, si el servicio antivirus del Agente de OfficeScan no funciona, el agente se cuenta en la categoría **Antivirus**. Si no funciona más de un servicio, el agente se cuenta en cada categoría para la que no sea compatible.

Reinicie los servicios que no funcionen en la consola Web o el Agente de OfficeScan. Si los servicios funcionan tras el reinicio, el agente no aparecerá como no compatible en la siguiente valoración.

Componentes

La función Conformidad con las normas de seguridad determina las incoherencias de las versiones de los componentes entre el servidor de OfficeScan y los Agentes de OfficeScan. Las incoherencias ocurren, por lo general, cuando los agentes no se pueden conectar al servidor para actualizar componentes. Si el agente obtiene actualizaciones de otro origen (como Trend Micro ActiveUpdate Server), es posible que una versión del componente del agente sea más reciente que la del servidor.

La función Conformidad con las normas de seguridad comprueba los siguientes componentes:

- Smart Scan Agent Pattern
- Patrón de virus
- Patrón de IntelliTrap
- Patrón de excepciones de IntelliTrap
- Motor de exploración antivirus de 32 y 64 bits
- Patrón de spyware y grayware
- Patrón de supervisión activa de spyware
- Motor de exploración de spyware/grayware de 32/64 bits
- Plantilla de Damage Cleanup
- Motor de Damage Cleanup de 32 y 64 bits
- Patrón del cortafuegos habitual
- Controlador del cortafuegos habitual de 32/64 bits
- Controlador básico de la supervisión del comportamiento de 32 y 64 bits
- Servicio básico de la supervisión de comportamiento de 32 y 64 bits
- Patrón de configuración de la supervisión de comportamiento
- Patrón de firmas digitales
- Patrón de aplicación de políticas
- Patrón de detección de la supervisión de comportamiento (32/64 bits)
- Lista de IP de C&C general
- Patrón de regla de relevancia
- Early Boot Cleanup Driver de 32/64 bits
- Patrón del activador de exploración de memoria (32/64 bits)
- Patrón de inspección de la memoria
- Patrón de prevención de explotación del explorador
- Patrón unificado del analizador de secuencias de comando
- Patrón de supervisión de inspección del programa
- Patrón de Damage Recovery
- Patrón antimalware de inicio temprano de 32/64 bits
- Motor de inteligencia contextual de 32/64 bits
- Patrón de inteligencia contextual
- Controlador de consultas de inteligencia contextual de 32/64 bits
- Motor de exploración de amenazas avanzadas de 32/64 bits
- Patrón de correlación de amenazas avanzadas
- Versión del programa

Un agente no compatible se cuenta dos veces como mínimo en el informe de conformidad.

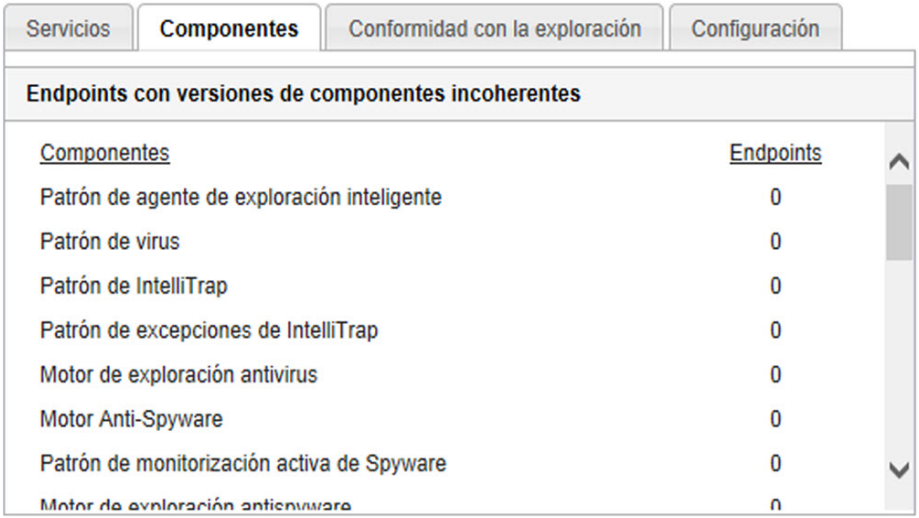


FIGURA 15-4. Informe de conformidad: pestaña Componentes

- En la categoría **Endpoints con versiones de componentes incoherentes**
- En la categoría para la cual el agente no sea compatible. Si, por ejemplo, la versión de Smart Scan Agent Pattern del agente no coincide con la del servidor, el agente se incluirá en la categoría **Smart Scan Agent Pattern**. Si hay más de una versión de componente que no coincida, el agente se cuenta en cada categoría para la que no sea compatible.

Para resolver incoherencias de las versiones de los componentes, actualice los componentes obsoletos en los agentes o en el servidor.

Conformidad con la exploración

La función Conformidad con las normas de seguridad comprueba que las opciones Explorar ahora o Exploración programada se ejecuten de manera regular y que se completen en un periodo de tiempo razonable.

Nota

La función Conformidad con las normas de seguridad solo puede emitir informes sobre el estado de la exploración programada si esta función está activada para los agentes.

La función Conformidad con las normas de seguridad utiliza los siguientes criterios de conformidad con la exploración:

- **No se han ejecutado Explorar ahora ni Exploración programada en los últimos (x) días**: el Agente de OfficeScan no es compatible si no ejecuta las opciones Explorar ahora ni Exploración programada en el número de días que se han especificado.
- **Las opciones Explorar ahora o Exploración programada han superado las (x) horas**: el Agente de OfficeScan no es compatible si la última ejecución de Explorar ahora o Exploración programada ha superado el número de horas que se ha especificado.

Un agente no compatible se cuenta dos veces como mínimo en el informe de conformidad.

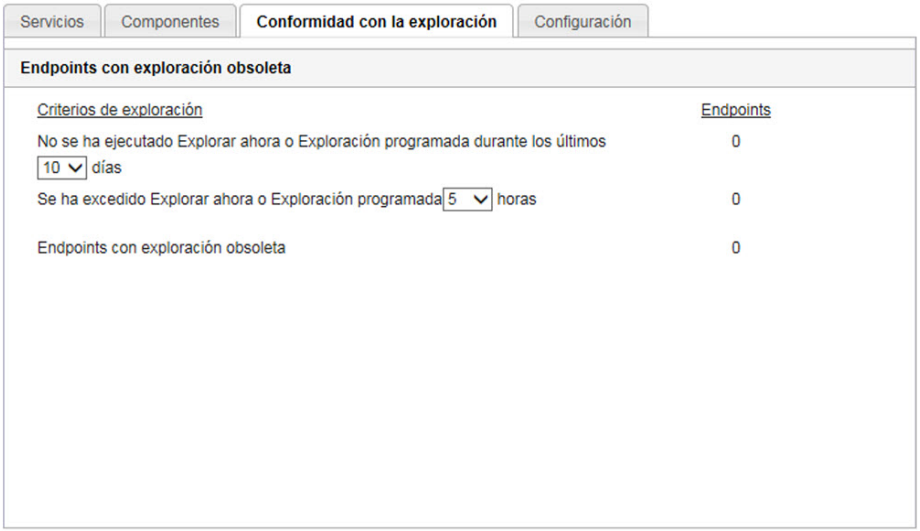


FIGURA 15-5. Informe de conformidad: pestaña Conformidad con la exploración

- En la categoría **Endpoints con exploración obsoleta**.
- En la categoría para la que el agente no sea compatible. Por ejemplo, si la última ejecución de la opción Exploración programada ha excedido el número de horas que se ha especificado, el agente se cuenta en la categoría **Las opciones Explorar ahora o Exploración programada han superado las (x) horas**. Si el agente cumple con más de un criterio de conformidad con la exploración, se cuenta en cada categoría para la que no sea compatible.

Ejecute las opciones Explorar ahora o Exploración programada en agentes que no han realizado tareas de exploración o que no pudieron completarlas.

Configuración

La función de conformidad con las nomras de seguridad comprueba que los agentes tengan la misma configuración que sus dominios primarios en el árbol de agentes. Puede que la configuración no coincida si se mueve cualquier agente a otro dominio que tenga una configuración distinta o si un agente con ciertos derechos ha configurado parámetros de forma manual en la consola del Agente de OfficeScan.

OfficeScan comprueba los siguientes valores de configuración:

- Método de exploración
- Configuración de la exploración manual
- Configuración de la exploración en tiempo real
- Configuración de la exploración programada
- Configuración de Explorar ahora
- Derechos y otras configuraciones
- Configuración de servicios adicionales
- Reputación Web
- Supervisión del comportamiento
- Control de dispositivos
- Lista de spyware/grayware permitido
- Configuración de la prevención de pérdida de datos
- Conexión sospechosa
- Lista de programas de confianza
- Envío de muestras
- Aprendizaje automático predictivo

Un agente no compatible se cuenta dos veces como mínimo en el informe de conformidad.

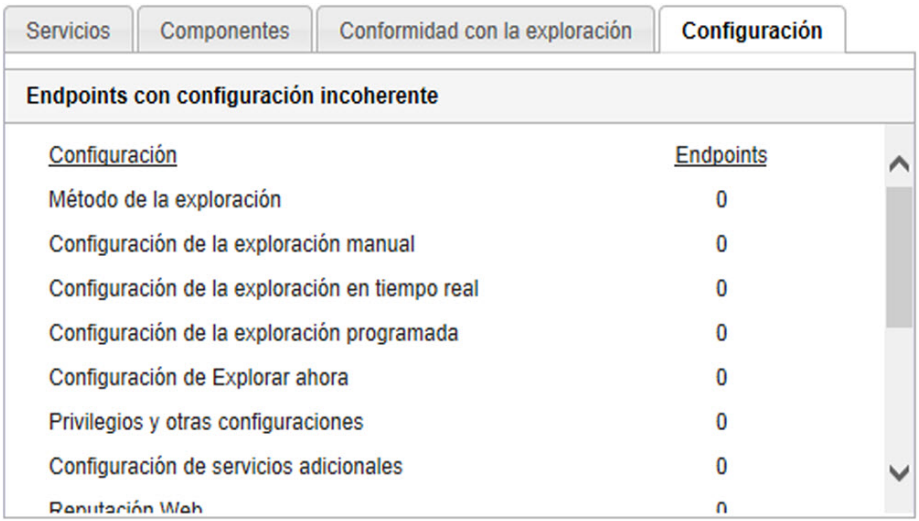


FIGURA 15-6. Informe de conformidad: pestaña Configuración

- En la categoría **Endpoints con parámetros de configuración incoherentes**.
- En la categoría para la cual el agente no sea compatible. Si, por ejemplo, la configuración del método de exploración del agente no coincide con la de su dominio primario, el agente se cuenta en la categoría **Método de exploración**. Si hay más de un conjunto de parámetros de configuración que no coincida, el agente se cuenta en cada categoría para la que no sea compatible.

Para resolver las incoherencias de configuración, aplique al agente la configuración del dominio.

Informes de conformidad bajo petición

La función Conformidad con las normas de seguridad puede generar informes de conformidad bajo petición. Los informes permiten valorar el estado de seguridad de los Agentes de OfficeScan que gestiona el servidor de OfficeScan.

Para obtener más información acerca de los informes de conformidad, consulte *Conformidad con las normas de seguridad para agentes administrados en la página 15-63*.

Generar un informe de conformidad a petición

Procedimiento

1. Vaya a **Valoración** > **Conformidad con las normas de seguridad** > **Informe manual**.
2. Vaya a la sección **Alcance del árbol de agentes**.
3. Seleccione el dominio raíz o un dominio y haga clic en **Valorar**.
4. Visualice el informe de conformidad para los servicios del agente.

   Para obtener más información sobre los servicios del agente, consulte *Servicios en la página 15-64*.

   a. Haga clic en la pestaña **Servicios**.

   b. En **Endpoints con servicios no compatibles**, compruebe el número de agentes con servicios que no sean compatibles.

   c. Haga clic en el enlace de número para que se muestren en el árbol de agentes todos los agentes afectados.

   d. Seleccione los agentes desde el resultado de la consulta.

   e. Haga clic en **Reiniciar el agente de OfficeScan** para reiniciar el servicio.

   > **Nota**
   >
   > Reinicie el servicio en el endpoint del agente en caso de que este aún aparezca como no compatible después de realizar otra valoración.

   f. Para guardar la lista de los agentes en un archivo, haga clic en **Exportar**.
5. Visualice el informe de conformidad para los componentes del agente.

   Para obtener información detallada acerca de los componentes del agente, consulte *Componentes en la página 15-66*.

a. Haga clic en la pestaña **Components** tab.

b. En **Endpoints con versiones de componentes incoherentes**, compruebe el número de agentes con versiones de los componentes que no coincidan con las versiones del servidor.

c. Haga clic en el enlace de número para que se muestren en el árbol de agentes todos los agentes afectados.

Nota

Si hay al menos un agente que tenga un componente más actualizado que el servidor de OfficeScan, actualice el servidor de OfficeScan manualmente.

d. Seleccione los agentes desde el resultado de la consulta.

e. Haga clic en **Actualizar ahora** para aplicar agentes a los componentes de descarga.

Nota

- Con el fin de garantizar que los agentes puedan actualizar el programa del agente, desactive la opción **Los agentes de OfficeScan pueden actualizar componentes, pero no el programa del agente, y no pueden implementar archivos HotFix** en **Agentes** > **Administración de agentes > Configuración** > **Derechos y otra configuración**.
- Reinicie el endpoint en lugar de hacer clic en **Actualizar ahora** para actualizar el driver del Cortafuegos común.

f. Para guardar la lista de los agentes en un archivo, haga clic en **Exportar**.

6. Visualice el informe de conformidad para las exploraciones.

Para obtener información detallada acerca de las exploraciones, consulte *Conformidad con la exploración en la página 15-68*.

a. Haga clic en la pestaña **Conformidad con la exploración**.

b. En **Endpoints con exploración obsoleta**, configure lo siguiente:

- Número de días en los que el agente no ha ejecutado Explorar ahora o Exploración programada

- Número de horas que Explorar ahora o Exploración programada se están ejecutando

Nota

Si se excede el número de días u horas, se tratará al agente como no compatible.

c. Haga clic en **Valorar**, junto a la sección **Alcance del árbol de agentes**.

d. En **Endpoints con exploración obsoleta**, compruebe el número de agentes que se ajuste a los criterios de exploración.

e. Haga clic en el enlace de número para que se muestren en el árbol de agentes todos los agentes afectados.

f. Seleccione los agentes desde el resultado de la consulta.

g. Haga clic en **Explorar ahora** para iniciar la opción Explorar ahora en los agentes.

Nota

Con el fin de evitar que se repita la exploración, la opción **Explorar ahora** se desactivará si esta ha durado un número mayor de horas que las especificadas.

h. Para guardar la lista de los agentes en un archivo, haga clic en **Exportar**.

7. Visualice el informe de conformidad para la configuración.

Para obtener información detallada acerca de la configuración, consulte *Configuración en la página 15-70*.

a. Haga clic en la pestaña **Configuración**.

b. En **Equipos con parámetros de configuración incoherentes**, compruebe el número de agentes con configuraciones que no coincidan con las del dominio del árbol de agentes.

c. Haga clic en el enlace de número para que se muestren en el árbol de agentes todos los agentes afectados.

d. Seleccione los agentes desde el resultado de la consulta.

e. Haga clic en **Aplicar configuración del dominio**.

f. Para guardar la lista de los agentes en un archivo, haga clic en **Exportar**.

Informes de conformidad programados

La función Conformidad con las normas de seguridad puede generar informes de conformidad según un programa. Los informes permiten valorar el estado de seguridad de los Agentes de OfficeScan que gestiona el servidor de OfficeScan.

Para obtener más información acerca de los informes de conformidad, consulte *Conformidad con las normas de seguridad para agentes administrados en la página 15-63*.

Definir una configuración para informes de conformidad programados

Procedimiento

1. Vaya a **Valoración** > **Conformidad con las normas de seguridad** > **Informe programado**.
2. Seleccione **Activar informes programados**.
3. Introduzca un título para el informe.
4. Seleccione una o todas de las opciones siguientes:
   - *Servicios en la página 15-64*
   - *Componentes en la página 15-66*
   - *Conformidad con la exploración en la página 15-68*
   - *Configuración en la página 15-70*
5. Especifique las direcciones de correo electrónico en las que recibirá notificaciones sobre informes de conformidad programados.

Nota

Defina la configuración de las notificaciones de correo electrónico para garantizar que estas se envíen correctamente. Para conocer más detalles, consulte *Configuración de las notificaciones del administrador en la página 14-39*.

6. Especifique el programa.
7. Haga clic en **Guardar**.

Conformidad con las normas de seguridad para Endpoints no administrados

La función Conformidad con las normas de seguridad puede realizar consultas de los Endpoints no administrados en la red a la que pertenezca el servidor de OfficeScan. Utilice Active Directory y las direcciones IP para realizar consultas de los Endpoints.

El estado de seguridad de los Endpoints no administrados puede ser cualquiera de los siguientes:

TABLA 15-8. Estado de seguridad de Endpoints no administrados

ESTADO	DESCRIPCIÓN
Gestionado por otro servidor de OfficeScan	Los Agentes de OfficeScan que están instalados en el equipo los administra otro servidor de OfficeScan. Los Agentes de OfficeScan están conectados y ejecutan esta versión de OfficeScan o una versión anterior.
No hay ningún Agente de OfficeScan instalado	El Agente de OfficeScan no está instalado en el endpoint.
No accesible	El servidor de OfficeScan no se puede conectar al endpoint para determinar su estado de seguridad.

Estado	Descripción
Valoración de Active Directory sin resolver	El endpoint pertenece a un dominio de Active Directory, pero el servidor de OfficeScan no puede determinar su estado de seguridad. **Nota** La base de datos del servidor de OfficeScan contiene una lista de agentes gestionados por el servidor. El servidor solicita información sobre los GUID del equipo a Active Directory y los compara con el GUID almacenado en la base de datos. Si un GUID no se encuentra en la base de datos, el endpoint formará parte de la categoría Valoración de Active Directory sin resolver.

Para ejecutar una valoración de seguridad, lleve a cabo las siguientes tareas:

1. Defina el alcance de la consulta. Para conocer más detalles, consulte *Definir el alcance y la consulta de Active Directory/de la dirección IP en la página 15-77*.
2. Compruebe los equipos que no estén protegidos desde el resultado de la consulta. Para conocer más detalles, consulte *Ver los resultados de la consulta en la página 15-80*.
3. Instale el Agente de OfficeScan. Para conocer más detalles, consulte *Instalar de conformidad con las normas de seguridad en la página 5-68*.
4. Configure las consultas programadas. Para conocer más detalles, consulte *Configurar las valoraciones de consulta programadas en la página 15-81*.

Definir el alcance y la consulta de Active Directory/de la dirección IP

Cuando realice consultas por primera vez, defina el alcance de Active Directory/de la dirección IP, el cual incluye los objetos de Active Directory y las direcciones IP que el servidor de OfficeScan consultará bajo petición o de forma periódica. Tras definir el alcance, comience el proceso de consulta.

Nota

Para definir un alcance de Active Directory, OfficeScan se debe integrar primero con Active Directory. Si desea obtener información detallada acerca de la integración, consulte *Integración con Active Directory en la página 2-42*.

Procedimiento

1. Vaya a **Valoración** > **Endpoints no administrados**.
2. En la sección **Alcance de Active Directory/de la dirección IP**, haga clic en **Definir alcance**.

   Se abrirá una nueva pantalla.
3. Para definir un alcance de Active Directory:

   a. Vaya a la sección **Alcance de Active Directory**.

   b. Seleccione **Utilizar valoración a petición** para realizar consultas en tiempo real y, de este modo, obtener resultados más precisos. La desactivación de esta opción hace que OfficeScan realice las consultas en la base de datos en lugar de en cada Agente de OfficeScan. La realización de consultas solo en la base de datos puede ser más rápida, pero es menos precisa.

   c. Seleccione los objetos que deban consultarse. Si la consulta se está realizando por primera vez, seleccione un objeto que tenga menos de 1,000 cuentas y, a continuación, anote cuánto tiempo tarda en realizar la consulta. Utilice esta información como su referencia en cuanto a rendimiento.
4. Para definir un alcance de la dirección IP:

   a. Vaya a la sección **Alcance de la dirección IP**.

   b. Seleccione **Activar alcance de la dirección IP**.

   c. Especifique un intervalo de direcciones IP. Haga clic en los botones más o menos para agregar o eliminar intervalos de direcciones IP.

   - Si el servidor de OfficeScan solo utiliza IPv4, escriba un intervalo de direcciones IPv4.

- Si el servidor de OfficeScan solo utiliza IPv6, escriba un prefijo y longitud de IPv6.
- Si el servidor de OfficeScan es de doble pila, escriba un intervalo de direcciones IPv4 y/o un prefijo y longitud de IPv6.

  El límite del intervalo de direcciones IPv6 es de 16 bits, que es similar al límite de los intervalos de direcciones IPv4. Por lo tanto, la longitud del prefijo ha de estar comprendida entre 112 y 128.

TABLA 15-9. Longitud de prefijos y números de direcciones IPv6

LONGITUD:	NÚMERO DE DIRECCIONES IPV6
128	2
124	16
120	256
116	4,096
112	65,536

5. En Configuración avanzada, especifique los puertos que utilizan los servidores de OfficeScan para comunicarse con los agentes. La instalación aleatoria genera el número de puerto durante la instalación del servidor de OfficeScan.

   Para ver el puerto de comunicación que utiliza el servidor de OfficeScan, vaya a **Agentes** > **Administración de agentes** y seleccione un dominio. El puerto se muestra junto a la columna de dirección IP. Trend Micro recomienda anotar los números de puerto para que le sirvan como referencia.

   a. Haga clic en **Especificar puertos**.

   b. Escriba el número de puerto y haga clic en **Agregar**. Repita este paso hasta que haya introducido todos los números de puerto que desea agregar.

   c. Haga clic en **Guardar**.

6. Para comprobar la conectividad de los endpoints mediante un número de puerto en concreto, seleccione **Declarar un endpoint no accesible comprobando el puerto <x>**. Cuando no se pueda establecer la conexión, OfficeScan

inmediatamente trata el endpoint como no accesible. El número de puerto predeterminado es el 135.

Si se activa este ajuste se agilizará la consulta. Cuando no se puede establecer la conexión con los endpoints, el servidor de OfficeScan ya no necesita realizar el resto de tareas de comprobación de la conexión antes de tratar los endpoints como no accesibles.

7. Para guardar el alcance e iniciar la consulta, haga clic en **Guardar y volver a valorar**. Para únicamente guardar la configuración, haga clic en **Sólo guardar**.

   En la pantalla **Administración de servidores externos** se muestra el resultado de la consulta.

   Nota

   Es posible que la consulta tarde bastante en completarse, sobre todo si su alcance es amplio. No realice otra consulta hasta que en la pantalla Administración de servidores externos no se muestre el resultado. Si lo hace, la sesión de consulta que esté en curso finalizará y volverá a iniciarse el proceso de consulta.

Ver los resultados de la consulta

El resultado de la consulta aparece en la sección **Estado de seguridad**. Un endpoint no administrado tendrá uno de los siguientes estados:

- Gestionado por otro servidor de OfficeScan
- No hay ningún Agente de OfficeScan instalado
- No accesible
- Valoración de Active Directory sin resolver

Procedimiento

1. En la sección **Estado de seguridad**, haga clic en el enlace de un número para mostrar todos los equipos afectados.

2. Utilices las funciones de búsqueda y búsqueda avanzada para buscar y mostrar únicamente los equipos que cumplen los criterios de búsqueda.

   En el caso de que utilice la función de búsqueda avanzada, especifique lo siguiente:

   - Intervalo de direcciones IPv4
   - Prefijo y longitud de IPv6 (el prefijo ha de estar comprendido entre 112 y 128)
   - Nombre del endpoint
   - Nombre del servidor de OfficeScan
   - Árbol de Active Directory
   - Estado de seguridad

   OfficeScan no ofrecerá ningún resultado si el nombre está incompleto. Utilice el carácter comodín (*) si no está seguro de cuál es el nombre completo.

3. Para guardar la lista de los equipos en un archivo, haga clic en **Exportar**.

4. En el caso de los Agentes de OfficeScan que otro servidor de OfficeScan administra, utilice la herramienta Agent Mover para que el servidor de OfficeScan actual administre estos Agentes de OfficeScan. Para obtener más información sobre esta herramienta, consulte *Agent Mover en la página 15-24*.

Configurar las valoraciones de consulta programadas

Con el fin de asegurar que se implementen las directrices de seguridad, configure el servidor de OfficeScan para que realice consultas periódicas de Active Directory y de las direcciones IP.

Procedimiento

1. Vaya a **Valoración** > **Endpoints no administrados**.

2. En la parte superior del árbol de agentes, haga clic en **Definir programación**.

3. Active la consulta programada.

4. Especifique el programa.
5. Haga clic en **Guardar**.

Compatibilidad con Trend Micro Virtual Desktop

Optimice la protección de un equipo de sobremesa virtual mediante la Compatibilidad con Trend Micro Virtual Desktop. Esta función regula las tareas en Agentes de OfficeScan que se hallen en un único servidor virtual.

Ejecutar varios equipos de sobremesa en un único servidor y realizar exploraciones libres o actualizaciones de componentes consume una cantidad considerable de los recursos del sistema. Utilice esta función para prohibir que los agentes ejecuten exploraciones o actualizaciones de componentes al mismo tiempo.

Por ejemplo, si un servidor de VMware vCenter tiene tres equipos de sobremesa virtuales que ejecutan los Agentes de OfficeScan, OfficeScan puede iniciar el proceso Explorar ahora e implementar las actualizaciones de forma simultánea en los tres agentes. Virtual Desktop Support reconoce que los agentes se encuentran en el mismo servidor físico. Virtual Desktop Support permite que una tarea se ejecute en el primer agente y la pospone para los otros dos hasta que el primer agente ha terminado dicha tarea.

El Soporte para Virtual Desktop puede utilizarse en las siguientes plataformas:

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

En el caso de administradores que utilizan otras aplicaciones de virtualización, el servidor de OfficeScan también puede actuar como un hipervisor emulado para administrar agentes virtuales.

Para obtener más información sobre estas plataformas, consulte los sitios Web de VMware View, Citrix XenDesktop o Microsoft Hyper-V.

Utilice la Herramienta de creación de plantillas de exploración previa de VDI de OfficeScan para optimizar exploraciones bajo petición o eliminar los GUID de las imágenes de base o doradas.

Instalación del Soporte para Virtual Desktop

El Soporte para Virtual Desktop es una característica nativa de OfficeScan, pero con licencia individual. Tras instalar el servidor de OfficeScan, esta característica está disponible, pero no operativa. La instalación de esta característica implica la descarga de un archivo desde el servidor de ActiveUpdate (o desde una fuente de actualización personalizada si se ha configurado alguna). Cuando dicho archivo se haya incorporado al servidor de OfficeScan, podrá activar el Soporte para Virtual Desktop con el fin de activar todas sus funciones. La instalación y la activación se realizan desde Plug-in Manager.

Nota

El Soporte para Virtual Desktop no es totalmente compatible en entornos en los que solo se utilice IPv6. Para conocer más detalles, consulte *Limitaciones de los servidores que solo utilizan IPv6 en la página A-3*.

Instalar el Soporte de Virtual Desktop

Procedimiento

1. Abra la consola Web de OfficeScan y haga clic en **Complementos** en el menú principal.

2. En la pantalla de **Plug-in Manager**, vaya a la sección **Compatibilidad con Trend Micro Virtual Desktop** y haga clic en **Descargar**.

   El tamaño del paquete se figura junto al botón **Descargar**.

   Plug-in Manager almacena el archivo descargado en <*carpeta de instalación del servidor*>`\PCCSRV\Download\Product`.

Nota

Si Plug-in Manager no puede descargar el archivo, lo vuelve a intentar de forma automática una vez transcurridas 24 horas. Para activar manualmente OfficeScan Plug-in Manager con el fin de que descargue el paquete, reinicie el servicio Plug-in Manager desde Microsoft Management Console.

3. Supervise el progreso de descarga. Puede ignorar la pantalla durante la descarga.

   Si tiene problemas durante la descarga del paquete, compruebe los registros de actualización del servidor en la consola de producto de OfficeScan. En el menú principal, haga clic en **Registros** > **Actualización del servidor**.

   Después de que Plug-in Manager haya descargado el archivo, el Soporte de Virtual Desktop se abrirá en una nueva pantalla.

   Nota

   Si no se visualiza el Soporte de Virtual Desktop, consulte los posibles motivos y sus soluciones en *Solución de problemas de Plug-in Manager en la página 17-13*.

4. Para instalar al instante la función Soporte de Virtual Desktop, haga clic en **Instalar ahora**. Para instalarlo después:

   a. Haga clic en **Instalar más tarde**.

   b. Abra la pantalla de **Plug-in Manager**.

   c. Vaya a la sección **Compatibilidad con Trend Micro Virtual Desktop** y haga clic en **Instalar**.

5. Lea el contrato de licencia y haga clic en **Aceptar** para aceptar las condiciones.

   Comienza la instalación.

6. Supervise el progreso de la instalación. Tras la instalación, se muestra la versión del Soporte de Virtual Desktop.

Licencia del Soporte para Virtual Desktop

Visualice, active y renueve la licencia del Soporte para Virtual Desktop desde Plug-in Manager.

Obtenga el código de activación de manos de Trend Micro y, después, utilícelo para activar toda la funcionalidad del Soporte para Virtual Desktop.

Activar o renovar el Soporte para Virtual Desktop

Procedimiento

1. Abra la consola Web de OfficeScan y haga clic en **Complementos** en el menú principal.
2. En la pantalla de **Plug-in Manager**, vaya a la sección **Compatibilidad con Trend Micro Virtual Desktop** y haga clic en **Administrar programa**.
3. Haga clic en **Ver información sobre la licencia**.
4. En la pantalla **Detalles de la licencia del producto** que se abre, haga clic en **Nuevo código de activación**.
5. Escriba el código de activación en la pantalla que se abre y haga clic en **Guardar**.
6. De nuevo en la pantalla Detalles de la licencia del producto, haga clic en **Información de la actualización** para actualizar la página con los detalles nuevos de la licencia y el estado de la función. Esta pantalla también muestra un enlace al sitio Web de Trend Micro en el que puede visualizar información detallada sobre la licencia.

Ver información sobre la licencia del Soporte para Virtual Desktop

Procedimiento

1. En el menú principal, abra la consola Web de OfficeScan y haga clic en **Complementos** > **[Soporte de Trend Micro Virtual Desktop] Administrar programa**.
2. Haga clic en **Ver información sobre la licencia**.
3. Vea los detalles de la licencia en la pantalla que se abre.

   En la sección Licencia del Soporte para Virtual Desktop se proporciona la siguiente información:

   - **Estado**: muestra "Activada", "No activada" o "Caducada".
   - **Versión**: muestra si la versión es "Completa" o "De prueba". Si tiene tanto la versión completa, como la de prueba, la versión se mostrará como "Completa".
   - **Fecha de vencimiento**: si el Soporte de Virtual Desktop tiene múltiples licencias, se muestra la fecha de vencimiento más reciente. Por ejemplo, si las fechas de caducidad son 31.12.10 y 30.06.10, aparecerá 31.12.10.
   - **N.º de licencias**: muestra cuántos Agentes de OfficeScan pueden utilizar Soporte de Virtual Desktop.
   - **Código de activación**: muestra el código de activación.

   Durante los casos siguientes aparecen recordatorios sobre las licencias:

   Si cuenta con una licencia de versión completa:

   - Durante el periodo de gracia de la función. La duración del periodo de gracia puede varía entre una zona y otra. Consulte con su representante de Trend Micro para comprobar la duración de su periodo de gracia.
   - Cuando la licencia caduca y finaliza el periodo de gracia. Durante este tiempo no podrá obtener asistencia técnica.

   Si cuenta con una licencia de versión de evaluación

- Cuando caduca la licencia. Durante este tiempo no podrá obtener asistencia técnica.

4. Haga clic en **Ver licencia detallada en línea** para ver información sobre su licencia en el sitio Web de Trend Micro.

5. Haga clic en **Actualizar información** para actualizar la pantalla con la información más reciente sobre la licencia.

Conexiones de Virtual Server

Optimice la exploración bajo petición o las actualizaciones de componentes agregando VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4) o Microsoft Hyper-V Server. Los servidores de OfficeScan se comunican con los servidores virtuales especificados para determinar los Agentes de OfficeScan que se encuentran en el mismo servidor físico.

En el caso de otros servidores VDI, el servidor de OfficeScan emula un hipervisor virtual para administrar agentes virtuales en otras plataformas. El hipervisor de OfficeScan procesa las solicitudes de cada agente virtual en el mismo orden en el que el servidor las recibe. El servidor de OfficeScan procesa una solicitud a la vez y pone el resto en una cola.

Añadir conexiones del servidor

Procedimiento

1. En el menú principal, abra la consola Web de OfficeScan y haga clic en **Complementos** > **[Soporte de Trend Micro Virtual Desktop] Administrar programa**.

2. Seleccione **Servidor de VMware vCenter**, **Citrix XenServer**, **Microsoft Hyper-V** u **Otras aplicaciones de virtualización**.

Nota

Si selecciona **Otras aplicaciones de virtualización**, no hará falta más información. El servidor de OfficeScan procesa las solicitudes del agente virtual en el mismo orden en el que el servidor las recibe.

3. Active la conexión con el servidor.
4. Especifique la siguiente información:
   - Para los servidores VMware vCenter y Citrix XenServer:
     - Dirección IP
     - Puerto
     - Protocolo de conexión (HTTP o HTTPS)
     - Nombre de usuario
     - Contraseña
   - Para los servidores Microsoft Hyper-V:
     - Nombre de host o dirección IP
     - Dominio\nombre de usuario

       Nota

       La cuenta de inicio de sesión debe ser una cuenta de dominio del grupo Administradores.

     - Contraseña
5. Active de forma opcional la conexión del proxy para VMware vCenter o Citrix XenServer.
   a. Especifique el nombre del servidor proxy o la dirección IP y el puerto.
   b. Si el servidor proxy necesita autenticación, especifique el nombre de usuario y la contraseña.
6. Haga clic en **Probar la conexión** para verificar que el servidor de OfficeScan se puede conectar correctamente al servidor.

Nota

Para obtener información sobre cómo solucionar problemas relacionados con las conexiones a Microsoft Hyper-V, consulte *Soluciones de problemas de las conexiones a Microsoft Hyper-V en la página 15-91*.

7. Haga clic en **Guardar**.

Añadir conexiones del servidor adicionales

Procedimiento

1. En el menú principal, abra la consola Web de OfficeScan y haga clic en **Complementos** > **[Soporte de Trend Micro Virtual Desktop] Administrar programa**.
2. Haga clic en **Agregar nueva conexión a vCenter**, **Agregar nueva conexión a XenServer** o **Agregar una nueva conexión a Hyper-V**.
3. Repita los pasos para proporcionar la información de servidor pertinente.
4. Haga clic en **Guardar**.

Eliminar una configuración de conexión

Procedimiento

1. En el menú principal, abra la consola Web de OfficeScan y vaya a **Complementos** > **[Soporte de Trend Micro Virtual Desktop] Administrar programa**.
2. Haga clic en **Eliminar esta conexión**.
3. Haga clic en **Aceptar** para confirmar que desea eliminar esta conexión.
4. Haga clic en **Guardar**.

Cambio de la capacidad de exploración VDI

Los administradores pueden aumentar el número de endpoints VDI que ejecutan escaneo simultáneo mediante la modificación del archivo `vdi.ini`. Trend Micro recomienda vigilar estrictamente el efecto de cambiar la capacidad de VDI para asegurar que los recursos del sistema puedan manejar cualquier aumento de exploración.

Procedimiento

1. En el equipo servidor de OfficeScan, vaya a <*Carpeta de instalación del servidor*>`PCCSRV\Private\vdi.ini`.
2. Busque el parámetro `[TaskController]`.

   Los parámetros TaskController son los siguientes:

   - Para clientes OfficeScan 10.5:

     ```
     [TaskController]

     Controller_00_MaxConcurrentGuests=1

     Controller_01_MaxConcurrentGuests=3
     ```

     Donde:

     - `Controller_00_MaxConcurrentGuests=1` es igual al número máximo de clientes que pueden realizar exploraciones simultáneamente.
     - `Controller_01_MaxConcurrentGuests=3` es igual al número máximo de clientes que pueden realizar actualizaciones simultáneamente.

   - Para clientes de OfficeScan 10.6 y agentes de OfficeScan 11.0 (o posterior):

     ```
     [TaskController]

     Controller_02_MaxConcurrentGuests=1

     Controller_03_MaxConcurrentGuests=3
     ```

     Donde:

     - `Controller_02_MaxConcurrentGuests=1` es igual al número máximo de clientes que pueden realizar exploraciones simultáneamente.

- `Controller_03_MaxConcurrentGuests=3` es igual al número máximo de clientes que pueden realizar actualizaciones simultáneamente.

3. Aumente o disminuya el recuento en cada controlador según sea necesario.

   El valor mínimo de todos los parámetros es 1.

   El valor máximo de todos los parámetros es 65536.

4. Guarde y cierre el archivo `vdi.ini`.

5. Reinicie el OfficeScan Master Service.

6. Supervise la CPU, la memoria y los recursos de uso del disco de los Endpoints de VDI. Modifique aún más la configuración del controlador para aumentar/disminuir el número de exploraciones simultáneas que mejor se adapte al entorno VDI repitiendo los pasos 1 a 5.

Soluciones de problemas de las conexiones a Microsoft Hyper-V

La conexión a Microsoft Hyper-V utiliza el Instrumental de administración de Windows (WMI) y DCOM para la comunicación entre el servidor y el agente. Las políticas del cortafuegos pueden bloquear esta comunicación, lo que provoca que no se establezca conexión con el servidor Hyper-V.

El puerto de escucha del servidor Hyper-V se establece de forma predeterminada en el 135 y, a continuación, selecciona un puerto configurado aleatoriamente para las comunicaciones adicionales. Si el cortafuegos bloquea el tráfico de WMI o cualquiera de estos dos puertos, no se podrá establecer comunicación con el servidor. Los administradores pueden modificar la política del cortafuegos para que permita la comunicación satisfactoria con el servidor Hyper-V.

Compruebe que todos los parámetros de conexión, incluida la dirección IP, el dominio/nombre de usuario y la contraseña, sean correctos antes de realizar las siguientes modificaciones en el cortafuegos.

Permitir la comunicación de WMI a través del Firewall de Windows

Procedimiento

1. En el servidor Hyper-V, abra la pantalla **Firewall de Windows - Programas permitidos**.

   En los sistemas Windows 2008 R2, desplácese a **Panel de control** > **Sistema y seguridad** > **Firewall de Windows** > **Permitir un programa o una característica a través de Firewall de Windows**.

2. Seleccione **Instrumental de administración de Windows (WMI)**.

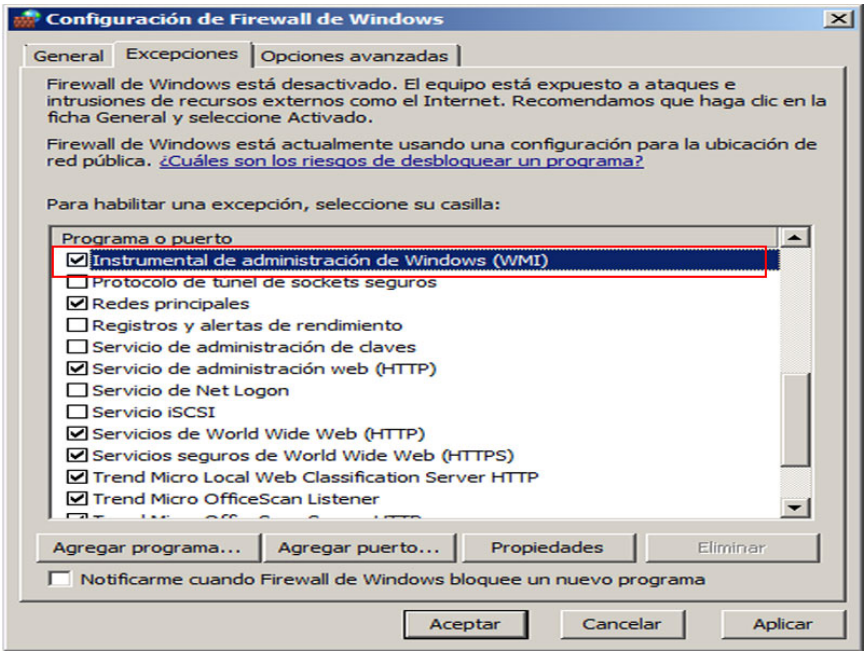


FIGURA 15-7. Pantalla Firewall de Windows - Programas permitidos

3. Haga clic en **Guardar**.

4. Pruebe de nuevo la conexión a Hyper-V.

Abrir la comunicación de puertos a través del Firewall de Windows o un cortafuegos de otros fabricantes

Procedimiento

1. En el servidor Hyper-V, asegúrese de que el cortafuegos permita la comunicación a través del puerto 135 y pruebe de nuevo la conexión a Hyper-V.

   Para obtener información sobre cómo abrir puertos, consulte la documentación del cortafuegos.

2. Si la conexión con el servidor Hyper-V se ha establecido correctamente, configure WMI para que utilice un puerto fijo.

   Para obtener información sobre la *configuración un puerto fijo para WMI*, consulte:

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Abra los puertos 135 y el puerto fijo creado recientemente (24158) para la comunicación a través del cortafuegos.

4. Pruebe de nuevo la conexión a Hyper-V.

Herramienta de creación de plantillas de exploración previa de VDI

Utilice la herramienta de creación de plantillas de exploración previa de VDI de OfficeScan para optimizar exploraciones bajo petición o eliminar los GUID de las imágenes de base o doradas. Esta herramienta explora la imagen de base o dorada y certifica la imagen. Cuando se exploran duplicados de la imagen, OfficeScan sólo comprueba las partes que han cambiado. Este proceso garantiza un menor tiempo de exploración.

Consejo

Trend Micro recomienda generar la plantilla de exploración previa después de aplicar una actualización de Windows o de instalar una nueva aplicación.

Crear una plantilla de exploración previa

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Seleccione una versión de la herramienta de creación de plantillas de exploración previa de VDI. Las versiones siguientes están disponibles:

   TABLA 15-10. Versiones de la herramienta de creación de plantillas de exploración previa de VDI

NOMBRE DEL ARCHIVO	INSTRUCCIÓN
TCacheGen.exe	Seleccione este archivo si desea ejecutar la herramienta directamente en una plataforma de 32 bits.
TCacheGen_x64.exe	Seleccione este archivo si desea ejecutar la herramienta directamente en una plataforma de 64 bits.
TCacheGenCli.exe	Seleccione este archivo si desea ejecutar la herramienta desde la interfaz de línea de comandos en una plataforma de 32 bits.
TCacheGenCli_x64.exe	Seleccione este archivo si desea ejecutar la herramienta desde la interfaz de línea de comandos en una plataforma de 64 bits.

3. Copie la versión de la herramienta que ha elegido en el paso anterior en el endpoint.

4. Ejecute la herramienta.

   - Para ejecutar la herramienta directamente:

a. Haga doble clic en `TCacheGen.exe` o `TCacheGen_x64.exe`.

b. Seleccione **Crear plantilla de exploración previa** y haga clic en **Siguiente**.

- Para ejecutar la herramienta desde la interfaz de la línea de comandos:

a. Abra el símbolo del sistema y cambie el directorio a `<carpeta de instalación del agente>`.

b. Escriba el siguiente comando:

```
TCacheGenCli Generate_Template
```

O

```
TcacheGenCli_x64 Generate_Template
```

Nota

La herramienta explora la imagen en busca de amenazas de seguridad antes de crear la plantilla de exploración previa y eliminar el GUID.

Tras crear la plantilla de exploración previa, la herramienta descarga el Agente de OfficeScan. No vuelva a cargar el Agente de OfficeScan. Si el Agente de OfficeScan se vuelve a cargar, tendrá que crear de nuevo la plantilla de exploración previa.

Eliminar GUID de las plantillas

Procedimiento

1. En el equipo del servidor de OfficeScan, vaya a <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Seleccione una versión de la herramienta de creación de plantillas de exploración previa de VDI. Las versiones siguientes están disponibles:

TABLA 15-11. Versiones de la herramienta de creación de plantillas de exploración previa de VDI

NOMBRE DEL ARCHIVO	INSTRUCCIÓN
TCacheGen.exe	Seleccione este archivo si desea ejecutar la herramienta directamente en una plataforma de 32 bits.
TCacheGen_x64.exe	Seleccione este archivo si desea ejecutar la herramienta directamente en una plataforma de 64 bits.
TCacheGenCli.exe	Seleccione este archivo si desea ejecutar la herramienta desde la interfaz de línea de comandos en una plataforma de 32 bits.
TCacheGenCli_x64.exe	Seleccione este archivo si desea ejecutar la herramienta desde la interfaz de línea de comandos en una plataforma de 64 bits.

3. Copie la versión de la herramienta que ha elegido en el paso anterior en el endpoint.

4. Ejecute la herramienta.

   - Para ejecutar la herramienta directamente:

     a. Haga doble clic en `TCacheGen.exe` o `TCacheGen_x64.exe`.

     b. Seleccione **Eliminar el GUID de la plantilla** y haga clic en **Siguiente**.

   - Para ejecutar la herramienta desde la interfaz de la línea de comandos:

     a. Abra el símbolo del sistema y cambie el directorio a `<carpeta de instalación del agente>`.

     b. Escriba el siguiente comando:

     ```
     TCacheGenCli Remove GUID
     ```

     O

     ```
     TcacheGenCli_x64 Remove GUID
     ```

Configuración global para los agentes

OfficeScan aplica la configuración general del agente a todos los agentes o solo a los agentes con ciertos derechos.

Procedimiento

1. Vaya a **Agentes** > **Configuración global para los agentes**.
2. Defina los siguientes valores de configuración:

TABLA 15-12. Configuración global para los agentes

PESTAÑA	PARÁMETRO	REFERENCIA
Configuración de seguridad	Configuración de la exploración	*Sección Configuración de la exploración en la página 7-78*
	Configuración de la exploración programada	*Sección Configuración de la exploración programada en la página 7-84*
	Configuración del cortafuegos	*Configuración general del cortafuegos en la página 13-26*
	Configuración de conexión sospechosa	*Configurar los ajustes de las listas de IP generales definidas por el usuario en la página 8-6*
	Configuración de la supervisión de comportamiento	*Configuración de las opciones de supervisión de comportamiento global en la página 9-13*

Pestaña	Parámetro	Referencia
System	Configuración del servicio de software seguro certificado	*Configuración general de la exploración en la página 7-76*
	Proxy del servicio Smart Protection	*Configurar los ajustes de proxy del servicio global de Smart Protection en la página 15-56*
	Actualizaciones	• *ActiveUpdate Server como el origen de actualización del agente de OfficeScan en la página 6-40* • *Configuración del espacio en disco reservado para las actualizaciones de los agentes de OfficeScan en la página 6-52*
	Reinicio de los servicio	*Reinicio del servicio Agente de OfficeScan en la página 15-12*
Red	Configuración del servidor proxy	*Configuración automática del proxy del agente de OfficeScan en la página 15-59*
	Dirección IP preferida	*Direcciones IP del agente en la página 5-12*
	Comunicación entre servidor y agente	*Cifrado mejorado para la comunicación entre servidor y agente en la página 14-63*
	Configuración del ancho de banda del registro de virus/malware	*Configuración general de la exploración en la página 7-76*
	Red no accesible	*Agentes no accesibles en la página 15-49*

PESTAÑA	PARÁMETRO	REFERENCIA
Control de agentes	Configuración general	*Configuración general de la exploración en la página 7-76*
	Configuración de las alertas	*Configuración de las notificaciones de actualización del agente de OfficeScan en la página 6-54*
	Configuración de idioma de agente	*Configuración de idioma del agente de OfficeScan en la página 15-23*

3. Haga clic en **Guardar**.

Configuración de derechos y otras configuraciones de los agentes

Conceda a los usuarios los derechos para modificar determinados parámetros de configuración y realizar tareas de alto nivel en el Agente de OfficeScan.

Nota

La configuración del antivirus solo parece tras activar la característica OfficeScan Antivirus.

Consejo

Para aplicar una configuración y políticas uniformes en toda la empresa, conceda derechos limitados a los usuarios.

Procedimiento

1. Vaya a **Agentes** > **Administración de agentes**.
2. En el árbol de agentes, haga clic en el icono del dominio raíz ( ) para incluir todos los agentes o seleccionar dominios o agentes específicos.
3. Haga clic en **Configuración** > **Derechos y otras configuraciones**.

4. En la pestaña **Derechos**, configure los siguientes derechos del usuario:

TABLA 15-13. Derechos del agente

DERECHOS DEL AGENTE	REFERENCIA
Derecho del modo independiente	*Derecho del modo independiente del Agente de OfficeScan en la página 15-20*
Derechos de exploración	*Derechos de tipo de exploración en la página 7-59*
Derechos de exploración programada	*Derechos y otras configuraciones de la exploración programada en la página 7-62*
Derechos del cortafuegos	*Derechos del cortafuegos en la página 13-24*
Privilegios de supervisión de comportamiento	*Privilegios de supervisión de comportamiento en la página 9-15*
Lista de programas de confianza	*Derechos de lista de programas de confianza en la página 7-74*
Derechos de exploración del correo	*Derechos y otras configuraciones de la exploración del correo en la página 7-68*
Derechos de configuración del proxy	*Derechos de configuración del proxy para agentes en la página 15-57*
Derechos de actualización de componentes	*Configurar los derechos y otras configuraciones de la actualización en la página 6-50*
Descargar y desbloquear	*Concesión del derecho de descarga y desbloqueo al agente en la página 15-20*
Desinstalación	*Conceder el derecho de desinstalación del agente de OfficeScan en la página 5-80*

5. Haga clic en la pestaña **Otras configuraciones** y configure los siguientes valores:

TABLA 15-14. Otras configuraciones del agente

PARÁMETRO	REFERENCIA
Configuración de actualización	*Configurar los derechos y otras configuraciones de la actualización en la página 6-50*
Configuración de la reputación Web	*Notificaciones de amenazas Web para usuarios del agente en la página 12-14*
Configuración de la supervisión de comportamiento	*Privilegios de supervisión de comportamiento en la página 9-15*
Configuración de alerta de contacto de C&C	*Notificaciones de C&C Contact Alert para los usuarios del agente en la página 12-19*
Configuración de alertas de Central Quarantine Restore	Muestra un mensaje de notificación en el endpoint tras restaurar un archivo en cuarentena.
Configuración del aprendizaje automático predictivo	Muestra un mensaje de notificación en el endpoint tras detectar una amenaza desconocida.
Autoprotección del agente de OfficeScan	*Autoprotección del agente de OfficeScan en la página 15-13*
Configuración de la exploración programada	*Concesión de derechos de exploración programada y visualización de la notificación de los derechos en la página 7-63*
Configuración de la caché para las exploraciones	*Configuración de la caché para las exploraciones en la página 7-70*
Configuración de la exploración del correo electrónico POP3	*Concesión de derechos de exploración de correo y habilitación de la exploración del correo POP3 en la página 7-69*
Restricción de acceso del agente de OfficeScan	*Restricción de acceso del agente de OfficeScan en la página 15-18*
Notificación de reinicialización	*Notificaciones de riesgos de seguridad para los usuarios del agente de OfficeScan en la página 7-94*

6. Si ha seleccionado dominios o agentes del árbol de agentes, haga clic en **Guardar**. En caso de que haya hecho clic en el icono del dominio raíz, seleccione alguna de las siguientes opciones:

   - **Aplicar a todos los agentes**: aplica la configuración a todos los agentes que ya existen y a los nuevos que se añadan a un dominio existente o futuro. Los futuros dominios son dominios todavía no creados en el momento en que haya realizado la configuración.
   - **Aplicar solo a futuros dominios**: aplica la configuración solo a los agentes que se añadan a futuros dominios. Esta opción no aplicará la configuración a los nuevos agentes que se añadan a un dominio existente.

Parte IV

Protección adicional

Capítulo 16

Protección de los agentes fuera de las instalaciones

En este capítulo se describen los pasos de instalación y configuración de Edge Relay Server que son necesarios para proteger los Agentes de OfficeScan que abandonen la intranet de la empresa.

Los temas que se incluyen son:

- *Edge Relay Server en la página 16-2*
- *Requisitos del sistema de Edge Relay Server en la página 16-3*
- *Instalación de Edge Relay Server en la página 16-4*
- *Conexión con Edge Relay Server en la página 16-13*
- *Administración de la conexión de Edge Relay Server en la página 16-14*
- *Administración de certificados de Edge Relay Server en la página 16-16*

Edge Relay Server

OfficeScan Edge Relay Server ofrece a los administradores visibilidad y mayor protección de los endpoints que los usuarios emplean fuera de la intranet de la compañía. La instalación de Edge Relay Server en la red perimetral permite a los Agentes de OfficeScan que se encuentran fuera de las instalaciones que no puedan establecer una conexión funcional con el servidor de OfficeScan realizar las tareas de la siguiente tabla.

Importante

Edge Relay Server no admite la comunicación IPv6.

TAREA	DESCRIPCIÓN
Sincronización de listas de objetos sospechosos	Edge Relay Server recibe las listas de objetos sospechosos actualizadas del servidor de OfficeScan en función de la programación configurada y las distribuye a los agentes fuera de las instalaciones. Para obtener más información, consulte *Configuración de la lista de objetos sospechosos en la página 14-34*.
Envío de muestras	Los agentes fuera de las instalaciones que detecten una amenaza desconocida pueden enviar el objeto sospechoso a la instancia configurada de Analizador virtual. El envío de objetos sospechosos de los agentes fuera de las instalaciones a Analizador virtual se produce del siguiente modo: 1. Los agentes fuera de las instalaciones envían el objeto a Edge Relay Server. 2. Edge Relay Server transfiere el objeto al servidor de OfficeScan durante la siguiente sincronización configurada. 3. A continuación, el servidor de OfficeScan transfiere el objeto a Analizador virtual para su análisis. Para obtener más información, consulte *Envío de muestras en la página 8-9*.

Tarea	Descripción
Envío de registros	Edge Relay Server recopila registros de los agentes fuera de las instalaciones y envía los datos de los registros de forma periódica al servidor de OfficeScan según la programación configurada.
Informe de estado	Los agentes fuera de las instalaciones envían actualizaciones de estado a Edge Relay Server, como las versiones actuales de patrones y componentes.

Tras configurar Edge Relay Server, los Agentes de OfficeScan reciben los ajustes e informan automáticamente a Edge Relay Server cuando no se puede establecer la conexión con el servidor de OfficeScan.

La comunicación entre Edge Relay Server, el servidor de OfficeScan y los Agentes de OfficeScan se cifra mediante la autenticación de certificado.

Para obtener más información, consulte *Administración de certificados de Edge Relay Server en la página 16-16*.

Requisitos del sistema de Edge Relay Server

Antes de instalar Edge Relay Server, asegúrese de que el equipo del servidor de destino cumple los requisitos mínimos del sistema.

Recurso	Requisitos
Procesador	Núcleo doble de 2 GHz
Memoria	4 GB
Espacio en disco	50 GB
Sistema operativo	Windows Server 2012 R2

Recurso	Requisitos

Tarjeta de red	• 2 tarjetas de red
	  • Una para la conexión con la intranet del servidor de OfficeScan
	  • Otra para la conexión externa con los Agentes de OfficeScan fuera de las instalaciones
	• 1 tarjeta de red configurada para usar puertos diferentes para conexiones de intranet e Internet

Base de datos	• SQL Server™ 2008 R2 Express (o posterior) • SQL Server™ 2008 R2 (o posterior) **Nota** El programa de instalación de OfficeScan Edge Relay Server ofrece la opción de instalar SQL Server 2014 SP2 Express durante la instalación.

Instalación de Edge Relay Server

Antes de instalar Edge Relay Server, asegúrese de que el equipo del servidor de destino cumple los requisitos mínimos del sistema.

Para obtener más información, consulte *Requisitos del sistema de Edge Relay Server en la página 16-3*.

Importante

Edge Relay Server no admite la comunicación IPv6.

Procedimiento

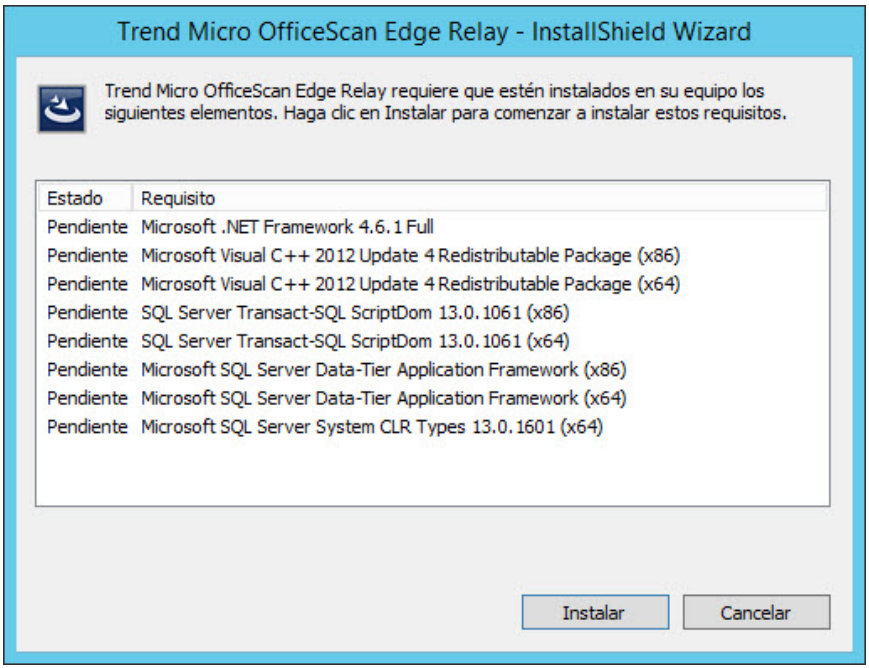
1. Busque la <*carpeta de instalación del servidor*>`\PCCSRV\Admin\Utility\EdgeServer` en el equipo del servidor de OfficeScan y cópiela en el equipo de Edge Relay Server de destino.

2. En el Edge Relay Server de destino, abra la carpeta `EdgeServer` y ejecute el archivo `setup.exe` para iniciar el proceso de instalación.

   El paquete de instalación buscará los componentes necesarios en el servidor.

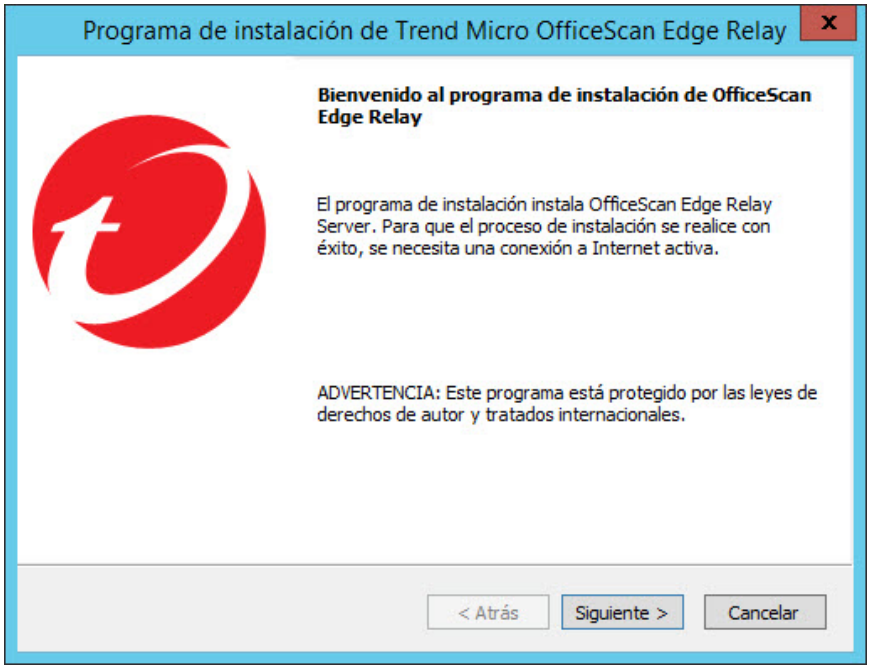
3. Si alguno de los siguientes componentes no se encuentra en el servidor, haga clic en **Instalar** para permitir que el programa de instalación instale los componentes que faltan durante el proceso de instalación de Edge Relay Server.

   - Microsoft .NET Framework 4.5 Completo
   - Microsoft Visual C++ 2012 Update 4 Redistributable Package (x64)
   - Microsoft SQL Server System CLR Types 10.00.2531 (x64)
   - SQL Server Transact-SQL ScriptDom (x64)
   - Microsoft SQL Server Data-Tier Application Framework (x64)



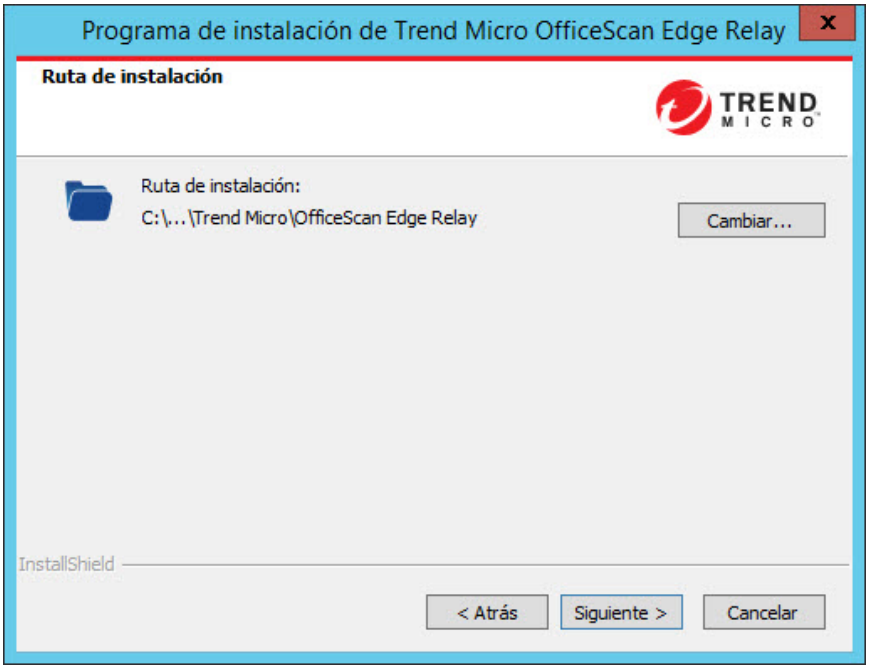
Aparecerá la pantalla de bienvenida.

4. Haga clic en **Siguiente**.



Aparecerá la pantalla **Ruta de instalación**.

5. Acepte el directorio de instalación predeterminado o haga clic en **Cambiar...** para seleccionar otra ubicación.



6. Haga clic en **Siguiente>**.

   Aparecerá la pantalla **Edge Relay Server: conexión del agente de OfficeScan**.

7. Especifique las opciones siguientes que usarán los Agentes de OfficeScan fuera de las instalaciones para conectarse a Edge Relay Server:

   - **Nombre de dominio completo (FQDN)**: escriba el FQDN de Edge Relay Server.
   - **Dirección IP**: seleccione el formato de la dirección IP.

     Importante

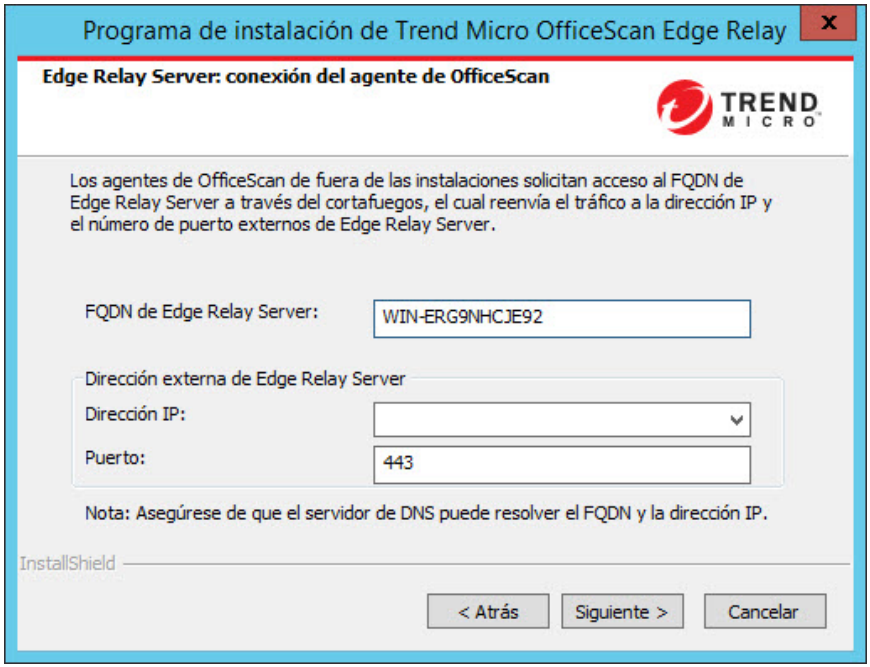
     Edge Relay Server no admite la comunicación IPv6.

   - **Puerto**: acepte el puerto predeterminado o especifique otro.

Importante

Debe configurar el cortafuegos y la puerta de enlace para permitir:

- La redirección de la comunicación del agente de OfficeScan desde Internet hasta Edge Relay Server.
- La comunicación a través del puerto indicado.



8. Haga clic en **Siguiente>**.

   Aparecerá la pantalla **Edge Relay Server: conexión del servidor de OfficeScan**.

9. Especifique las opciones siguientes que usará el servidor de OfficeScan para conectarse a Edge Relay Server:

   - **Dirección IP**: seleccione el formato de la dirección IP.

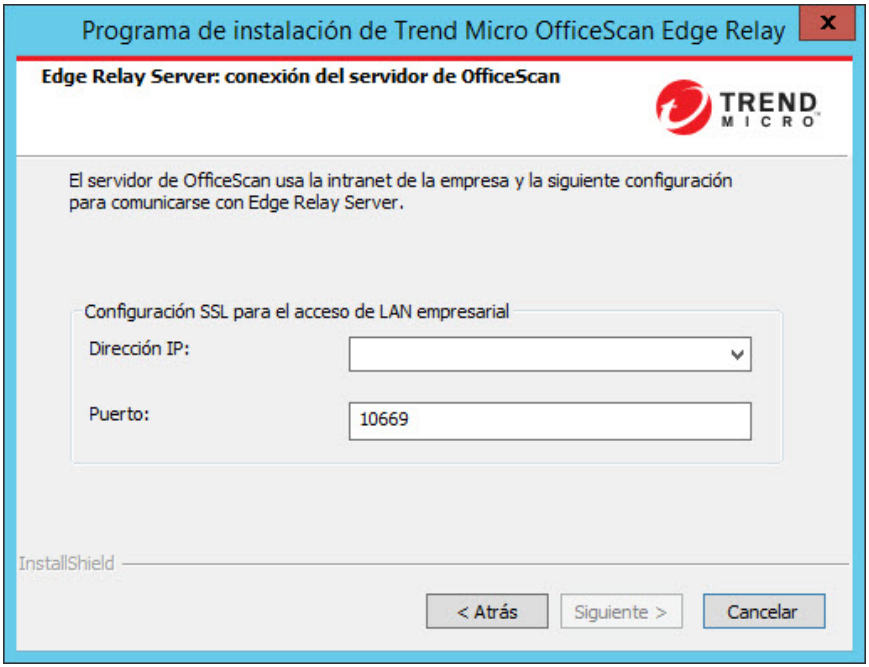
Importante

Edge Relay Server no admite la comunicación IPv6.

- **Puerto**: acepte el puerto predeterminado o especifique otro.

Importante

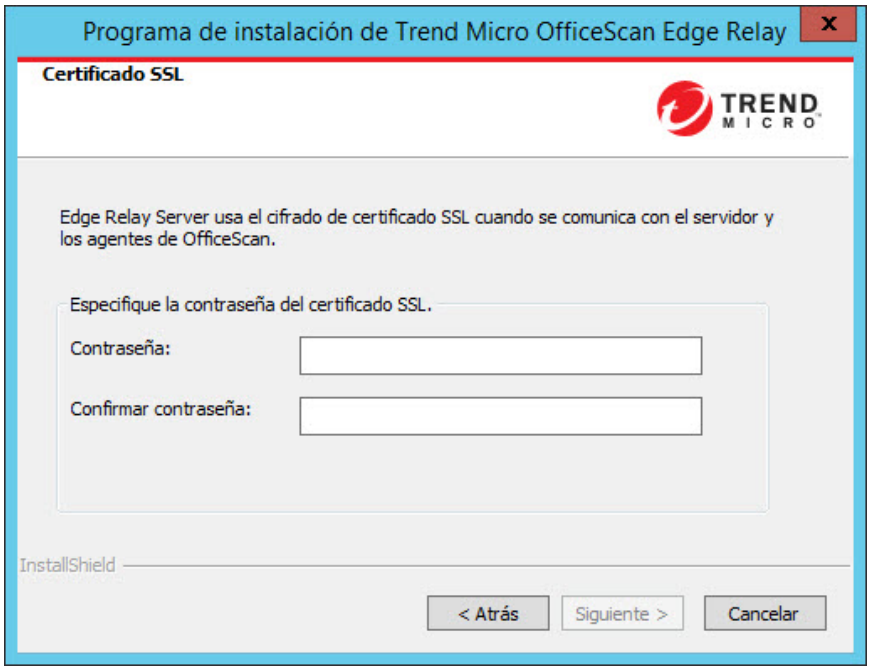
- El puerto del servidor de OfficeScan no puede ser el mismo que el puerto configurado para los Agentes de OfficeScan fuera de las instalaciones.
- Asegúrese de que el cortafuegos permite la comunicación a través del puerto especificado.



10. Haga clic en **Siguiente>**.

Aparecerá la pantalla **Certificado SSL**.

11. Especifique y confirme la contraseña utilizada para el certificado de Edge Relay Server.



12. Haga clic en **Siguiente>**.

    Aparecerá la pantalla **Servidor de base de datos**.

13. Especifique la base de datos de SQL Server usada por Edge Relay Server:

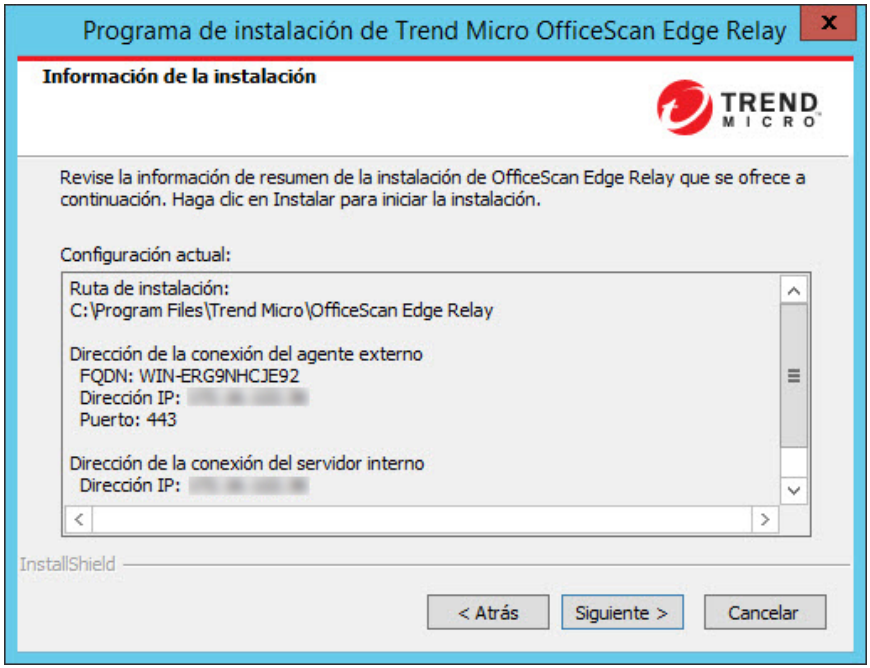
    - **Instalar una nueva instancia de SQL Server 2008 R2 SP2 Express**
    - **Usar un servidor de base de datos SQL existente**: haga clic en **Examinar...** para seleccionar uno de los servidores disponibles en la lista.

14. Especifique la contraseña utilizada para conectarse a la base de datos de SQL Server. Si instala una nueva base de datos de SQL Server Express, confirme la contraseña.

15. Haga clic en **Siguiente>**.

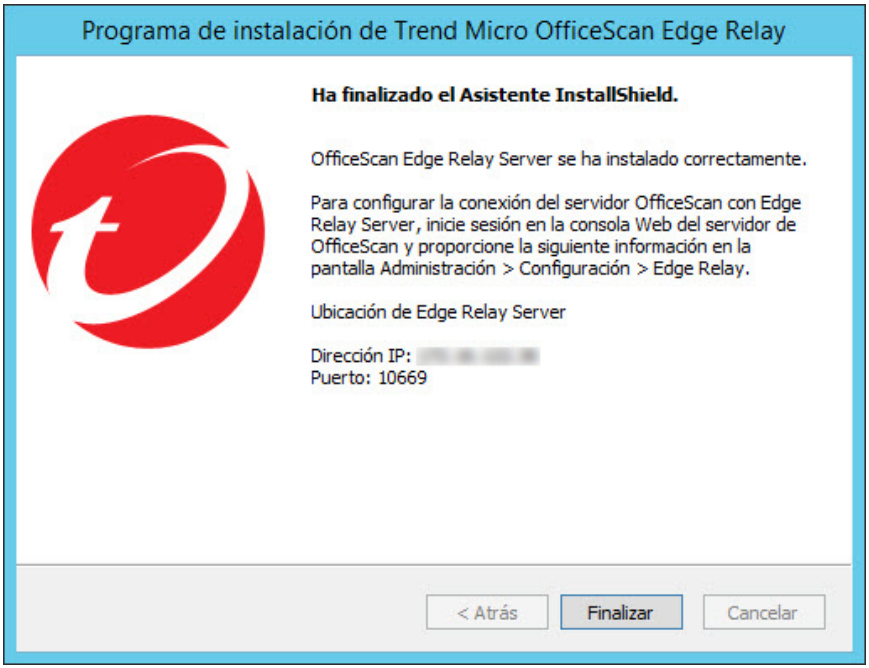
    Aparecerá la pantalla **Información de la instalación**.

16. Haga clic en **Siguiente >** para empezar la instalación.



Cuando finalice la instalación, aparecerá la pantalla **Ha finalizado el Asistente InstallShield**.

17. Por último, haga clic en **Finalizar**.



Edge Relay Server estará listo para usarse. Puede configurar el servidor de OfficeScan para que se conecte con Edge Relay Server.

Para obtener más información, consulte *Conexión con Edge Relay Server en la página 16-13*.

Conexión con Edge Relay Server

Tras instalar Edge Relay Server, debe configurar la configuración de conexión de Edge Relay Server en el servidor de OfficeScan. Tras conectarse a Edge Relay Server, los Agentes de OfficeScan que informan al servidor de OfficeScan recibirán la configuración de conexión y podrán comunicarse automáticamente con Edge Relay Server tras abandonar la intranet empresarial.

Procedimiento

1. En la consola Web de OfficeScan, vaya a **Administración** > **Configuración** > **Edge Relay**.

   Aparecerá la pantalla **Configuración de Edge Relay**.

2. Escriba la **Dirección IP** y el **Puerto** de Edge Relay Server.

   Nota

   Asegúrese de que introduce la dirección IP y el puerto que configuró para la comunicación de la intranet con Edge Relay Server.

3. Si el entorno requiere un servidor proxy para comunicarse con Edge Relay Server en la red perimetral, habilite **Conectarse mediante la configuración del servidor proxy externo**.

   Para configurar la configuración del proxy externo, haga clic en **Configuración del servidor proxy externo** para ir a la pantalla **Configuración del proxy**. Configure la información del proxy necesaria en la sección **Actualizaciones del servidor de OfficeScan**.

   Para obtener más información, consulte *Configurar el proxy en la página 6-21*.

4. Haga clic en **Conectar**.

   Cuando se conecte correctamente a Edge Relay Server, la pantalla se actualizará con la información de la conexión.

   Para obtener más información, consulte *Administración de la conexión de Edge Relay Server en la página 16-14*.

Administración de la conexión de Edge Relay Server

Tras conectarse a Edge Relay Server, los Agentes de OfficeScan que informan al servidor de OfficeScan recibirán la configuración de conexión y podrán comunicarse

automáticamente con Edge Relay Server tras abandonar la intranet empresarial. A continuación, podrá supervisar el estado de conexión de Edge Relay Server, configurar la programación de sincronización y realizar una sincronización inmediata desde la pantalla **Configuración de Edge Relay**.

Procedimiento

1. En la consola Web de OfficeScan, vaya a **Administración** > **Configuración** > **Edge Relay**.

   Aparecerá la pantalla **Configuración de Edge Relay**.

2. Supervise o configure los ajustes de Edge Relay Server.

PARÁMETRO	DESCRIPCIÓN
Dirección IP	La dirección IP actual de Edge Relay Server. Para configurar los nuevos ajustes de conexión de Edge Relay Server, haga clic en **Desconectar** y vuelva a configurarlos. Para obtener más información, consulte *Conexión con Edge Relay Server en la página 16-13*.
Estado	El estado de conexión «Conectado» o «Desconectado» entre el servidor de OfficeScan y Edge Relay Server.
Sincronizado	La última vez que Edge Relay Server se sincronizó con el servidor de OfficeScan. Haga clic en **Sincronizar ahora** para realizar una sincronización inmediata entre el servidor de OfficeScan y Edge Relay Server.
Sincronización programada	La frecuencia con la que se sincronizan el servidor de OfficeScan y Edge Relay Server. Según las características del ancho de banda, defina la frecuencia de sincronización como **Cada hora** o **Cada 15 minutos**.

3. Haga clic en **Guardar**.

Administración de certificados de Edge Relay Server

OfficeScan ofrece una herramienta de línea de comandos que le permite crear o renovar el certificado de Edge Relay Server que usan los agentes para comunicarse. Tras crear un certificado nuevo, Edge Relay Server lo envía al servidor de OfficeScan que, a continuación, lo implementa en los agentes cuando estos se conectan al servidor de OfficeScan.

Importante

Los Agentes de OfficeScan fuera de las instalaciones se deben conectar al servidor de OfficeScan para obtener el nuevo certificado de Edge Relay Server. Los agentes fuera de las instalaciones que no reciban el certificado actualizado ya no podrán comunicarse con Edge Relay Server hasta que se conecten al servidor de OfficeScan.

Procedimiento

1. En Edge Relay Server, abra un editor de línea de comandos y diríjase al siguiente directorio:

   ```
   C:\Archivos de programa\Trend Micro\OfficeScan Edge
   \OfcEdgeSvc\web\service
   ```

2. Ejecute la herramienta de certificados ejecutando el siguiente comando:

   `OfcEdgeCfg.exe --renewcert -certpwd <password>`

   Donde:

   - **`--renewcert`**: crea el certificado nuevo.
   - **`-certpwd <password>`**: especifica la contraseña del paquete de certificados.

   Edge Relay Server crea el nuevo paquete de certificados y lo envía automáticamente al servidor de OfficeScan. El servidor de OfficeScan implementa el nuevo

certificado en los Agentes de OfficeScan la próxima vez que los Agentes de OfficeScan informan al servidor de OfficeScan.

Capítulo 17

Uso de Plug-in Manager

En este capítulo se explica cómo configurar Plug-in Manager y ofrece una visión general de soluciones de complementos que se proporcionan con Plug-in Manager.

Los temas que se incluyen son:

- *Acerca de Plug-in Manager en la página 17-2*
- *Instalación de Plug-in Manager en la página 17-3*
- *Administrar las características nativas de OfficeScan en la página 17-4*
- *Administración de Programas de complemento en la página 17-5*
- *Desinstalación de Plug-in Manager en la página 17-12*
- *Solución de problemas de Plug-in Manager en la página 17-13*

Acerca de Plug-in Manager

OfficeScan incluye un marco llamado Plug-in Manager que integra nuevas soluciones al entorno de OfficeScan existente. Para facilitar la administración de estas soluciones, Plug-in Manager ofrece datos de un vistazo para las soluciones en forma de componentes.

Nota

Actualmente ninguna de las soluciones de complemento es compatible con IPv6. El servidor puede descargar estas soluciones, pero no podrá implementar las soluciones en hosts o Agentes de OfficeScan que solo utilizan IPv6.

Plug-in Manager ofrece estas características:

- **Características del producto nativas**

  Algunas características nativas de OfficeScan cuentan con licencia individual y se activan a través de Plug-in Manager. En esta versión, hay dos características que entran en esta categoría, que son el **Soporte para Trend Micro Virtual Desktop** y la **protección de datos de OfficeScan**.

- **Programas de complemento**

  Los programas de complemento no son parte del programa de OfficeScan. Los programas de complemento tienen licencias y consolas de administración independientes. Acceda a las consolas de administración desde la OfficeScan Web Console. **Trend Micro OfficeScan ToolBox** y **Seguridad de Trend Micro (para Mac)** son ejemplos de programas de complemento.

- **Pestañas y componentes de la consola**

  La pantalla **Panel** de OfficeScan requiere que Plug-in Manager muestre las pestañas y los componentes usados para supervisar el estado de protección del servidor y los agentes de OfficeScan.

Este documento ofrece información general de la instalación y la administración de los programas de complemento y aborda los datos de estos programas disponibles en los

componentes. Consulte la documentación del programa de complemento específico para obtener más información sobre su configuración y administración.

Agentes o Endpoints del programa de complemento

Algunos programas de complemento (como Seguridad de Trend Micro (para Mac)) cuentan con agentes que se instalan en los sistemas operativos Windows de los endpoints. Plug-in Manager del Agente de OfficeScan, que se ejecuta con el nombre de proceso `CNTAoSMgr.exe`, administra estos agentes.

OfficeScan instala `CNTAoSMgr.exe` con el Agente de OfficeScan. El único requisito adicional del sistema para `CNTAoSMgr.exe` es Microsoft XML Parser (MSXML) versión 3.0 o posterior.

Nota

Otros programas de complemento tienen agentes que no se instalan en sistemas operativos Windows y que no se gestionan desde Plug-in Manager del Agente de OfficeScan. El agente de Seguridad de Trend Micro (para Mac) es un ejemplo de estos agentes.

Componentes

Utilice los componentes para obtener una visión general de los datos de las soluciones de complemento implementadas. Los componentes se encuentran disponibles en la pantalla **Panel** del servidor de OfficeScan. **OfficeScan y Plug-ins Mashup** es un componente especial que combina los datos de los Agentes de OfficeScan y los soluciones de complemento instalados y, luego, presenta los datos en un árbol de agentes.

Este Manual del administrador ofrece información general de los componentes y de las soluciones que admiten componentes.

Instalación de Plug-in Manager

En las versiones anteriores de Plug-in Manager, el paquete de instalación se descarga desde Trend Micro ActiveUpdate Server y, luego, se instala en el equipo que aloja al

servidor de OfficeScan. En esta versión, el paquete de instalación se incluye en la siguiente ubicación del servidor de OfficeScan:

<*Carpeta de instalación del servidor*>\PCCSRV\Admin\Utility\PLM\PLMSetup.exe

Ejecute el archivo `PLMSetup.exe` para instalar Plug-in Manager.

Los nuevos usuarios de OfficeScan tendrán tanto el servidor de OfficeScan como Plug-in Manager instalados tras completar la instalación de OfficeScan. Los usuarios que actualicen a esta versión de OfficeScan y hayan utilizado Plug-in Manager anteriormente deberán detener el servicio Plug-in Manager antes de ejecutar el paquete de instalación.

Realizar las tareas posteriores a la instalación

Realice las siguientes acciones tras instalar Plug-in Manager:

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. Administre las soluciones de complemento.
3. Acceda al panel **Panel** de la OfficeScan Web Console para administrar los componentes para las soluciones de complemento.

Administrar las características nativas de OfficeScan

Las características nativas de OfficeScan se instalan con OfficeScan y los administradores pueden activarlas mediante Plug-in Manager. Administre algunas características, como el soporte de Trend Micro Virtual Desktop, a través de Plug-in Manager, y otras, como la protección de datos de OfficeScan, desde la consola Web de OfficeScan.

Administración de Programas de complemento

Instale y active los programas de complemento de forma independiente a OfficeScan. Cada complemento cuenta con su propia consola para la administración del producto. Se puede acceder a las consolas de administración desde la OfficeScan Web Console.

Instalación de los programas de complemento

Los programas de complemento aparecen en la consola de **Plug-in Manager**. Utilice la consola para descargar, instalar y administrar los programas. Plug-in Manager descarga los paquetes de instalación de un programa de complemento desde el servidor ActiveUpdate de Trend Micro o desde una fuente de actualización personalizada, siempre que se haya configurado una de forma correcta. Es necesaria una conexión a Internet para descargar el paquete desde el servidor de ActiveUpdate.

Cuando Plug-in Manager descarga un paquete de instalación o inicia una instalación, desactiva temporalmente otras funciones de programa de complemento como descargas, instalaciones y actualizaciones.

Plug-in Manager no admite la instalación de programas de complemento ni su administración desde la función de inicio de sesión único de Trend Micro Control Manager.

Instalación de Programas de complemento

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Descargar**.

   El tamaño del paquete de programas de complemento figura junto al botón **Descargar**. Plug-in Manager almacena el paquete descargado en `<Carpeta de instalación del servidor>\PCCSRV\Download\Product`.

Plug-in Manager almacena el paquete descargado en `<Carpeta de instalación del servidor>\PCCSRV\Download\Product`

Supervise el progreso o ignore la pantalla durante la descarga.

Nota

Si OfficeScan encuentra problemas durante la descarga o la instalación del paquete, compruebe los registros de actualización del servidor en la OfficeScan Web Console. En el menú principal, haga clic en **Registros** > **Actualización del servidor**.

3. Haga clic en **Instalar ahora** o **Instalar más tarde**.

   - Tras hacer clic en **Instalar ahora**, se inicia la instalación y aparece la pantalla del progreso de la instalación.
   - Tras hacer clic en **Instalar más tarde**, aparece la pantalla **Plug-in Manager**.

     Instale el programa de complemento haciendo clic en el botón **Instalar** que se encuentra en la sección del programa de complemento en la pantalla **Plug-in Manager**.

   Aparecerá la pantalla **Contrato de licencia para usuario final de Trend Micro**.

   Nota

   No todos los programas de complemento tienen esta pantalla. Si esta pantalla no aparece, se inicia la instalación del programa de complemento.

4. Haga clic en **Acepto** para instalar el programa de complemento.

   Supervise el progreso o ignore la pantalla durante la instalación.

   Nota

   Si OfficeScan encuentra problemas durante la descarga o la instalación del paquete, compruebe los registros de actualización del servidor en la OfficeScan Web Console. En el menú principal, haga clic en **Registros** > **Actualización del servidor**.

Tras la instalación, se muestra la versión actual del programa de complemento en la pantalla **Plug-in Manager**.

Activación de la licencia del Programa de complemento

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Administrar programa**.

   Aparecerá la pantalla **Nuevo código de activación de la licencia del producto**.
3. Escriba o copie y pegue el código de activación en los campos de texto.
4. Haga clic en **Guardar**.

   Aparecerá la consola del complemento.

Ver y renovar la información sobre la licencia

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Administrar programa**.
3. Vaya al hipervínculo **Ver información sobre la licencia** de la consola del complemento.

   No todos los programas de complemento muestran el hipervínculo **Ver información sobre la licencia** en el mismo sitio. Consulte la documentación del usuario del programa de complemento para obtener más información.

4. Vea los siguientes detalles de la licencia en la pantalla que se abre.

Opción	Descripción
Estado	Muestra "Activada", "No activada" o "Caducada".
Versión	Muestra versión "Completa" o de "Evaluación". **Nota** La activación de las versiones completa y de evaluación se muestra solo como "Completa".
N.º de licencias	Muestra cuántos endpoints el programa de complemento puede administrar.
La licencia caduca el	Si el programa de complemento tiene varias licencias, se muestra la fecha de caducidad de mayor duración. Por ejemplo, si las fechas de caducidad son 31.12.11 y 30.06.11, aparecerá 31.12.11.
Código de activación	muestra el código de activación
Recordatorios	En función de la versión de licencia actual, el complemento muestra recordatorios acerca de la fecha de caducidad de la licencia durante el periodo de gracia (solo para las versiones completas) o en el momento en que expire.

Nota

La duración del periodo de gracia puede varía entre una zona y otra. Consulte a un representante de Trend Micro acerca del período de gracia de un programa de complemento.

Una vez que caduca la licencia de un programa de complemento, el complemento continúa funcionando pero las actualizaciones y la asistencia ya no estarán disponibles.

5. Haga clic en **Ver licencia detallada en línea** para ver información sobre la licencia actual en el sitio Web de Trend Micro.

6. Haga clic en **Actualizar información** para actualizar la pantalla con la información más reciente sobre la licencia.

7. Haga clic en **Nuevo código de activación** para abrir la pantalla **Nuevo código de activación de la licencia del producto**.

   Para conocer más detalles, consulte *Activación de la licencia del Programa de complemento en la página 3-4*.

Gestión de los programas de complemento

Configure los parámetros y realice tareas relacionadas con los programas desde la consola de administración de los programas de complemento, a la que se puede acceder a través de la consola OfficeScan Web. Estas tareas incluyen la activación del programa y la implementación potencial de los agentes del programa de complemento en los endpoints. Consulte la documentación del programa de complemento específico para obtener información sobre su configuración y administración.

Administración de Programas de complemento

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Administrar programa**.

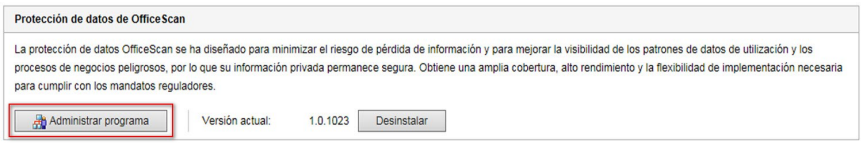


FIGURA 17-1. Botón Administrar programa

Cuando se administra el programa de complemento por primera vez, es posible que haya que activarlo. Para conocer más detalles, consulte *Activación de la licencia del Programa de complemento en la página 3-4*.

Actualizaciones del Programa de complemento

Las versiones nuevas de los programas de complemento instalados aparecen en la consola de Plug-in Manager. Descargue el paquete y actualice el programa de complemento en la consola. Plug-in Manager descarga el paquete desde el servidor ActiveUpdate de Trend Micro o desde una fuente de actualización personalizada, siempre que se haya configurado una de forma correcta. Es necesaria una conexión a Internet para descargar el paquete desde el servidor de ActiveUpdate.

Cuando Plug-in Manager descarga un paquete de instalación o inicia una actualización, desactiva temporalmente otras funciones del programa de complemento como descargas, instalaciones y actualizaciones.

Plug-in Manager no admite la actualización de programas de complemento mediante la función de inicio de sesión único de Trend Micro Control Manager.

Actualizar Programas de complemento

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Descargar**.

   El tamaño del paquete de actualización figura junto al botón **Descargar**.

   Supervise el progreso o ignore la pantalla durante la descarga.

   Nota

   Si OfficeScan encuentra problemas durante la descarga o la instalación del paquete, compruebe los registros de actualización del servidor en la OfficeScan Web Console. En el menú principal, haga clic en **Registros** > **Actualización del servidor**.

3. Cuando Plug-in Manager descarga el paquete, se muestra una nueva pantalla.
4. Haga clic en **Actualizar ahora** o **Actualizar más tarde**.

- Tras hacer clic en **Actualizar ahora**, se inicia la descarga y aparece la pantalla del progreso de la actualización.
- Tras hacer clic en **Actualizar más tarde**, aparece la pantalla **Plug-in Manager**.

  Haga clic en el botón **Actualizar** que se encuentra en la sección del programa de complemento en la pantalla **Plug-in Manager** para actualizar el programa de complemento.

Tras la actualización, es posible que deba reiniciar el servicio Plug-in Manager, por lo que la pantalla **Plug-in Manager** no estará disponible temporalmente. Cuando la pantalla vuelve a estar disponible, se visualiza la versión actual del programa de complemento.

Desinstalación del Programa de complemento

Desinstale un programa de complemento de las siguientes formas:

- Desinstalar el programa de complemento desde la consola de Plug-in Manager:
- Desinstale el servidor de OfficeScan, lo cual conlleva la desinstalación de Plug-in Manager y todos los programas de complemento instalados. Para obtener más instrucciones acerca del servidor de OfficeScan, consulte *Manual de instalación y actualización de OfficeScan*.

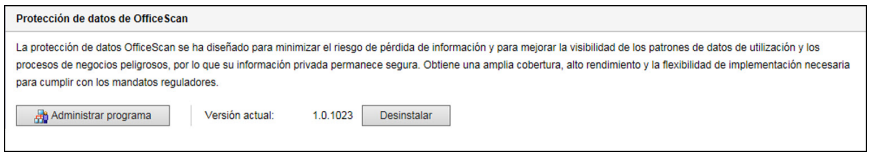
En el caso de programas de complemento con agentes en el endpoint:

- Consulte la documentación del programa de complemento para saber si la desinstalación del programa de complemento también desinstala el agente del complemento.
- En el caso de agentes del complemento instalados en el mismo endpoint que el Agente de OfficeScan, la desinstalación del Agente de OfficeScan también implica la desinstalación de los agentes del complemento y de Plug-in Manager del Agente de OfficeScan (`CNTAoSMgr.exe`).

Desinstalación del programa de complemento desde la consola de Plug-in Manager

Procedimiento

1. En el menú principal, abra la OfficeScan Web Console y haga clic en **Complementos**.
2. En la pantalla de **Plug-in Manager**, vaya a la sección del programa de complemento y haga clic en **Desinstalar**.



3. Supervise el progreso de desinstalación o ignore la pantalla durante la desinstalación.
4. Actualice la pantalla de **Plug-in Manager** después de la desinstalación.

   El programa de complemento vuelve a estar disponible para la instalación.

Desinstalación de Plug-in Manager

Desinstale el servidor de OfficeScan para desinstalar Plug-in Manager y todos los programas de complemento instalados. Para obtener más instrucciones acerca del servidor de OfficeScan, consulte *Manual de instalación y actualización de OfficeScan*.

Solución de problemas de Plug-in Manager

Busque la información de depuración de Plug-in Manager y los programas de complemento en los registros de depuración del servidor de OfficeScan y el Agente de OfficeScan.

El programa de complemento no aparece en la consola de Plug-in Manager.

Puede que cualquier programa de complemento disponible para descarga e instalación no aparezca en la consola de Plug-in Manager por las siguientes razones:

Procedimiento

1. Plug-in Manager todavía está descargando el programa de complemento, proceso que puede tardar algún tiempo si el tamaño del paquete del programa es muy grande. Compruebe la pantalla de vez en cuando para ver si se visualiza el programa de complemento.

   Nota

   Si Plug-in Manager no puede descargar el programa de complemento, se vuelve a descargar de forma automática tras 24 horas. Para activar Plug-in Manager de forma manual para que descargue el programa de complemento, reinicie el servicio OfficeScan Plug-in Manager.

2. El equipo servidor no se puede conectar a Internet. Si el servidor se conecta a Internet a través de un servidor proxy, asegúrese de que la conexión pueda establecerse mediante la configuración del proxy.

3. La fuente de actualización de OfficeScan no es el servidor ActiveUpdate. En la consola Web de OfficeScan, vaya a **Actualizaciones** > **Servidor** > **Origen de actualización** y marque el origen de actualización. Si la fuente de actualización no es el servidor ActiveUpdate, tiene las siguientes opciones:

   - Seleccione el servidor ActiveUpdate como fuente de actualización.

- Si selecciona **Otra fuente de actualización**, seleccione la primera entrada de la lista de **fuentes de actualización Otras** y compruebe que se puede conectar correctamente al servidor ActiveUpdate. Plug-in Manager solo es compatible con la primera entrada de la lista.
- Si selecciona **Ubicación de la intranet que contiene una copia del archivo actual**, asegúrese de que el endpoint de la intranet también pueda conectarse a ActiveUpdate Server.

Problemas de instalación y visualización del agente del complemento en endpoints

Pueden ocurrir errores durante la instalación del agente del programa de complemento en el endpoint, o bien este agente puede no aparecer en la consola del Agente de OfficeScan por las siguientes razones:

Procedimiento

1. Plug-in Manager (`CNTAosMgr.exe`) no se está ejecutando en el endpoint. En el endpoint del Agente de OfficeScan, abra el Administrador de tareas de Windows y ejecute el proceso `CNTAosMgr.exe`.
2. No se ha descargado el paquete de instalación del agente del complemento en la carpeta del endpoint del Agente de OfficeScan ubicada en `<Carpeta de instalación del agente>\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Revise `Tmudump.txt` ubicado en `\AU_Data\AU_Log\` para conocer los motivos del error en la descarga.

   Nota

   Si el agente se instala correctamente, su información se encontrará disponible en `<carpeta de instalación del agente>\AOSSvcInfo.xml`.
3. La instalación del agente no se ha realizado correctamente o requiere alguna acción adicional. Puede comprobar el estado de la instalación en la consola de administración del programa de complemento y realizar acciones como, por

ejemplo, reiniciar el endpoint del Agente de OfficeScan tras la instalación o instalar las revisiones necesarias para el sistema operativo antes de la instalación.

Los agentes de los endpoints no se pueden iniciar si la secuencia de comandos de configuración automática de Internet Explorer redirecciona a un servidor proxy.

Plug-in Manager del Agente de OfficeScan (`CNTAosMgr.exe`) no puede iniciar un agente en los endpoints porque el comando de inicio del agente redirecciona a un servidor proxy. Este problema solo se produce cuando la configuración del proxy redirecciona el tráfico HTTP del usuario a la dirección 127.0.0.1.

Para resolver este problema, utilice una política de servidor proxy correctamente definida. Por ejemplo, no redireccione el tráfico HTTP a 127.0.0.1.

Si necesita utilizar una configuración de proxy que controle las solicitudes HTTP 127.0.0.1, realice las siguientes tareas.

Procedimiento

1. Defina la configuración de OfficeScan Firewall en la consola OfficeScan Web.

   Nota

   Lleve a cabo este paso solo si ha activado OfficeScan Firewall en los Agentes de OfficeScan.

   a. En la consola Web, vaya a **Agentes** > **Cortafuegos** > **Políticas** y haga clic en **Editar la plantilla de excepciones**.

   b. En la pantalla Editar la plantilla de excepciones, haga clic en **Agregar**.

   c. Utilice la siguiente información:

      - **Nombre**: su nombre favorito.
      - **Acción**: permitir el tráfico de red.

- **Dirección**: entrante.
- **Protocolo**: TCP.
- **Puertos**: cualquier número de puerto comprendido entre 5000 y 49151.

d. **Direcciones IP**: seleccione **Dirección IP única** y especifique la dirección IP de su servidor proxy (opción recomendada) o elija **Todas las direcciones IP**.

e. Haga clic en **Guardar**.

f. En la pantalla Editar la plantilla de excepciones, haga clic en **Guardar y aplicar las políticas existentes**.

g. Vaya a **Agentes** > **Cortafuegos** > **Perfiles** y haga clic en **Asignar perfil a los agentes**.

Si no existe ningún perfil del cortafuegos, cree uno haciendo clic en Agregar. Utilice la siguiente configuración:

- **Nombre**: su nombre favorito.
- **Descripción**: la descripción que prefiera.
- **Política**: política de acceso total.

Después de guardar el perfil nuevo, haga clic en **Asignar perfil a los agentes**.

2. Modifique el archivo `ofcscan.ini`.

a. Abra el archivo `ofcscan.ini` en la `<Carpeta de instalación del servidor>` mediante un editor de texto.

b. Busque **`[Global Setting]`** y añada `FWPortNum=21212` a la siguiente línea. Cambie "21212" por el número de puerto que haya especificado en el paso C anterior.

Por ejemplo:

```
[Global Setting]

FWPortNum=5000
```

c. Guarde el archivo.

3. En la consola Web, vaya a **Agentes** > **Configuración global para los agentes** y haga clic en **Guardar**.

Se ha producido un error en el sistema, módulo de actualización o programa Plug-in Manager y el mensaje de error proporciona un código de error específico

Plug-in Manager muestra alguno de los siguientes códigos de error en un mensaje de error. Si no puede resolver un problema después de consultar el apartado de soluciones que se proporciona en la tabla mostrada a continuación, póngase en contacto con su proveedor de asistencia.

TABLA 17-1. Códigos de error de Plug-in Manager

CÓDIGO DE ERROR	MENSAJE, CAUSA Y SOLUCIÓN
001	Se ha producido un error en el programa Plug-in Manager. El módulo de actualización de Plug-in Manager no responde cuando se consulta el progreso de una tarea de actualización. Puede que no se haya inicializado el controlador del módulo o del comando. Reinicie el servicio de OfficeScan Plug-in Manager y vuelva a realizar la tarea.

CÓDIGO DE ERROR	MENSAJE, CAUSA Y SOLUCIÓN
002	Se ha producido un error en el sistema. El módulo de actualización Plug-in Manager no puede abrir la clave de registro `SOFTWARE\TrendMicro\OfficeScan\service\AoS` debido a que es posible que se haya eliminado. Siga los pasos que se detallan a continuación: 1. Abra el editor del registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Restablezca el valor en 1.0.1000. 2. Reinicie el servicio Plug-in Manager de OfficeScan. 3. Descargue o desinstale el programa de complemento.

CÓDIGO DE ERROR	MENSAJE, CAUSA Y SOLUCIÓN
028	Se ha producido un error de actualización. Causas posibles: • El módulo de actualización de Plug-in Manager no puede descargar un programa de complemento. Compruebe que la conexión de red funciona correctamente y vuelva a intentarlo. • El módulo de actualización de Plug-in Manager no puede instalar el programa de complemento debido a que el agente del parche AU ha devuelto un error. El agente de correcciones de AU es el programa que inicia la instalación de los nuevos programas de complemento. Para conocer la causa exacta del error, consulte el registro de depuración "`TmuDump.txt`" del módulo ActiveUpdate en `\PCCSRV\Web\Service\AU_Data\AU_Log`. Siga los pasos que se detallan a continuación: 1. Abra el editor del registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Restablezca el valor en 1.0.1000. 2. Elimine la clave de registro del programa de complemento `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx` 3. Reinicie el servicio Plug-in Manager de OfficeScan. 4. Descargue el programa de complemento e instálelo.
170	Se ha producido un error en el sistema. El módulo de actualización de Plug-in Manager no puede procesar una operación entrante debido a que está llevando a cabo otra operación actualmente. Ejecute la tarea más adelante.

CÓDIGO DE ERROR	MENSAJE, CAUSA Y SOLUCIÓN
202	Se ha producido un error en el programa Plug-in Manager. El programa Plug-in Manager no se puede encargar de una tarea que se ejecuta en la consola Web. Actualice la consola Web o Plug-in Manager si existe alguna actualización disponible para este programa.
203	Se ha producido un error en el programa Plug-in Manager. El programa Plug-in Manager detectó un error de comunicación entre procesos (IPC) al intentar establecer comunicación con los servicios de extremo final de Plug-in Manager. Reinicie el servicio de OfficeScan Plug-in Manager y vuelva a realizar la tarea.
Otros códigos de error	Se ha producido un error en el sistema. Al descargar un nuevo programa de complemento, Plug-in Manager comprueba la lista de programas de complemento en el servidor ActiveUpdate. Plug-in Manager no ha podido obtener la lista. Siga los pasos que se detallan a continuación: 1. Abra el editor del registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Restablezca el valor en `1.0.1000`. 2. Reinicie el servicio Plug-in Manager de OfficeScan. 3. Descargue el programa de complemento e instálelo.

Capítulo 18

Recursos de solución de problemas

En este capítulo se proporciona una lista de recursos que puede utilizar para solucionar problemas del servidor de OfficeScan y de los Agente de OfficeScan.

Los temas que se incluyen son:

- *Soporte de sistema de inteligencia en la página 18-2*
- *Herramienta de diagnóstico de casos en la página 18-2*
- *Herramienta de ajuste del rendimiento de Trend Micro en la página 18-2*
- *Registros del servidor de OfficeScan en la página 18-3*
- *Registros de agentes de OfficeScan en la página 18-15*

Soporte de sistema de inteligencia

Soporte de sistema de inteligencia es una página en la que puede enviar archivos fácilmente a Trend Micro para que se analicen. Este sistema determina el GUID del servidor de OfficeScan y envía la información junto con el archivo. Al enviar el GUID del servidor de OfficeScan, garantiza que Trend Micro puede ofrecer comentarios sobre los archivos que se envían para su valoración.

Herramienta de diagnóstico de casos

Trend Micro Case Diagnostic Tool (CDT) recopila la información de depuración necesaria de un producto de cliente siempre que se originan problemas. Activa y desactiva automáticamente el estado de depuración del producto y recopila los archivos necesarios de acuerdo con las categorías de problemas. Trend Micro utiliza esta información para solucionar problemas relacionados con el producto.

Ejecute la herramienta en todas las plataformas compatibles con OfficeScan. Para obtener esta herramienta y la documentación correspondiente, póngase en contacto con el proveedor de asistencia.

Herramienta de ajuste del rendimiento de Trend Micro

Trend Micro proporciona una herramienta de ajuste del rendimiento independiente que permite identificar las aplicaciones que podrían provocar problemas con el rendimiento. Conviene ejecutar la Herramienta de ajuste del rendimiento de Trend Micro, disponible en la base de conocimientos de Trend Micro, en una imagen de estación de trabajo estándar y/o en unas cuantas estaciones de trabajo de destino en un proceso de implementación piloto para atribuir problemas de rendimiento en la implementación real de las funciones Supervisión del comportamiento y Control de dispositivos.

Para obtener más información, visite http://esupport.trendmicro.com/solution/en-us/1056425.aspx.

Registros del servidor de OfficeScan

Además de los registros disponibles en la consola Web, puede utilizar otros tipos de registros (por ejemplo, los de depuración) para solucionar los problemas del producto.

¡ADVERTENCIA!

los registros de depuración pueden afectar el rendimiento del servidor y consumir gran cantidad de espacio en el disco. Active la creación de registros de depuración solo cuando sea necesario y desactívela inmediatamente cuando ya no necesite datos de depuración. Elimine el archivo de registro si necesita conservar espacio en disco.

Registros de depuración del servidor con LogServer.exe

Utilice el archivo `LogServer.exe` para recopilar los registros sobre la depuración para:

- Registros básicos del Servidor de OfficeScan
- Trend Micro Vulnerability Scanner
- Registros de integración de Active Directory
- Registros de agrupación de agentes
- Registros de conformidad con las normas de seguridad
- Role-based administration
- Smart scan

Activar el registro de depuración

Procedimiento

1. Inicie sesión en la consola Web.
2. En el banner de la consola Web, haga clic en la primera "O" de "OfficeScan".
3. Seleccione **Activar el registro de depuración**.

4. Especifique la configuración del registro de depuración.
5. Haga clic en **Guardar**.
6. Compruebe el archivo de registro (`ofcdebug.log`) se encuentra en la ubicación predeterminada: <*Carpeta de instalación del servidor*>`\PCCSRV\Log`.

Desactivar el registro de depuración

Procedimiento

1. Inicie sesión en la consola Web.
2. En el banner de la consola Web, haga clic en la primera "O" de "OfficeScan".
3. Desactive **Activar el indicador de depuración**.
4. Haga clic en **Guardar**.

Activar el registro de depuración para la instalación y la actualización del servidor

Active la creación de registros de depuración antes de realizar las tareas siguientes:

- Desinstalar el servidor y volverlo a instalar
- Actualizar OfficeScan a una nueva versión
- Realizar una instalación o actualización remota (el registro de depuración se activa en el endpointdonde se inició el programa de instalación y no en el endpoint remoto).

Procedimiento

1. Copie la carpeta `LogServer` ubicada en <*carpeta de instalación del servidor*>`\PCCSRV\Private` en `C:\`.
2. Cree un archivo llamado `cdebug.ini` con el contenido siguiente:

```
[debug]

debuglevel=9

debuglog=c:\LogServer\ofcdebug.log

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. Guarde `ofcdebug.ini` en `C:\LogServer`.
4. Realice la tarea pertinente (es decir, desinstalar/reinstalar el servidor, actualizar a una nueva versión del servidor o realizar una instalación/actualización remota).
5. Compruebe el archivo `ofcdebug.log` en `C:\LogServer`.

Registros de la instalación

- Registros de instalación/actualización local

  Nombre de archivo: `OFCMAS.LOG`

  Ubicación: `%windir%`

- Registros de instalación/actualización remota
  - En el endpoint donde inició el programa de instalación:

    Nombre de archivo: `ofcmasr.log`

    Ubicación: `%windir%`
  - En el endpoint de destino:

    Nombre de archivo: `OFCMAS.LOG`

    Ubicación: `%windir%`

Registros de Active Directory

- Nombre de archivo: `ofcdebug.log`
- Nombre de archivo: `ofcserver.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\`
- Nombres de archivo:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Ubicación: `<Carpeta de instalación del servidor>\PCCSRV\HTTPDB\`

Registros de Role-based Administration

Para obtener información detallada de Role-based Administration, proceda como se indica a continuación:

- Ejecute Trend Micro Case Diagnostics Tool. Para obtener información, consulte *Herramienta de diagnóstico de casos en la página 18-2*.
- Recopile los siguientes registros:
  - Todos los archivos de <*carpeta de instalación del servidor*>`\PCCSRV\Private\AuthorStore`.
  - *Registros del servidor de OfficeScan en la página 18-3*

Registros de agrupación de agentes de OfficeScan

- Nombre de archivo: `ofcdebug.log`
- Nombre de archivo: `ofcserver.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\`
- Nombre de archivo: `SortingRule.xml`

  Ubicación: `<Carpeta de instalación del servidor>\PCCSRV\Private\SortingRuleStore\`
- Nombres de archivo:
  - `dbADScope.cdx`
  - `dbADScope.dbf`

  Ubicación: `<Carpeta de instalación del servidor>\HTTPDB\`

Registros de actualización de componentes

Nombre de archivo: `TmuDump.txt`

Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Web\Service\AU_Data\AU_Log`

Obtener información detallada de actualización del servidor

Procedimiento

1. Cree un archivo denominado `aucfg.ini` con el siguiente contenido:

```
[Debug]

level=-1

[Downloader]

ProxyCache=0
```

2. Guarde el archivo en <*carpeta de instalación del servidor*>\PCCSRV\Web\Service.
3. Reinicie el OfficeScan Master Service.

Detener la recopilación de información detalla de actualización del servidor

Procedimiento

1. Elimine `aucfg.ini`.
2. Reinicie el OfficeScan Master Service.

Registros de Agent Packager

Activación del registro para la creación de Agent Packager

Procedimiento

1. Modifique `ClnExtor.ini` en <*carpeta de instalación del servidor*>\PCCSRV\Admin\Utility\ClientPackager, como se indica a continuación:

```
[Common]

DebugMode=1
```

2. Compruebe que `ClnPack.log` esté en `C:\`.

Desactivación del registro para la creación de Agent Packager

Procedimiento

1. Abra `ClnExtor.ini`.
2. Cambie el valor de "DebugMode" de 1 a 0.

Registros de informe de conformidad con las normas de seguridad

Para obtener información detallada sobre la conformidad con las normas de seguridad, reúna los siguientes datos:

- Nombre de archivo: `RBAUserProfile.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\AuthorStore\`

- Todos los archivos de la carpeta `<carpeta de instalación del servidor>\PCCSRV\Registro\Informe de conformidad con las normas de seguridad\`.

- *Registros del servidor de OfficeScan en la página 18-3*

Registros de administración de servidores externos

- Nombre de archivo: `ofcdebug.log`

- Nombre de archivo: `ofcserver.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Private\`

- Todos los archivos de la carpeta `<carpeta de instalación del servidor>\PCCSRV\Registro\informe de administración del servidor externo\`.

- Nombres de archivo:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbClientInfo.cdx`
  - `dbclientInfo.dbf`

  Ubicación: `<Carpeta de instalación del servidor>\HTTPDB\`

Registros de excepción de control de dispositivos

Para obtener información detallada sobre la excepción de control de dispositivos, reúna los siguientes datos:

- Nombre de archivo: `ofcscan.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\`

- Nombre de archivo: `dbClientExtra.dbf`

  Ubicación: `<Carpeta de instalación del servidor>\HTTPDB\`

- Lista de excepciones de Control de dispositivos desde la consola OfficeScan Web.

Registros de Web Reputation de servidor de Smart Protection Server integrado

Nombre del archivo: `diagnostic.log`

Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\LWCS\`

Registros de ServerProtect Normal Server Migration Tool

Para activar el registro de depuración de ServerProtect Normal Server Migration Tool:

Procedimiento

1. Cree un archivo llamado `ofcdebug.ini` con el contenido siguiente:

   ```
   [Debug]

   DebugLog=C:\ofcdebug.log

   DebugLevel=9
   ```

2. Guarde el archivo en `C:\`.

3. Compruebe que `ofcdebug.log` esté en `C:\`.

Nota

Para desactivar el registro de depuración, elimine el archivo `ofcdebug.ini`.

Registros de VSEncrypt

OfficeScan crea automáticamente el registro de depuración (`VSEncrypt.log`) en la carpeta temporal de la cuenta de usuario. Por ejemplo, `C:\Documents and Settings\<nombre de usuario>\Local Settings\Temp`.

Registros del agente MCP de Control Manager

Depure los archivos de <*carpeta de instalación del servidor*>`\PCCSRV\CMAgent`.

- `Agent.ini`
- `Product.ini`
- La captura de pantalla de la página Configuración de Control Manager
- `ProductUI.zip`

Activar el registro de depuración para el agente MCP

Procedimiento

1. Modifique `product.ini` en <*carpeta de instalación del servidor*>`\PCCSRV\CmAgent`, como se indica a continuación:

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Reinicie el servicio del OfficeScan Control Manager Agent desde la consola de administración de Microsoft.

3. Compruebe que `CMAgent_debug.log` esté en `C:\`.

Desactivar el registro de depuración para el agente MCP

Procedimiento

1. Abra `product.ini` y elimine lo siguiente:

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Reinicie el servicio Control Manager para OfficeScan.

Registros de virus/malware

Nombre de archivo:

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\HTTPDB\`

Registros de spyware/grayware

Nombre de archivo:

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\HTTPDB\`

Registros de epidemias

TIPO DE REGISTRO	ARCHIVO
Registros de la epidemia actual de violación del cortafuegos	Nombre de archivo: `Cfw_Outbreak_Current.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`
Registros de la última epidemia de violación del cortafuegos	Nombre de archivo: `Cfw_Outbreak_Last.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`

TIPO DE REGISTRO	ARCHIVO
Registros de la epidemia actual de virus/malware	Nombre de archivo: `Outbreak_Current.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`
Registros de la última epidemia de virus/malware	Nombre de archivo: `Outbreak_Last.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`
Registros de la epidemia de spyware y grayware actual	Nombre de archivo: `Spyware_Outbreak_Current.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`
Registros de la última epidemia de spyware y grayware	Nombre de archivo: `Spyware_Outbreak_Last.log` Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\Log\`

Registros de Soporte de Virtual Desktop

- Nombre de archivo: `vdi_list.ini`

  Ubicación: <*Carpeta de instalación del servidor*>`\PCCSRV\TEMP\`

- Nombre de archivo: `vdi.ini`

  Ubicación: `<Carpeta de instalación del servidor>\PCCSRV\Private\`

- Nombre de archivo: `ofcdebug.txt`

  Ubicación: `<Carpeta de instalación del servidor>\PCCSRV\`

Para generar `ofcdebug.txt`, active el registro de depuración. Para obtener instrucciones sobre la activación del registro de depuración, consulte *Activar el registro de depuración en la página 18-3*.

Registros de agentes de OfficeScan

Utilice los registros del Agente de OfficeScan (por ejemplo, registros de depuración) para solucionar problemas en el Agente de OfficeScan.

¡ADVERTENCIA!

Los registros de depuración pueden afectar el rendimiento del agente y utilizar gran cantidad de espacio en el disco. Active la creación de registros de depuración solo cuando sea necesario y desactívela inmediatamente cuando ya no necesite datos de depuración. Elimine el archivo de registro si empieza a ocupar mucho.

Registros de depuración del agente de OfficeScan con LogServer.exe

Para activar el registro de depuración del Agente de OfficeScan:

Procedimiento

1. Cree un archivo llamado `ofcdebug.ini` con el contenido siguiente:

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Envíe `ofcdebug.ini` a los usuarios e indíqueles que guarden el archivo en `C:\`.

Nota

`LogServer.exe` se ejecuta automáticamente cada vez que se inicia el endpoint del Agente de OfficeScan. Indique a los usuarios que NO cierren la ventana de comandos de LogServer.exe que se abre cuando el endpoint se inicia, ya que este hecho solicita a OfficeScan que detenga la creación de registros de depuración. Si los usuarios cierran la ventana de comandos, pueden volver a iniciar la creación de registros de depuración ejecutando `LogServer.exe` que está ubicado en <*carpeta de instalación del agente*>.

3. Para cada endpoint del Agente de OfficeScan, puede comprobar ofcdebug.log en C:\.

Nota

Para desactivar el módulo de depuración del Agente de OfficeScan, elimine `ofcdebug.ini`.

Registros de instalación nueva

Para instalaciones de paquetes MSI:

- Nombre de archivo: `OFCNT.LOG`
- Ubicación: <*Carpeta de instalación del agente*>

Para instalaciones Web:

- Nombre de archivo: `WebInstall.log`
- Ubicación: `C:\`

Para instalaciones remotas:

- Nombre de archivo: `OFCNT.LOG`
- Ubicación: `C:\`

Para instalaciones de paquetes Autopcc y EXE:

- Nombre de archivo: `OFCNT.LOG`

- Ubicación: <*Carpeta de instalación del agente*>`%windir%\`

Registro de actualizaciones/Hotfix

Nombre de archivo: `upgrade_yyyymmddhhmmss.log`

Ubicación: <*Carpeta de instalación del agente*>`\Temp`

Registros de Damage Cleanup Services

Activar el registro de depuración de Damage Cleanup Services

Procedimiento

1. Abra el archivo `TSC.ini` que se encuentra en <*carpeta de instalación del agente*>.
2. Modifique la siguiente línea, como se indica a continuación:

   `DebugInfoLevel=5`
3. Compruebe el archivo `TSCDebug.log` que se encuentra en `<carpeta de instalación del agente>\debug`.

Desactivar el registro de depuración de Damage Cleanup Services

Abra el archivo `TSC.ini` y cambie el valor "`DebugInfoLevel`" de 5 a 0.

Limpiar el registro

Nombre de archivo: `yyyymmdd.log`

Ubicación: <*Carpeta de instalación del agente*>`\report\`

Registros de exploración de correo

Nombre de archivo: `SmolDbg.txt`

Ubicación: <*Carpeta de instalación del agente*>

Registros de conexiones de agentes de OfficeScan

Nombre de archivo: `Conn_YYYYMMDD.log`

Ubicación: <*Carpeta de instalación del agente*>`\ConnLog`

Registros de actualización de los agentes de OfficeScan

Nombre de archivo: `Tmudump.txt`

Ubicación: <*Carpeta de instalación del agente*>`\AU_Data\AU_Log`

Obtener información detallada de actualización del agente de OfficeScan

Procedimiento

1. Cree un archivo denominado `aucfg.ini` con el siguiente contenido:

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. Guarde el archivo en <*carpeta de instalación del agente*>.

3. Vuelva a cargar el Agente de OfficeScan.

Nota

Para detener la recopilación de información detallada de actualización del agente, elimine el archivo `aucfg.ini` y vuelva a cargar el Agente de OfficeScan.

Registros del Motor de Escaneo de Virus

Para activar el registro de depuración del motor de exploración antivirus:

Procedimiento

1. Abra el Editor del registro (`regedit.exe`).
2. Vaya a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.
3. Cambie el valor de "`DebugLogFlags`" a "`00003eff`".
4. Reproduzca los pasos que desencadenaron el problema de exploración.
5. Compruebe que `TMFilter.log` está en `%windir%`.

Nota

Restaure el valor de "`DebugLogFlags`" a "`00000000`".

Registros de prevención de epidemias

Nombre de archivo: `OPPLogs.log`

Ubicación: <*Carpeta de instalación del agente*>`\OppLog`

Registros de restablecimiento de prevención de epidemias

Nombres de archivo:

- `TmOPP.ini`
- `TmOPPRestore.ini`

Ubicación: <*Carpeta de instalación del agente*>\

Registros de depuración de la supervisión de comportamiento

Para activar los registro de depuración de la supervisión de comportamiento:

Procedimiento

1. Abra el Editor del registro (`regedit.exe`).
2. Vaya a `HKLM\SOFTWARE\TrendMicro\Aegis`.
3. Cambie el valor de "`DebugLogFlags`" a "`dword:00000032`".
4. Reproduzca los pasos que desencadenaron el problema.
5. Compruebe los siguientes registros en la carpeta `C:\Archivos de programa (x86)\Trend Micro\BM\log\`:
   - `TmCommengyyyymmdd_nn.log`
   - `TMPEMyyyymmdd_nn.log`

Registros de OfficeScan Firewall

Activación de la creación de registros de depuración del driver del cortafuegos común en los equipos con Windows Vista/Server 2008/7/Server 2012/8/8.1/10

Procedimiento

1. Modifique los siguientes valores de registro:

CLAVE DE REGISTRO	VALORES
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters`	Tipo: `DWORD` value `(REG_DWORD)` Nombre: `DebugCtrl` Valor: `0x00001111`
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters`	Tipo: `DWORD` value `(REG_DWORD)` Nombre: `DebugCtrl` Valor: `0x00001111`

2. Reinicie el endpoint.
3. Compruebe que `wfp_log.txt` y `lwf_log.txt` estén en `C:\`.

Activar la creación de registros de depuración del driver del Cortafuegos común en los equipos con Windows XP y Windows Server 2003

Procedimiento

1. Añada los datos siguientes a `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters`:

- Tipo: `DWORD value (REG_DWORD)`
- Nombre: `DebugCtrl`
- Valor: `0x00001111`

2. Reinicie el endpoint.
3. Compruebe que `cfw_log.txt` esté en `C:\`.

Desactivar el registro de depuración del Driver del cortafuegos común (todos los sistemas operativos)

Procedimiento

1. Elimine "`DebugCtrl`" en la clave de registro.
2. Reinicie el endpoint.

Activar el registro de depuración para el servicio del cortafuegos OfficeScan NT

Procedimiento

1. Modifique el archivo `TmPfw.ini` que se encuentra en <*carpeta de instalación del agente*>, como se indica a continuación:

```
[ServiceSession]

Enable=1
```

2. Vuelva a cargar el agente.
3. Compruebe que `ddmmyyyy_NSC_TmPfw.log` esté en `C:\temp`.

Desactivar el registro de depuración para el servicio del cortafuegos OfficeScan NT

Procedimiento

1. Abra el archivo `TmPfw.ini` y cambie el valor de "`Enable`" de 1 a 0.
2. Vuelva a cargar el Agente de OfficeScan.

Registro de la exploración de correo POP3 y Reputación Web

Activar el registro de depuración de la función Reputación Web y las funciones de exploración de correo POP3

Procedimiento

- Para agentes con Windows Vista o Windows Server 2008:
  a. Modifique el archivo `TmProxy.ini` que se encuentra en la <*carpeta de instalación del agente*>, como se indica a continuación:

```
[InteractiveSession]

Enable=1

LogFolder=C:\temp

[ServiceSession]

Enable=1

LogFolder=C:\temp
```

  b. Vuelva a cargar el Agente de OfficeScan.
  c. Compruebe que el registro de `ddmmyyyy_NSC_TmProxy.log` esté en `C:\temp`.

- Para agentes que ejecuten otras versiones de Windows:

  a. Modifique el archivo `TmOsprey.ini` que se encuentra en la <*carpeta de instalación del agente*>, como se indica a continuación:

  ```
  [InteractiveSession]

  Enable=1

  LogFolder=C:\temp

  [ServiceSession]

  Enable=1

  LogFolder=C:\temp
  ```

  b. Vuelva a cargar el Agente de OfficeScan.

  c. Compruebe que el registro de `ddmmyyyy_NSC_TmProxy.log` esté en `C:\temp`.

Desactivar el registro de depuración de la función Reputación Web y las funciones de exploración de correo POP3

Procedimiento

- Para agentes con Windows Vista o Windows Server 2008:

  a. Modifique el archivo `TmProxy.ini` que se encuentra en la <*carpeta de instalación del agente*>, como se indica a continuación:

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:\temp

  [ServiceSession]

  Enable=0
  ```

```
LogFolder=C:\temp
```

b. Vuelva a cargar el Agente de OfficeScan.

- Para agentes que ejecuten otras versiones de Windows:

a. Modifique el archivo `TmOsprey.ini` que se encuentra en la <*carpeta de instalación del agente*>, como se indica a continuación:

```
[InteractiveSession]

Enable=0

LogFolder=C:\temp

[ServiceSession]

Enable=0

LogFolder=C:\temp
```

b. Vuelva a cargar el Agente de OfficeScan.

Registros de listas de excepción de control de dispositivos

Nombre de archivo: `DAC_ELIST`

Ubicación: <*Carpeta de instalación del agente*>\

Registros de depuración de protección de datos

Para activar los registros de depuración de la protección de datos:

Procedimiento

1. Obtenga el archivo `logger.cfg` de su proveedor de asistencia.
2. Añada los siguientes datos en `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:

- Tipo: `String`
- Nombre: `debugcfg`
- Valor: `C:\Log\logger.cfg`

3. Cree una carpeta con el nombre «Log» en el directorio `C:\`.
4. Copie el archivo `logger.cfg` en la carpeta `Log`.
5. Implemente la configuración de prevención de pérdida de datos y Control de dispositivos desde la consola Web para empezar a recopilar registros.

Nota

Para desactivar los registros de depuración del módulo de protección de datos, elimine `debugcfg` de la clave de registro y reinicie el endpoint.

Registros de sucesos de Windows

El visualizador de sucesos de Windows registra los sucesos de aplicaciones que se han realizado correctamente, como los inicios de sesión o los cambios realizados en la configuración de la cuenta.

Procedimiento

1. Realice una de las operaciones siguientes:
   - Haga clic en **Iniciar** > **Panel de control** > **Rendimiento y Mantenimiento** > **Herramientas administrativas** > **Administración del equipo**.
   - Abra la consola MMC que contiene el visualizador de sucesos.
2. Haga clic en **Visualizador de sucesos**.

Registros de la interfaz del controlador de transporte (TDI)

Para activar los registros de la interfaz del controlador de transporte (TDI):

Procedimiento

1. Añada los datos siguientes a `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`:

PARÁMETRO	VALORES
Clave 1	Tipo: `DWORD value (REG_DWORD)` Nombre: `Debug` Valor: `1111 (Hexadecimal)`
Clave 2	Tipo: `String value (REG_SZ)` Nombre: `LogFile` Valor: `C:\tmtdi.log`

2. Reinicie el endpoint.
3. Compruebe que `tmtdi.log` esté en `C:\`.

Nota

Desactive el registro de depuración de TDI. Para ello, elimine `Debug` y `LogFile` de la clave de registro y reinicie el endpoint.

Capítulo 19

Asistencia técnica

Obtenga más información sobre los siguientes temas:

- *Recursos de solución de problemas en la página 19-2*
- *Ponerse en contacto con Trend Micro en la página 19-3*
- *Enviar contenido sospechoso a Trend Micro en la página 19-4*
- *Otros recursos en la página 19-5*

Recursos de solución de problemas

Antes de ponerse en contacto con el servicio de asistencia técnica, consulte los siguientes recursos en línea de Trend Micro.

Uso del portal de asistencia

El portal de asistencia de Trend Micro constituye un recurso de funcionamiento ininterrumpido que contiene la información más actualizada sobre problemas habituales e inusuales.

Procedimiento

1. Visite http://docs.trendmicro.com/es-es/enterprise/trend-micro-security-(for-mac).aspx.
2. Seleccione entre los productos disponibles o haga clic en el botón adecuado para buscar soluciones.
3. Utilice el cuadro **Buscar asistencia** para buscar las soluciones disponibles.
4. Si no encuentra ninguna solución, haga clic en **Ponerse en contacto con el equipo de asistencia** y seleccione el tipo de asistencia que necesita.

   Consejo

   Para enviar un caso de asistencia en línea, visite la siguiente URL:

   http://esupport.trendmicro.com/srf/srfmain.aspx

   Un ingeniero de asistencia de Trend Micro investigará el caso y responderá en un plazo máximo de 24 horas.

Enciclopedia de amenazas

En la actualidad, la mayor parte del malware consiste en amenazas mezcladas, que combinan dos o más tecnologías, para evitar los protocolos de seguridad informática.

Trend Micro hace frente a este complejo malware con productos que crean una estrategia de defensa personalizada. La enciclopedia de amenazas ofrece una amplia lista de nombres y síntomas de las diferentes amenazas combinadas, además de todo el malware, spam, URL maliciosas y vulnerabilidades conocidas.

Vaya a http://about-threats.trendmicro.com/es/threatencyclopedia#malware para obtener más información sobre:

- Malware y código móvil malicioso actualmente en circulación o "salvajes"
- Páginas de información correlacionada sobre amenazas para formar un historial completo de ataques Web
- Advertencias sobre amenazas de Internet, ataques con destino y amenazas de seguridad
- Ataques Web e información sobre tendencias en línea
- Informes de malware semanales

Ponerse en contacto con Trend Micro

En los Estados Unidos, los representantes de Trend Micro están disponibles por teléfono o correo electrónico:

Dirección	Trend Micro, Incorporated TREND MICRO España Plaza de las Cortes, 4 – 8º Izq. Madrid, 28014 España Irving, Texas 75062 EE. UU.
Teléfono	Teléfono: +1 (817) 569-8900 Gratuito: (888) 762-8736
Sitio Web	http://www.trendmicro.es/acerca/contacto/index.html
Dirección de correo electrónico	reception_es@trendmicro.es

- Oficinas de asistencia técnica de todo el mundo:

  http://www.trendmicro.es/acerca/contacto/index.html

- Documentación de productos de Trend Micro:

  http://www.trendmicro.es/acerca/contacto/index.html

Agilizar la llamada al servicio de asistencia

Para mejorar la solución de problemas, tenga a mano la siguiente información:

- Pasos para reproducir el problema
- Información del dispositivo o de la red
- Marca y modelo del equipo, además de hardware y dispositivos conectados adicionales
- Cantidad de memoria y espacio disponible en disco
- Sistema operativo y versión de Service Pack
- Versión del agente instalado
- Número de serie o código de activación
- Descripción detallada del entorno de instalación
- Texto exacto de cualquier mensaje de error recibido

Enviar contenido sospechoso a Trend Micro

Hay disponibles varias opciones para enviar contenido sospechoso a Trend Micro para su análisis.

Email Reputation Services

Consulte la reputación de una dirección IP específica y nombre a un agente de transferencia de correo para que la incluya en la lista global permitida:

https://ers.trendmicro.com/

Consulte la siguiente entrada de la base de conocimientos para enviar muestras de mensajes a Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Servicios de File Reputation

Recopile la información del sistema y envíe el contenido del archivo sospechoso a Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Anote el número de incidencia para poder realizar su seguimiento.

Servicios de Reputación Web

Consulte la clasificación de seguridad y el tipo de contenido de una URL de la que sospeche que es un sitio de phishing o de los llamados "de vector de enfermedades" (la fuente intencionada de las amenazas Web como el spyware y los virus):

http://global.sitesafety.trendmicro.com/

Si la clasificación asignada no es la correcta, envíe una solicitud de reclasificación a Trend Micro.

Otros recursos

Además de soluciones y asistencia técnica, también hay disponibles otros muchos recursos útiles que le permitirán estar actualizado, obtener información acerca de las novedades y estar información sobre de las tendencias de seguridad.

Centro de descarga

Cada cierto tiempo, Trend Micro puede publicar una revisión para un problema conocido comunicado o una actualización aplicable a un determinado producto o servicio. Para obtener más información sobre las revisiones disponibles, vaya a:

http://www.trendmicro.com/download/emea/?lng=es

Si no se ha aplicado una revisión (tienen fecha), abra el archivo Léame para determinar si es o no relevante para su entorno. El archivo Léame también incluye instrucciones de instalación.

Evaluación de la documentación

Trend Micro trata constantemente de mejorar la documentación. Si tiene alguna duda, comentario o sugerencia con relación a este documento u otros de Trend Micro, vaya al sitio Web siguiente:

http://www.trendmicro.com/download/documentation/rating.asp

Apéndices

Apéndices

Apéndice A

Compatibilidad con IPv6 en OfficeScan

Es necesario que los usuarios que vayan a implementar OfficeScan en un entorno que sea compatible con el direccionamiento IPv6 lean este apéndice. Este apéndice contiene información acerca de la amplitud de compatibilidad de IPv6 en OfficeScan.

Trend Micro asume que el lector está familiarizado con los conceptos de IPv6 y las tareas que implica la configuración de una red compatible con el direccionamiento IPv6.

Compatibilidad de IPv6 con el servidor y los agentes de OfficeScan

La versión 10.6 de OfficeScan es la primera compatible con IPv6. Las versiones anteriores de OfficeScan no son compatibles con las direcciones IPv6. La compatibilidad con IPv6 se activa de forma automática tras la instalación o la actualización del servidor de OfficeScan y los Agentes de OfficeScan que cumplen los requisitos de IPv6.

Requisitos del servidor de OfficeScan

Los requisitos de IPv6 para el servidor de OfficeScan son los siguientes:

- El servidor se debe instalar en Windows Server 2008, Windows Server 2012 o Windows Server 2016.
- El servidor debe utilizar un servidor Web IIS.
- Si el servidor va a administrar Agentes de OfficeScan IPv4 e IPv6, este debe tener direcciones tanto IPv4 como IPv6 e identificarse mediante su nombre de host. Si un servidor se identifica por su dirección IPv4, los Agentes de OfficeScan IPv6 no se podrán conectar al servidor. Lo mismo ocurre si los agentes IPv4 se conectan a un servidor identificado mediante su dirección IPv6.
- Si el servidor va a administrar solo agentes IPv6, el requisito mínimo es una dirección IPv6. El servidor se puede identificar mediante su nombre de host o su dirección IPv6. Cuando el servidor se identifica por su nombre de host, es preferible utilizar el nombre de dominio completo (FQDN). Esto se debe que, en un entorno en el que solo se utilice IPv6, un servidor WINS no puede convertir un nombre de host en la dirección IPv6 correspondiente.

Nota

El FQDN solo se puede especificar cuando se realiza una instalación local del servidor. No es compatible con las instalaciones remotas.

Requisitos del agente de OfficeScan

El Agente de OfficeScan se debe instalar en:

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows 10
- Windows Server 2016

Es preferible que el Agente de OfficeScan tenga direcciones tanto IPv4 como IPv6, ya que algunas de las entidades a las que se conecta solo son compatibles con las direcciones IPv4.

Limitaciones de los servidores que solo utilizan IPv6

En la siguiente tabla se muestran las limitaciones de un servidor de OfficeScan con direcciones IPv6 únicamente.

TABLA A-1. Limitaciones de los servidores que solo utilizan IPv6

EVENTO	LIMITACIÓN
Administración de agentes	Un servidor que solo utilice IPv6 no puede: • Implementar Agentes de OfficeScan en endpoints IPv4. • Administrar Agentes de OfficeScan que solo utilizan IPv4.

EVENTO	LIMITACIÓN
Actualizaciones y administración centralizada	Un servidor que solo utilice IPv6 no puede actualizarse desde fuentes de actualización que solo utilicen IPv4, como: • Trend Micro ActiveUpdate Server • Una fuente de actualización personalizada que solo utilice IPv4.
Registro, activación y renovación del producto	Un servidor que solo utilice IPv6 no se puede conectar al servidor de registro en línea de Trend Micro para registrar el producto, y obtener y activar o renovar la licencia.
Conexión proxy	Un servidor que solo utilice IPv6 no se puede conectar a través de un servidor proxy que solo utilice IPv4.
Soluciones de complemento	Un servidor que solo utilice IPv6 contará con Plug-in Manager, pero no podrá implementar ninguna de las soluciones de complemento en: • Los Agentes de OfficeScan o los hosts que solo utilizan IPv4 (debido a que no se cuenta con una conexión directa). • Los Agentes de OfficeScan o los hosts que solo utilizan IPv6, ya que ninguna de las soluciones de complemento es compatible con IPv6.

La mayoría de estas limitaciones se pueden subsanar estableciendo un servidor proxy con doble pila que pueda realizar conversiones entre las direcciones IPv4 e IPv6 (como DeleGate). Coloque el servidor proxy entre el servidor de OfficeScan y las entidades a las que se conecta o para las que ejerce de servidor.

Limitaciones de Agente de OfficeScan que solo utiliza IPv6

En la siguiente tabla se muestran las limitaciones cuando Agente de OfficeScan utiliza una dirección IPv6 únicamente.

TABLA A-2. Limitaciones de Agente de OfficeScan que solo utiliza IPv6

EVENTO	LIMITACIÓN
Servidor de OfficeScan principal	Los Agentes de OfficeScan que solo utilizan IPv6 no se pueden administrar con un servidor de OfficeScan que solo utiliza IPv4.
Actualizaciones	Un Agente de OfficeScan que solo utilice IPv6 no puede actualizarse desde fuentes de actualización que solo utilicen IPv4, como: • Servidor ActiveUpdate de Trend Micro • Un servidor de OfficeScan que solo utilice IPv4 • Un agente de actualización que solo utilice IPv4 • Una fuente de actualización personalizada que solo utilice IPv4.
Consultas de exploración, consultas de Reputación Web y Feedback Inteligente	Un Agente de OfficeScan que solo utilice IPv6 no puede enviar consultas a fuentes de Smart Protection , como: • Servidor de Protección Inteligente 2.0 (integrado o independiente) **Nota** La versión 2.5 del Servidor de Protección Inteligente es la primera compatible con IPv6. • Red de Protección Inteligente de Trend Micro (también para Feedback Inteligente)
Seguridad del software	Los Agentes de OfficeScan que solo utilicen IPv6 no se pueden conectar con el Servicio de software seguro certificado alojado por Trend Micro.
Soluciones de complemento	Los Agentes de OfficeScan que solo utilizan IPv6 no pueden instalar soluciones de complemento, ya que ninguna de ellas es compatible con IPv6.
Conexión proxy	Un Agente de OfficeScan que solo utilice IPv6 no se puede conectar a través de un servidor proxy que solo utilice IPv4.

La mayoría de estas limitaciones se pueden subsanar estableciendo un servidor proxy con doble pila que pueda realizar conversiones entre las direcciones IPv4 e IPv6 (como DeleGate). Coloque el servidor proxy entre los Agentes de OfficeScan y las entidades a las que se conectan.

Configuración de direcciones IPv6

La consola Web permite configurar una dirección IPv6 o un intervalo de direcciones IPv6. A continuación se recogen algunas directrices de configuración.

- OfficeScan acepta presentaciones de direcciones IPv6 estándares.

  Por ejemplo:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- OfficeScan también admite direcciones IPv6 locales vinculadas, como:

  `fe80::210:5aff:feaa:20a2`

  ¡ADVERTENCIA!

  Tenga cuidado al especificar una dirección IPv6 local vinculada ya que, aunque OfficeScan puede admitir la dirección, puede que no funcione como se espera en ciertas circunstancias. Por ejemplo, los Agentes de OfficeScan no pueden realizar actualizaciones desde una fuente de actualización si esta se encuentra en otro segmento de red y se identifica por medio de su dirección IPv6 local vinculada.

- Cuando la dirección IPv6 forme parte de la URL, escriba la dirección entre corchetes ([]).

- Normalmente, en el caso de los intervalos de direcciones IPv6, se necesitan un prefijo y una longitud de prefijo. En el caso de las configuraciones que requieren que el servidor solicite direcciones IP, se aplican restricciones en la longitud de

prefijo para evitar problemas de rendimiento que podrían surgir cuando el servidor realiza consultas en una cantidad significativa de direcciones IP. Por ejemplo, en la función Administración de servidores externos, la longitud de prefijo solo puede encontrarse entre 112 (65.536 direcciones IP) y 128 (2 direcciones IP).

- Algunas configuraciones que utilizan intervalos de direcciones o direcciones IPv6 se implementarán en Agentes de OfficeScan, pero Agentes de OfficeScan harán caso omiso de ellas. Por ejemplo, si ha configurado la lista de fuentes de Smart Protection y ha incluido un Servidor de Protección Inteligente que se identifica mediante su dirección IPv6, los Agentes de OfficeScan que solo utilicen IPv4 omitirán el servidor y se conectarán a las demás fuentes de Smart Protection.

Pantallas que muestran direcciones IP

En este tema se recogen las ubicaciones de la consola Web en las que se muestran las direcciones IP.

UBICACIÓN	DESCRIPCIÓN
Árbol de agentes	Siempre que aparezca el árbol de agentes, aparecerán las direcciones IPv6 de los Agentes de OfficeScan que solo utilizan IPv6 en la columna **Dirección IP**. En el caso de los Agentes de OfficeScan de doble pila, las direcciones IPv6 se mostrarán siempre que las hayan utilizado para registrarse en el servidor. **Nota** La dirección IP que utilizan los Agentes de OfficeScan de doble pila al registrarse en el servidor se puede controlar desde **Agentes** > **Configuración global para los agentes > Red** > **Dirección IP preferida**. Cuando se exporta la configuración de un árbol de agentes a un archivo, las direcciones IPv6 también aparecen en el archivo exportado.

Ubicación	Descripción
Estado del agente	Existe información detallada del agente en **Agentes** > **Administración de agentes > Estado**. En esa pantalla, verá las direcciones IPv6 de los Agentes de OfficeScan de doble pila que solo utilizan IPv6 y de los Agentes de OfficeScan que han utilizado sus direcciones IPv6 para registrarse en el servidor.
Registros	Las direcciones IPv6 de los Agentes de OfficeScan de doble pila y que solo utilizan IPv6 aparecen en los siguientes registros: • Registros de virus/malware • Registros de spyware/grayware • Registros del cortafuegos • Registros de comprobación de la conexión
Consola de Control Manager	En la siguiente tabla se muestran las direcciones IP del servidor de OfficeScan y de los Agentes de OfficeScan que aparecen en la consola de Control Manager. • Servidor de doble pila: IPv4 e IPv6 • Servidor que solo utiliza IPv4: IPv4 • Servidor que solo utiliza IPv6: IPv6 • Agente de OfficeScan de doble pila: La dirección IP utilizada cuando el Agente de OfficeScan se ha registrado en el servidor de OfficeScan • Agente de OfficeScan que solo utiliza IPv4: IPv4 • Agente de OfficeScan que solo utiliza IPv6: IPv6

Apéndice B

Compatibilidad de Windows Server Core

Este apéndice trata de la compatibilidad de OfficeScan con Windows Server Core.

Compatibilidad de Windows Server Core

Windows Server Core es una instalación mínima de una versión de Windows Server. En Server Core:

- Se eliminan muchas de las opciones y características de Windows Server.
- El servidor ejecuta un sistema operativo de núcleo mucho más fino.
- La mayoría de las tareas se efectúan desde la interfaz de la línea de comandos.
- El sistema operativo ejecuta menos servicios y necesita menos recursos durante el inicio.

OfficeScan admite instalaciones del Agente de OfficeScan en las siguientes versiones de Windows Server Core:

- Windows Server Core 2008
- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016

El Agente de OfficeScan es compatible con Server Core. Esta sección contiene información relativa a la compatibilidad con Server Core.

El servidor de OfficeScan no es compatible con Server Core.

Métodos de instalación para Windows Server Core

Los siguientes métodos de instalación no son compatibles o solo lo son de forma parcial:

- Página Web de instalación: este método no es compatible porque Server Core no cuenta con Internet Explorer.

- Trend Micro Vulnerability Scanner: la herramienta Vulnerability Scanner no se puede ejecutar de forma local en Server Core. Ejecute la herramienta desde el servidor de OfficeScan o desde otro endpoint.

Se admiten los siguientes métodos de instalación:

- Instalación remota. Para conocer más detalles, consulte *Instalar de forma remota desde la consola Web de OfficeScan en la página 5-23*.
- Configuración de inicio de sesión
- Agent Packager

Instalación del agente de OfficeScan utilizando la configuración de inicio de sesión

Procedimiento

1. En el endpoint de destino, abra un símbolo del sistema.
2. Asigne la ubicación del archivo `AutoPcc.exe` en el servidor de OfficeScan escribiendo el comando siguiente:

   ```
   net use <letra asignada a la unidad> \\<nombre de host o dirección IP del servidor de OfficeScan>\ofcscan
   ```

   Por ejemplo:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

3. Proporcione el nombre de usuario y la contraseña del servidor de destino.

   Aparecerá un mensaje en el que se le informará de que `AutoPcc.exe` se asignó correctamente.

4. Cambie a la ubicación de `AutoPcc.exe` escribiendo la letra de unidad asignada y dos puntos. Por ejemplo:

   ```
   P:
   ```

5. Escriba lo siguiente para iniciar la instalación:

`AutoPcc.exe`

La imagen siguiente muestra los comandos y resultados en la línea de comandos.

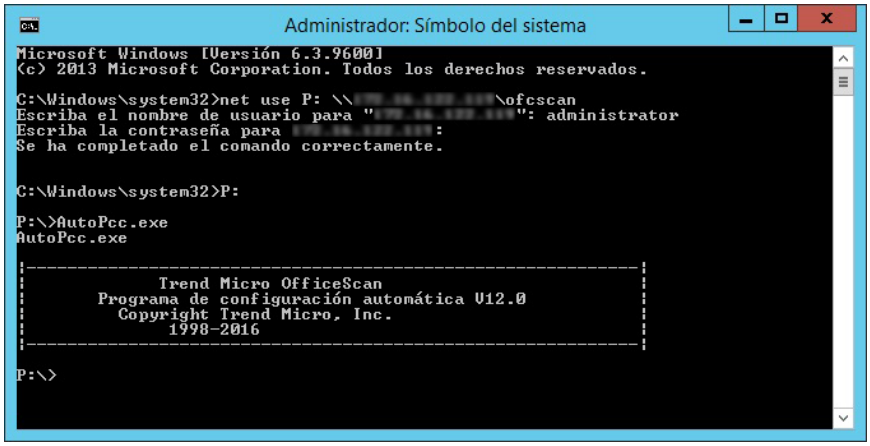


FIGURA B-1. Línea de comandos que muestra cómo instalar el Agente de OfficeScan utilizando la configuración de inicio de sesión

Instalación del agente de OfficeScan mediante el paquete del agente de OfficeScan

Procedimiento

1. Cree el paquete.

   Para conocer más detalles, consulte *Instalar con Agent Packager en la página 5-29*.

2. Abra una ventana de línea de comandos.

3. Asigne la ubicación del paquete del Agente de OfficeScan escribiendo el comando siguiente:

   `net use <letra de unidad asignada> \\<ubicación del paquete de agente>`

Por ejemplo:

```
net use P: \\10.1.1.1\Package
```

Aparecerá un mensaje en el que se le informará si la ubicación del paquete del Agente de OfficeScan se ha asignado correctamente.

4. Cambie a la ubicación del paquete del Agente de OfficeScan escribiendo la letra de unidad asignada y dos puntos. Por ejemplo:

   ```
   P:
   ```

5. Copie el paquete del Agente de OfficeScan en un directorio local en el endpoint de Server Core escribiendo el comando siguiente:

   ```
   copy <nombre de archivo del paquete> <directorio en el
   endpoint de Server Core donde desea copiar el paquete>
   ```

   Por ejemplo:

   ```
   copy officescan.msi C:\Client Package
   ```

   Aparecerá un mensaje en el que se le informará de que el paquete del Agente de OfficeScan se ha copiado correctamente.

6. Cambie al directorio local. Por ejemplo:

   ```
   C:
   ```

   ```
   cd C:\Client Package
   ```

7. Escriba el nombre de archivo del paquete para iniciar la instalación. Por ejemplo:

   ```
   officescan.msi
   ```

La imagen siguiente muestra los comandos y resultados en la línea de comandos.

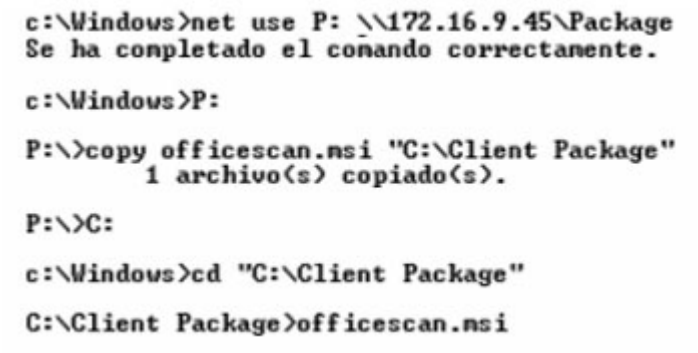


FIGURA B-2. Línea de comandos que muestra cómo instalar el Agente de OfficeScan utilizando un paquete de agente

Funciones del agente de OfficeScan en Windows Server Core

La mayoría de las características del Agente de OfficeScan disponibles en Windows Server 2008/2012/2016 funcionan en Server Core. La única característica que no es compatible es el modo independiente.

Para obtener una lista de las características disponibles en Windows Server 2008/2012/2016, consulte *Características del agente de OfficeScan en la página 5-3*.

Solo se puede acceder a la consola del Agente de OfficeScan desde la interfaz de la línea de comandos.

Nota

Algunas pantallas de la consola del Agente de OfficeScan incluyen un botón de Ayuda. Al hacer clic en él, se abre una ventana de Ayuda contextual basada en HTML. Dado que Windows Server Core 2008/2012/2016 no dispone de un explorador, el usuario de este sistema no dispondrá de Ayuda. Para ver la Ayuda, el usuario tendrá que instalar un explorador.

Comandos de Windows Server Core

Realice las tareas de Agente de OfficeScan mediante la emisión de comandos desde la interfaz de la línea de comandos.

Para ejecutar los comandos, vaya a la ubicación de `PccNTMon.exe`. Este proceso es el responsable de iniciar la consola del Agente de OfficeScan. Este proceso se halla en la <*carpeta de instalación del agente*>.

En la siguiente tabla figuran los comandos disponibles.

TABLA B-1. Comandos de Windows Server Core

COMANDO	ACCIÓN
`pccnt <unidad o ruta de la carpeta>`	Explora la unidad o carpeta especificada para comprobar si existen riesgos de seguridad. Directrices: • Si la ruta de carpeta contiene un espacio, ponga toda la ruta entre comillas. • No se admite la exploración de archivos individuales. Comandos correctos: • `pccnt C:\` • `pccnt D:\Files` • `pccnt "C:\Documents and Settings"` Comandos incorrectos: • `pccnt C:\Documents and Settings` • `pccnt D:\Files\example.doc`
`pccntmon -r`	Abre Real-Time Monitor.
`pccntmon -v`	Enumera los componentes del agente y sus versiones.
`pccntmon -u`	Actualiza los componentes de Agente de OfficeScan.
`pccntmon -n <unload_password>`	Descarga el Agente de OfficeScan. Para volver a cargar el Agente de OfficeScan, escriba el siguiente comando: `pccntmon`
`pccntmon -m <uninstall_password>`	Desinstala el Agente de OfficeScan.

COMANDO	ACCIÓN

`pccntmon -c`	Muestra en la línea de comandos la siguiente información:
	• Método de exploración
	  • Smart scan
	  • Exploración convencional
	• Estado del patrón
	  • Actualizado
	  • Obsoleto
	• Servicio de exploración en tiempo real
	  • Funcional
	  • Desactivado o no es funcional
	• Estado de la conexión del agente
	  • Conectado
	  • Independiente
	  • Desconectado
	• Servicios de Reputación Web
	  • Disponible
	  • Volviendo a conectar
	• Servicios de File Reputation
	  • Disponible
	  • Volviendo a conectar

`pccntmon -h`	Muestra todos los comandos disponibles.

Apéndice C

Compatibilidad con Windows 8/8.1/10 y Windows Server 2012/2016

Este apéndice describe la compatibilidad de OfficeScan con Windows 8/8.1/10 y Windows Server 2012/2016.

Acerca de Windows 8/8.1/10 y Windows Server 2012/2016

Windows 8/8.1 y Windows Server 2012/2016 ofrecen a los usuarios dos tipos de modos de funcionamiento: modo de escritorio y modo de interfaz de usuario de Windows. Los usuarios pueden elegir ejecutar Windows 10 en modo de escritorio o en modo de tableta El modo de escritorio es similar a la pantalla **Inicio** clásica de Windows.

El modo de interfaz de usuario de Windows le brinda a los usuarios una nueva experiencia de interfaz similar a la que se usa en los teléfonos de Windows. Algunas de las características nuevas son una interfaz de panel táctil de desplazamiento, mosaicos y notificaciones del sistema.

TABLA C-1. Mosaicos y notificaciones del sistema

CONTROL	DESCRIPCIÓN
Mosaicos	Los mosaicos son similares a los iconos de escritorio usados en las versiones anteriores de Windows. Los usuarios pueden hacer clic o puntear sobre un mosaico para iniciar la aplicación asociada con el mosaico. Los mosaicos dinámicos brindan a los usuarios información específica de la aplicación que se actualiza dinámicamente. Las aplicaciones pueden publicar información en los mosaicos incluso cuando no estén ejecutándose
Notificaciones del sistema	Las notificaciones del sistema son similares a los mensajes emergentes. Estas notificaciones brindan la información más reciente acerca de los eventos que se producen durante la ejecución de una aplicación. Aparecen en primer plano sin importar que Windows esté actualmente en el modo de escritorio, muestre la pantalla de bloqueo o ejecute otra aplicación. **Nota** Según cuál sea la aplicación, las notificaciones del sistema probablemente no aparezcan en todas las pantallas ni en todos los modos.

Compatibilidad de OfficeScan con mosaicos y notificaciones del sistema

La siguiente tabla describe cómo OfficeScan admite los mosaicos y las notificaciones del sistema en el modo de interfaz de usuario de Windows.

TABLA C-2. Compatibilidad de OfficeScan con mosaicos y notificaciones del sistema

CONTROL	OFFICESCAN SUPPORT
Mosaicos	OfficeScan brinda a los usuarios un mosaico que se vincula con el programa del Agente de OfficeScan. Cuando el usuario hace clic en el mosaico, Windows cambia al modo de escritorio y se muestra el programa del Agente de OfficeScan. **Nota** OfficeScan no admite mosaicos dinámicos.
Notificaciones del sistema	OfficeScan ofrece las siguientes notificaciones del sistema: • Programa sospechoso detectado • Exploración programada • Amenaza resuelta • Es necesario reiniciar el equipo • Se ha detectado un dispositivo de almacenamiento USB • Epidemia detectada **Nota** OfficeScan solamente muestra notificaciones del sistema en el modo de interfaz de usuario de Windows.

Habilitar notificaciones del sistema en Windows 8/8.1 y Windows Server 2012

Los usuarios pueden elegir recibir notificaciones del sistema modificando la **configuración del equipo** en el endpoint del Agente de OfficeScan. OfficeScan requiere que los usuarios habiliten las notificaciones del sistema.

Procedimiento

1. Mueva el puntero del mouse a la esquina inferior derecha de la pantalla para mostrar la barra **Accesos**.
2. Haga clic en **Configuración** > **Cambiar configuración de PC**.

   Aparecerá la pantalla **Configuración**.
3. Haga clic en **Notificaciones**.
4. En la sección **Notificaciones**, establezca la siguiente configuración en **Activada**:
   - **Mostrar notificaciones de las aplicaciones**
   - **Mostrar notificaciones de las aplicaciones en la pantalla de bloqueo** (opcional)
   - **Reproducir sonidos de notificaciones** (opcional)

Activación de las notificaciones del sistema en Windows 10 y Windows Server 2016

Los usuarios pueden elegir recibir notificaciones del sistema accediendo a **Active Center** en el endpoint del Agente de OfficeScan. OfficeScan requiere que los usuarios habiliten las notificaciones del sistema.

Procedimiento

1. En la bandeja del sistema, haga clic en el icono de notificaciones y en **Todas las configuraciones**.

2. En la pantalla Configuración, haga clic en **Sistema** y en **Notificaciones & Acciones**.

3. En la sección **Notificaciones**, establezca **Mostrar notificaciones de las aplicaciones** en **Activado**.

Compatibilidad de la característica OfficeScan por parte del modo de interfaz de usuario

El modo en el que los usuarios utilizan Windows 8/8.1 o Windows Server 2012/2016 afecta a la versión de Internet Explorer 10 y posteriores que se usa y, por tanto, mejora el nivel de compatibilidad que las diferentes características de OfficeScan proporcionan. En la siguiente tabla se enumera el nivel de compatibilidad con las diferentes características de OfficeScan en el modo de escritorio y en el modo de interfaz de usuario de Windows.

Nota

Las características no enumeradas brindan una total compatibilidad en ambos modos operativos de Windows.

TABLA C-3. Compatibilidad de la característica OfficeScan por parte del modo de interfaz de usuario

CARACTERÍSTICA	MODO DE ESCRITORIO	INTERFAZ DE USUARIO DE WINDOWS
Consola de servidor Web	Compatibilidad completa	Incompatible
Reputación Web	Compatibilidad completa	Compatibilidad limitada • Exploración HTTPS deshabilitada
Cortafuegos	Compatibilidad completa	Compatibilidad limitada • Filtro de aplicaciones deshabilitado

Internet Explorer 10/11 y Microsoft Edge

Internet Explorer (IE) 10 es el explorador predeterminado en Windows 8/8.1 y Windows Server 2012. Internet Explorer 10 viene en dos versiones diferentes: una para la interfaz de usuario de Windows y otra para el modo de escritorio.

Microsoft Edge es el explorador predeterminado de Windows 10 y Windows Server 2016.

Nota

En Microsoft Edge, la exploración HTTPS está desactivada porque Microsoft Edge no es compatible con la extensión del complemento.

Internet Explorer 10 y posterior para la interfaz de usuario de Windows ofrece una experiencia de exploración libre de complementos. Los programas de complemento para la exploración Web antes no seguían estándares establecidos y, por ello, la calidad del código empleado por estos programas es variable. Los complementos también necesitan usar más recursos del sistema y aumentan el riesgo de infecciones de malware.

Microsoft ha desarrollado Internet Explorer 10 y posterior para que la interfaz de usuario de Windows siga nuevas tecnologías basadas en estándares a fin de reemplazar las soluciones de complementos que se usaban anteriormente. En la siguiente tabla se enumeran las tecnologías que Internet Explorer 10 y posterior usa en lugar de la anterior tecnología de complementos.

TABLA C-4. Comparación de tecnologías basadas en estándares con programas de complemento

FUNCIONALIDAD	TECNOLOGÍA ESTÁNDAR WORLD WIDE WEB (W3C)	EQUIVALENTES DE COMPLEMENTOS DE EJEMPLO
Vídeo y audio	Vídeo y audio HTML5	• Flash • Apple QuickTime • Silverlight

Funcionalidad	Tecnología estándar World Wide Web (W3C)	Equivalentes de complementos de ejemplo
Gráficos	• Canvas HTML5 • Gráficos vectoriales escalables (SVG) • Transiciones y animaciones de hojas de estilo en cascada, nivel 3 (CSS3) • Transformaciones CSS	• Flash • Apple QuickTime • Silverlight • Subprogramas Java
Almacenamiento sin conexión	• Almacenamiento Web • API de archivo • IndexedDB • API de caché de aplicaciones	• Flash • Subprogramas Java • Google Gears
Comunicación de la red, uso compartido de recursos, carga de archivos	• Mensajería Web HTML • Uso compartido de recursos de origen cruzado (CORS)	• Flash • Subprogramas Java

Microsoft también desarrolló un complemento compatible con Internet Explorer 10 y posterior solamente para el modo de escritorio. Si los usuarios que están en el modo de interfaz de usuario de Windows encuentran un sitio Web que requiere el uso de programas de complemento adicionales, se muestra una notificación en Internet Explorer 10 y posterior que pide a los usuarios que cambien al modo de escritorio. Cuando ya estén en este modo, los usuarios pueden ver sitios Web que requieren el uso o la instalación de programas de complemento de terceros.

Apéndice D

Recuperación de OfficeScan

Este apéndice está dedicado a la compatibilidad con la recuperación del servidor de OfficeScan y el agente.

Recuperación del servidor de OfficeScan y los Agentes de OfficeScan mediante el paquete de copia de seguridad del servidor

El procedimiento de recuperación de OfficeScan implica la recuperación de los Agentes de OfficeScan y, a continuación, del servidor de OfficeScan.

Importante

- Los administradores solo pueden recuperar el servidor y los agentes de OfficeScan utilizando el siguiente procedimiento si el administrador ha decidido realizar copias de seguridad del servidor durante el proceso de instalación. Si los archivos de copia de seguridad del servidor no están disponibles, consulte el *Manual de instalación y actualización* de OfficeScan para obtener información sobre los procedimientos de recuperación manual.
- Esta versión de OfficeScan solo admite recuperaciones de las siguientes versiones de OfficeScan:
  - OfficeScan 11.0 Service Pack 1 con una revisión crítica
  - OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0
  - OfficeScan 10.6 Service Pack 3

Recuperación de servidor de los agentes de OfficeScan

OfficeScan solo puede recuperar los Agentes de OfficeScan de la misma versión del servidor que se restaura. No puede recuperar una versión de los Agentes de OfficeScan anterior a la del servidor.

Importante

Asegúrese de que recupera los Agentes de OfficeScan antes de recuperar el servidor de OfficeScan.

Procedimiento

1. Asegúrese de que los Agentes de OfficeScan no puedan actualizar el programa del agente.

   a. En la consola Web de OfficeScan XG, desplácese a **Agentes** > **Administración de agentes**.

   b. Seleccione los Agentes de OfficeScan que desee recuperar.

   c. Haga clic en la pestaña **Configuración** > **Derechos y otras configuraciones** > **Otras configuraciones**.

   d. Active la opción **Los agentes de OfficeScan pueden actualizar componentes pero no pueden actualizar el programa del agente ni implementar archivos Hotfix**.

2. En la consola Web de OfficeScan XG, desplácese a **Actualizaciones** > **Agentes** > **Origen de actualización**.

3. Seleccione **Fuente de actualización personalizada**.

4. En la lista **Fuente de actualización personalizada**, haga clic en **Añadir**.

   Se abrirá una nueva pantalla.

5. Escriba las direcciones IP de los Agentes de OfficeScan que se van a recuperar.

6. Escriba la URL de la fuente de actualizaciones.

   Por ejemplo:

   ```
   http://<dirección IP del servidor de OfficeScan>:<puerto>/
   OfficeScan/download/Rollback
   ```

7. Haga clic en **Guardar**.

8. Haga clic en **Notificar a todos los agentes**.

   Cuando un Agente de OfficeScan que se va a recuperar se actualiza a partir del origen de actualización, el Agente de OfficeScan se desinstala y, a continuación, se instala la versión anterior del Agente de OfficeScan en cuestión.

Consejo

Los administradores pueden iniciar una actualización manual en los Agentes de OfficeScan para acelerar el proceso de recuperación. Para conocer más detalles, consulte *Actualización manual de agente de OfficeScan en la página 6-48*.

9. Una vez instalada la versión anterior del Agente de OfficeScan, informe al usuario de que debe reiniciar el endpoint.

   Una vez que finalice el proceso de recuperación, el Agente de OfficeScan sigue enviando informes al mismo servidor de OfficeScan.

Nota

Después de recuperar el Agente de OfficeScan, todos los componentes, incluido el patrón de virus, se recuperan a la versión anterior. Si los administradores no recuperan el servidor de OfficeScan, el Agente de OfficeScan que se ha recuperado no podrá actualizar componentes. Los administradores deben cambiar el origen de actualización del Agente de OfficeScan que se ha recuperado al origen de actualización estándar para recibir nuevas actualizaciones de componentes.

Restauración de la versión previa del servidor de OfficeScan

El procedimiento de restauración del servidor de OfficeScan requiere que los administradores desinstalen el servidor de OfficeScan XG, vuelvan a instalar la versión anterior del servidor, detengan manualmente los servicios de Windows, actualicen el registro del sistema y reemplacen los archivos del servidor de OfficeScan en el directorio de instalación de OfficeScan.

Importante

Asegúrese de que recupera los Agentes de OfficeScan antes de restaurar el servidor de OfficeScan.

Procedimiento

1. Desinstale el servidor de OfficeScan XG.
2. Instale la versión anterior del servidor de OfficeScan.

   Consejo

   Trend Micro recomienda no cambiar la dirección IP ni el nombre de host al restaurar el servidor.

   Para verificar la versión anterior del servidor, vaya a <*carpeta de instalación del servidor*> y consulte la carpeta de restauración creada durante la instalación del servidor de OfficeScan XG. El nombre de la carpeta (denominado <versión_de_carpeta_de_restauración>) es uno de los siguientes:

   - OSCE11_SP1: OfficeScan 11.0 Service Pack 1
   - OSCE11: OfficeScan 11.0
   - OSCE106_SP3: OfficeScan 10.6 Service Pack 3

3. En el equipo del servidor de OfficeScan, detenga los siguientes servicios:
   - Intrusion Defense Firewall (si está instalado)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - Servicio World Wide Web Publishing
4. Copie todos los archivos y los directorios del directorio `<carpeta_de_instalación_del_servidor>\<versión_de_carpeta_de_restauración>\` y utilícelos para reemplazar los del directorio `<carpeta_de_instalación_del_servidor>\PCCSRV\`.

5. Restaure el registro de OfficeScan.

   a. Abra el **Editor del Registro** (`regedit.exe`).

   b. En el panel de navegación izquierdo, seleccione una de las siguientes claves de registro:

      - Para sistemas de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
      - Para sistemas de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

   c. Vaya a **Archivo** > **Importar...**.

   d. Seleccione el archivo `.reg` del servidor general de OfficeScan que se encuentra en el directorio `<carpeta_de_instalación_del_servidor>\<versión_de_carpeta_de_restauración>\`.

      El nombre del archivo de registro tiene el siguiente formato:

      `RegBak_<versión_de_carpeta_de_restauración>.reg`

   e. Haga clic en **Sí** para restaurar todas las claves de la versión anterior de OfficeScan.

6. También puede restaurar el programa de copia de seguridad de la base de datos.

   a. Abra el **Editor del Registro** (`regedit.exe`).

   b. En el panel de navegación izquierdo, seleccione una de las siguientes claves de registro:

      - Para sistemas de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
      - Para sistemas de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

   c. Vaya a **Archivo** > **Importar...**.

   d. Seleccione el archivo de la base de datos `.reg` que se encuentra en el directorio `<carpeta_de_instalación_del_servidor>\<versión_de_carpeta_de_restauración>\`.

El nombre del archivo de registro tiene el siguiente formato:

```
RegBak_DBBak_<versión_de_carpeta_de_restauración>.reg
```

e. Haga clic en **Sí** para restaurar todas las claves de la versión anterior de OfficeScan.

7. Abra un editor de línea de comandos (`cmd.exe`) y escriba los siguientes comandos para restablecer el contador de rendimiento del Servidor Local de Clasificación Web:

```
cd <carpeta de instalación del servidor>\PCCSRV\LWCS\

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

8. Reinicie los siguientes servicios:

- Intrusion Defense Firewall (si está instalado)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- OfficeScan Active Directory Integration Service
- OfficeScan Control Manager Agent
- OfficeScan Plug-in Manager
- OfficeScan Master Service
- Apache 2 (si se utiliza el servidor Web Apache)
- Servicio World Wide Web Publishing (si se utiliza el servidor Web de IIS)

9. Limpie la caché de Internet Explorer y elimine los controles ActiveX manualmente. Para obtener información sobre la eliminación de controles ActiveX en Internet Explorer 9, consultehttp://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

La configuración de la versión del servidor de OfficeScan anterior se ha restaurado.

Consejo

Los administradores pueden confirmar una recuperación correcta comprobando el número de versión de OfficeScan en la pantalla **Acerca de** (**Ayuda** > **Acerca de**).

10. También puede registrar el servidor de OfficeScan en el servidor de Control Manager mediante la consola Web.

11. También puede registrar el servidor de OfficeScan en el servidor de Deep Discovery mediante la consola Web.

Nota

La integración de Deep Discovery con el servidor de OfficeScan comenzó con OfficeScan 10.6 Service Pack 2.

12. Después de confirmar que OfficeScan se recuperó correctamente, elimine todos los archivos del directorio `<carpeta_de_instalación_del_servidor>\<versión_de_carpeta_de_restauración>\`.

Apéndice E

Glosario

Los términos incluidos en este glosario proporcionan información adicional acerca de los términos del endpoint a los que se hace referencia frecuentemente, así como sobre los productos y las tecnologías de Trend Micro.

ActiveUpdate

ActiveUpdate es una función incorporada en numerosos productos de Trend Micro. Conectado al sitio Web de actualizaciones de Trend Micro, ActiveUpdate ofrece descargas actualizadas de archivos de patrones, motores de exploración, programas y otros archivos de componentes de Trend Micro a través de Internet.

Archivo comprimido

Un archivo que contiene uno o varios archivos independientes además de información que permite extraerlos con un programa adecuado, como WinZip.

Cookie

Un mecanismo que almacena en el explorador Web información acerca de un usuario de Internet, como el nombre, las preferencias y los intereses, para usarla en futuras ocasiones. La próxima vez que acceda a algún sitio Web del cual el explorador haya almacenado una cookie, este enviará la cookie al servidor Web, que la utilizará para presentarle páginas Web personalizadas. Puede, por ejemplo, visitar un sitio Web que le dé la bienvenida por su nombre.

Ataque de denegación de servicio

Un ataque de denegación de servicio (DoS) es un ataque al endpoint o a la red que provoca una pérdida de "servicio", es decir, de la conexión de red. Generalmente, los ataques DoS influyen negativamente en el ancho de banda o sobrecargan los recursos del sistema como, por ejemplo, la memoria del endpoint.

DHCP

La función del protocolo de configuración dinámica de host (DHCP) consiste en asignar direcciones IP dinámicas a los dispositivos en una red. Con el direccionamiento

dinámico, un dispositivo puede tener una dirección IP diferente cada vez que se conecte a la red. En algunos sistemas, incluso puede cambiar la dirección IP del dispositivo mientras está conectado. Este protocolo también admite una combinación de direcciones IP dinámicas y estáticas.

DNS

El sistema de nombres de dominio (DNS) es un servicio de consulta de datos de carácter general que se utiliza principalmente en Internet para traducir nombres de host en direcciones IP.

Al proceso por el cual un agente DNS solicita los datos de la dirección y el nombre de host de un servidor DNS se le denomina resolución. La configuración básica DNS resulta en un servidor que realiza la resolución predeterminada. Por ejemplo, un servidor remoto solicita a otro servidor los datos de un equipo en la zona actual. El software del agente del servidor remoto consulta al servidor encargado de la resolución, que responde a la solicitud desde los archivos contenidos en la base de datos.

Nombre del dominio

El nombre completo de un sistema compuesto por el nombre de host local y su nombre de dominio como, por ejemplo, `tellsitall.com`. Un nombre de dominio debe bastar para determinar una dirección exclusiva de Internet para cualquier host de Internet. Este proceso, denominado "resolución del nombre", utiliza el sistema DNS (sistema de nombres de dominios).

Dirección IP dinámica

Una dirección IP dinámica es una dirección IP asignada por un servidor DHCP. La dirección MAC del endpoint seguirá siendo la misma, aunque el servidor DHCP podrá asignar una nueva dirección IP al endpoint según la disponibilidad.

ESMTP

El protocolo simple de transferencia de correo mejorado (ESMTP) incluye seguridad, autenticación y otros dispositivos para ahorrar ancho de banda y proteger los servidores.

Contrato de licencia para usuario final

Un contrato de licencia para usuario final es un contrato legal entre una empresa de software y el usuario del software. Suele describir las restricciones a las que está sometido el usuario, que puede renunciar al acuerdo no seleccionando la opción "Acepto" durante la instalación. Por supuesto, si se hace clic en "No acepto", finalizará la instalación del producto de software.

Gran parte de los usuarios aceptan la instalación de spyware y otros tipos de grayware en sus equipos sin percatarse de ello al hacer clic en "Acepto" en el contrato de licencia que aparece al instalar ciertos productos de software gratuitos.

Falso positivo

Un falso positivo se produce cuando el software de seguridad detecta que un archivo está infectado erróneamente.

FTP

El protocolo de transferencia de archivos (FTP) es un protocolo estándar utilizado para transportar archivos desde un servidor a un cliente a través de Internet. Consulte la RFC 959 sobre Grupo de trabajo de redes para obtener más información.

GeneriClean

La función GeneriClean, también denominada limpieza referencial, es una nueva tecnología de limpieza de virus/malware disponible incluso sin los componentes de

limpieza de virus. Con un archivo detectado como base, GeneriClean determina si el archivo detectado tiene un proceso/servicio correspondiente en memoria y una entrada de registro y los elimina conjuntamente.

Revisión

Un archivo hotfix es una solución para un problema específico que los usuarios han comunicado. Los archivos Hotfix son específicos para un problema y, por lo tanto, no se publican para todos los clientes. Los archivos Hotfix de Windows incluyen programas de instalación, mientras que los archivos Hotfix que no son de Windows no suelen facilitarlos (generalmente es necesario detener los demonios de programas, copiar el archivo para sobrescribir el archivo correspondiente de la instalación y reiniciar los demonios).

De forma predeterminada, los Agentes de OfficeScan pueden instalar archivos HotFix. Si no desea que los Agentes de OfficeScan instalen archivos HotFix, cambie la configuración de actualizaciones del agente en la consola Web. Para ello, vaya a **Agentes** > **Administración de agentes**, haga clic en **Configuración** > **Derechos y otras configuraciones pestaña** > **Otras configuraciones**.

Si intenta implementar sin éxito un archivo hotfix en el servidor de OfficeScan, utilice la herramienta Touch para cambiar la marca de hora de dicho archivo. De esta forma, OfficeScan interpretará que el archivo hotfix es nuevo y hará que el servidor intente instalarlo de nuevo automáticamente. Si desea obtener información detallada sobre esta herramienta, consulte *Ejecutar la herramienta Touch para archivos HotFix de los agentes de OfficeScan en la página 6-57*.

HTTP

El protocolo de transferencia de hipertexto (HTTP) es un protocolo estándar utilizado para transportar páginas Web (incluidos los gráficos y el contenido multimedia) desde un servidor a un cliente a través de Internet.

HTTPS

Protocolo de transferencia de hipertexto que utiliza SSL (Capa de conexión segura). HTTPS es una variante de HTTP utilizada para gestionar transacciones seguras.

ICMP

En ocasiones, los gateway o host de destino utilizan el protocolo de mensajes de control de Internet (ICMP) para comunicarse con un host de origen como, por ejemplo, para notificar un error durante el procesamiento de un datagrama. ICMP utiliza la compatibilidad básica con IP (protocolo de Internet) como si éste se tratara de un protocolo de nivel superior; no obstante, ICMP es en realidad una parte integral de IP que se implementa en todos los módulos IP. Los mensajes ICMP se envían en distintas situaciones: por ejemplo, cuando un datagrama no puede llegar a su destino, cuando un gateway no tiene capacidad de búfer suficiente para reenviar un datagrama y cuando el gateway puede dirigir el host para que envíe el tráfico a través de una ruta más corta. El protocolo de Internet no tiene un diseño que garantice una fiabilidad plena. El objetivo de estos mensajes de control consiste en proporcionar información sobre los problemas ocurridos en el entorno de comunicación, no en asegurar la fiabilidad del protocolo IP.

IntelliScan

IntelliScan es un método para identificar los archivos que se exploran. Cuando se trata de archivos ejecutables (como, por ejemplo, `.exe`), el tipo de archivo verdadero se determina en función del contenido del archivo. Cuando se trata de archivos no ejecutables (por ejemplo, `.txt`), el tipo de archivo verdadero se determina en función del encabezado del archivo.

Utilizar IntelliScan ofrece las siguientes ventajas:

- Optimización del rendimiento: IntelliScan no interfiere en las aplicaciones del agente porque utiliza unos recursos del sistema mínimos.
- Período de exploración más corto: IntelliScan utiliza la identificación de tipo de archivo verdadero, lo que permite explorar únicamente los archivos vulnerables a

infecciones. Por lo tanto, el tiempo de exploración es considerablemente inferior al que se invierte para explorar todos los archivos.

IntelliTrap

Los programadores de virus suelen intentar evitar el filtrado de virus mediante algoritmos de compresión en tiempo real. IntelliTrap ayuda a reducir el riesgo de que estos virus se infiltren en la red mediante el bloqueo de archivos ejecutables comprimidos en tiempo real y el emparejamiento de estos con otras características del malware. IntelliTrap identifica estos archivos como riesgos de seguridad y puede que bloquee incorrectamente archivos seguros; por tanto, es recomendable que ponga en cuarentena (sin eliminar ni limpiar) los archivos tras activar IntelliTrap. Si los usuarios intercambian frecuentemente archivos ejecutables comprimidos en tiempo real, desactive IntelliTrap.

IntelliTrap utiliza los siguientes componentes:

- Motor de Escaneo de Virus
- Patrón de IntelliTrap
- Patrón de Excepciones Intellitrap

IP

"El protocolo de Internet (IP) permite transmitir bloques de datos denominados datagramas desde un origen a un destino, donde tanto el origen como el destino son hosts identificados por direcciones de longitud fija." (RFC 791)

Archivo Java

Java es un lenguaje de programación de carácter general desarrollado por Sun Microsystems. Un archivo Java contiene código Java. Java es compatible con la programación para Internet en forma de "subprogramas" de Java de plataforma independiente. Un subprograma es un programa escrito con lenguaje de programación

Java que puede incluirse en una página HTML. Al utilizar un explorador con la tecnología Java habilitada para ver una página que contiene un subprograma, este último transfiere su código al endpoint y la máquina virtual de Java del explorador ejecuta el subprograma.

LDAP

El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para consultar y modificar servicios de directorio que se ejecuten a través de TCP/IP.

Puerto de escucha

Un puerto de escucha se utiliza para las solicitudes de conexión de los agentes destinadas a intercambiar datos.

Agente de MCP

Trend Micro Management Communication Protocol (MCP) es el agente de Trend Micro de próxima generación para productos administrados. MCP reemplaza a Trend Micro Management Infrastructure (TMI) como medio de comunicación de Control Manager con OfficeScan. MCP incluye varias características nuevas:

- Reducción de la carga de la red y tamaño del paquete
- Compatibilidad con cruce seguro del cortafuegos y NAT
- compatibilidad con HTTPS
- Compatibilidad con la comunicación unidireccional y bidireccional
- Compatibilidad con inicio de sesión único (SSO)
- Compatibilidad con nodo de grupos

Ataque de amenazas mixtas

Los ataques de amenazas mixtas se benefician de diversos puntos de entrada y de vulnerabilidades propios de las redes empresariales, tales como las amenazas “Nimda” o “CodeRed”.

NAT

La traducción de direcciones de red (NAT) es un estándar para la traducción de direcciones IP seguras a direcciones IP registradas, externas y temporales a partir de un grupo de direcciones. De esta forma, se permite que las redes de confianza con direcciones IP asignadas de forma privada tengan acceso a Internet. También significa que el usuario no necesita obtener una dirección IP registrada para cada equipo de la red.

NetBIOS

El sistema básico de entrada y salida de red (NetBIOS) es una interfaz de programación de aplicaciones (API) que añade funcionalidades como, por ejemplo, características de red, al sistema básico de entrada y salida (BIOS) del sistema operativo de disco (DOS).

Comunicación unidireccional

Comunicación unidireccional NAT transversal es un aspecto cada vez más importante en el entorno de red del mundo real actual. Para solucionar este problema, MCP utiliza la comunicación unidireccional. En la comunicación unidireccional, el agente MCP inicia la conexión con el servidor y realiza el sondeo de comandos del mismo. Cada solicitud es una transmisión de registro o consulta de comando similar a CGI. Para reducir el impacto en la red, el agente MCP mantiene la conexión activa y abierta tanto como sea posible. Una solicitud posterior utiliza una conexión abierta existente. Si la conexión se pierde, todas las conexiones SSL con el mismo host se benefician de la caché de ID de la sesión, lo que reduce enormemente el tiempo de reconexión.

Parche

Una revisión es un grupo de archivos hotfix y revisiones de seguridad que solucionan varios problemas del programa. Trend Micro publica revisiones regularmente. Los parches de Windows incluyen un programa de instalación, mientras que los parches que no son de Windows suelen disponer de una secuencia de comandos de instalación.

Ataques de phishing

El phish, o phishing, es una forma de fraude en auge con la que se intenta engañar a los usuarios de Internet para que revelen información privada mediante la imitación de un sitio Web legítimo.

En una situación típica, un usuario desprevenido recibe un mensaje urgente y alarmante (con un aspecto real) que le informa de que hay un problema con su cuenta que se debe resolver de inmediato o, de lo contrario, la cuenta se cerrará. El mensaje de correo electrónico incluye una URL de un sitio Web que tiene el mismo aspecto que el sitio legítimo. Es muy sencillo copiar un mensaje y un sitio Web legítimos y cambiar el denominado "extremo final", que entonces pasa a ser el destinatario de los datos recopilados.

El mensaje de correo le indica al usuario que inicie una sesión en el sitio y que confirme algunos datos de la cuenta. Un hacker recibe los datos que proporciona el usuario, como el nombre de inicio de sesión, la contraseña, el número de la tarjeta de crédito o el número de la seguridad social.

Este tipo de fraude es rápido, barato y muy fácil de realizar. También es potencialmente muy lucrativo para los delincuentes que lo practican. El phish es difícil de detectar, incluso para usuarios informáticos avanzados, y también es complicado de perseguir por parte de las autoridades competentes. Y, lo que es peor, es prácticamente imposible de juzgar legalmente.

Si sospecha de algún posible sitio Web de phishing, comuníqueselo a Trend Micro.

Ping

Se trata de una utilidad que envía una solicitud de eco ICMP a una dirección IP y espera una respuesta. La utilidad Ping puede determinar si el endpoint con la dirección IP que se ha especificado está conectado.

POP3

El protocolo de oficina de correo 3 (POP3) es un protocolo estándar para almacenar y transportar mensajes de correo electrónico desde un servidor a una aplicación de correo electrónico cliente.

Servidor proxy

Un servidor proxy es un servidor de Internet que acepta las direcciones URL con un prefijo especial que se utiliza para recuperar documentos desde un servidor remoto o de caché local y que, a continuación, devuelve la URL al solicitante.

RPC

La llamada de procedimiento remoto (RPC) es un protocolo de red que permite que el programa que se ejecute en un host dé lugar a que el código se ejecute en otro host.

Revisión de seguridad

Una revisión de seguridad se centra en problemas de seguridad que se puedan implementar en todos los clientes. Los parches de seguridad de Windows incluyen un programa de instalación, mientras que los parches que no son de Windows suelen disponer de una secuencia de comandos de instalación.

Service Pack

Un Service Pack es un conjunto de archivos hotfix, revisiones y mejoras funcionales suficientes para considerarse una actualización del producto. Tanto los Service Pack de Windows como los de otros fabricantes incluyen un programa y una secuencia de comandos de instalación.

SMTP

El protocolo simple de transferencia de correo (SMTP) es un protocolo estándar utilizado para transferir mensajes de correo electrónico de un servidor a otro, así como de un agente a un servidor, a través de Internet.

SNMP

El protocolo simple de administración de redes (SNMP) es un protocolo que admite la supervisión de los dispositivos conectados a una red para comprobar si presentan condiciones que requieran atención administrativa.

Captura SNMP

Una captura SNMP (protocolo simple de administración de redes) es un método de envío de notificaciones a administradores de la red que utilizan consolas de administración compatibles con este protocolo.

OfficeScan puede almacenar la notificación en bases de información de administración (MIB). Puede utilizar el explorador de MIB para ver la notificación de captura SNMP.

SSL

La capa de conexión segura (SSL) es un protocolo diseñado por Netscape para ofrecer capas de seguridad de los datos entre los protocolos de las aplicaciones (como HTTP,

Telnet o FTP) y TCP/ IP. Asimismo, este protocolo de seguridad ofrece opciones como el cifrado de datos, la autenticación del servidor, la integridad de los mensajes y autenticación opcional del agente para una conexión TCP/IP.

Certificado SSL

Este certificado digital establece una comunicación HTTPS segura.

TCP

El protocolo de control de transmisión (TCP) es un protocolo totalmente fiable de punto a punto, orientado a la conexión y diseñado para funcionar con jerarquías de capas de protocolos compatibles con aplicaciones multired. TCP utiliza datagramas IP para la resolución de direcciones. Consulte el código RFC 793 de la agencia DARPA sobre el Protocolo de control de la transmisión para obtener información.

Telnet

Telnet es un método estándar para crear interfaces de comunicación entre dispositivos de terminal a través de TCP creando un "terminal virtual de red". Consulte la RFC 854 sobre Grupo de trabajo de redes para obtener más información.

Puerto de troyano

Los programas de caballos de Troya suelen utilizar puertos de troyanos para conectarse a endpoints. Durante una epidemia, OfficeScan bloquea los siguientes números de puerto que los troyanos pueden utilizar.

TABLA E-1. Puertos de troyanos

NÚMERO DE PUERTO	PROGRAMA DE CABALLO DE TROYA	NÚMERO DE PUERTO	PROGRAMA DE CABALLO DE TROYA
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line

Número de puerto	Programa de caballo de Troya	Número de puerto	Programa de caballo de Troya
7300	Net Spy	1234	Valvo line

Puerto de confianza

El servidor y el Agente de OfficeScan utilizan puertos de confianza para comunicarse entre sí.

Si bloquea los puertos de confianza y restaura la configuración normal de red después de una epidemia, los Agentes de OfficeScan no reanudarán la comunicación con el servidor de inmediato. La comunicación entre el agente y el servidor solo se restaurará cuando transcurra el número de horas que se ha especificado en la pantalla Configuración de la prevención frente a epidemias.

OfficeScan utiliza el puerto HTTP (8080 de forma predeterminada) como puerto de confianza del servidor. Durante la instalación puede indicar un número de puerto distinto. Para bloquear este puerto de confianza y el puerto de confianza del Agente de OfficeScan, active la casilla de verificación Bloquear puertos de confianza que aparece en la pantalla Bloqueo de puertos.

El instalador maestro genera el puerto de confianza del Agente de OfficeScan de forma aleatoria durante la instalación.

Determinar los puertos de confianza

Procedimiento

1. Acceda a <Carpeta de instalación del servidor>\PCCSRV.
2. Utilice un editor de textos (p. ej. el Bloc de notas) para abrir el archivo ofcscan.ini.
3. Para el puerto de confianza del servidor, busque la cadena "Master_DomainPort" y compruebe el valor que aparece junto a la misma.

Por ejemplo, si la cadena aparece como `Master_DomainPort=80`, significa que el puerto de confianza del servidor es el puerto 80.

4. Para el puerto de confianza del agente, busque la cadena "Client_LocalServer_Port" y compruebe el valor que aparece junto a esta.

   Por ejemplo, si la cadena aparece como `Client_LocalServer_Port=41375`, significa que el puerto de confianza del agente es el puerto 41375.

Comunicación bidireccional

La comunicación bidireccional es una alternativa a la comunicación unidireccional. Basada en la comunicación unidireccional, pero con un canal HTTP adicional que recibe las notificaciones del servidor, la comunicación bidireccional puede mejorar los envíos en tiempo real y el procesamiento de comandos desde el servidor por parte del agente MCP.

UDP

El protocolo de datagramas de usuario (UDP) es un protocolo de comunicación sin conexión utilizado con IP para que los programas de aplicación envíen mensajes a otros programas. Consulte el código RFC 768 de la agencia DARPA sobre el Protocolo de control de la transmisión para obtener información.

Archivos que no se pueden limpiar

El motor de escaneo de virus no puede limpiar los siguientes archivos:

TABLA E-2. Soluciones para archivos que no se pueden limpiar

ARCHIVO QUE NO SE PUEDE LIMPIAR	EXPLICACIÓN Y SOLUCIÓN
Archivos infectados con troyanos	Los troyanos son programas que ejecutan acciones imprevistas o no autorizadas, por lo general malintencionadas como, por ejemplo, mostrar mensajes, eliminar archivos o formatear discos. Los troyanos no infectan los archivos, por lo que no es necesario limpiarlos. Solución: el motor de Damage Cleanup y la plantilla de Damage Cleanup eliminan troyanos.
Archivos infectados con gusanos	Un gusano es un programa (o conjunto de programas) completo capaz de propagar a otros sistemas endpoint copias funcionales de sí mismo o de sus segmentos. La propagación suele efectuarse mediante conexiones de red o archivos adjuntos de correo electrónico. Los gusanos no se pueden limpiar porque el archivo en sí es un programa completo. Solución: Trend Micro recomienda eliminar los gusanos.
Archivos protegidos contra escritura	Solución: Elimine la protección contra escritura para que se pueda limpiar el archivo.
Archivos protegidos mediante contraseña	Entre los archivos protegidos mediante contraseña se incluyen los archivos comprimidos o archivos de Microsoft Office protegidos con contraseña. Solución: elimine la protección contra contraseña para que se pueda limpiar el archivo.
Copia de seguridad de los archivos WFBS INI	Los archivos con la extensión RB0~RB9 son copias de seguridad de los archivos infectados. El proceso de limpieza crea una copia de seguridad del archivo infectado por si el virus/malware daña el archivo original durante el proceso de limpieza. Solución: si se consigue limpiar el archivo infectado correctamente, no es necesario conservar la copia de seguridad. Si el endpoint funciona con normalidad, puede borrar el archivo de copia de seguridad.
Archivos infectados de la Papelera de reciclaje	Si el sistema está en funcionamiento, es posible que el sistema no permita eliminar los archivos infectados de la Papelera de reciclaje.

Archivo que no se puede limpiar	Explicación y solución

	Solución para Windows XP o Windows Server 2003 con un sistema de archivos NTFS:
	1. Inicie sesión en el endpoint con derechos de administrador.
	2. Cierre todas las aplicaciones en ejecución para evitar que bloqueen el archivo, lo que podría impedir que Windows eliminara los archivos infectados.
	3. Abra el símbolo del sistema.
	4. Escriba lo siguiente para eliminar los archivos:
	`cd \`
	`cd recycled`
	`del *.* /S`
	El último comando elimina todos los archivos de la Papelera de reciclaje.
	5. Compruebe si se han eliminado los archivos.

	Solución para otros sistemas operativos (o aquellos sin NTFS):
	1. Reinicie el endpoint en modo MS-DOS.
	2. Abra el símbolo del sistema.
	3. Escriba lo siguiente para eliminar los archivos:
	`cd \`
	`cd recycled`
	`del *.* /S`
	El último comando elimina todos los archivos de la Papelera de reciclaje.

Archivos infectados de la carpeta temporal de Windows o de Internet Explorer	Es posible que el sistema no permita limpiar los archivos infectados en la carpeta temporal de Windows o de Internet Explorer debido a que el endpoint esté usando estos archivos. Los archivos que intenta limpiar pueden ser archivos temporales necesarios para el funcionamiento de Windows.

ARCHIVO QUE NO SE PUEDE LIMPIAR	EXPLICACIÓN Y SOLUCIÓN

	Solución para Windows XP o Windows Server 2003 con un sistema de archivos NTFS:
	1. Inicie sesión en el endpoint con derechos de administrador.
	2. Cierre todas las aplicaciones en ejecución para evitar que bloqueen el archivo, lo que podría impedir que Windows eliminara los archivos infectados.
	3. En caso de que el archivo infectado se encuentre en la carpeta temporal de Windows:
	a. Abra el símbolo del sistema y vaya a la carpeta temporal de Windows (ubicada de forma predeterminada en `C:\Windows\Temp` en el caso de equipos con endpoints Windows XP o Windows Server 2003).
	b. Escriba lo siguiente para eliminar los archivos:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	El último comando elimina todos los archivos de la carpeta temporal de Windows.
	4. En caso de que el archivo infectado se encuentre en la carpeta temporal de Internet Explorer:
	a. Abra el símbolo del sistema y vaya a la carpeta temporal de Internet Explorer (ubicada de forma predeterminada en `C:\Documents and Settings\<Su nombre de usuario>\Configuración local\Archivos temporales de Internet` para endpoints con Windows XP o Windows Server 2003).
	b. Escriba lo siguiente para eliminar los archivos:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`

ARCHIVO QUE NO SE PUEDE LIMPIAR	EXPLICACIÓN Y SOLUCIÓN
	El último comando elimina todos los archivos de la carpeta temporal de Internet Explorer. c. Compruebe si se han eliminado los archivos.

	Solución para otros sistemas operativos (o aquellos sin NTFS):
	1. Reinicie el endpoint en modo MS-DOS.
	2. En caso de que el archivo infectado se encuentre en la carpeta temporal de Windows:
	a. Abra el símbolo del sistema y vaya a la carpeta temporal de Windows (ubicada de forma predeterminada en `C:\Windows\Temp` en el caso de equipos con endpoints Windows XP o Windows Server 2003).
	b. Escriba lo siguiente para eliminar los archivos:
	`cd temp`
	`attrib -h`
	`del *.* /S`
	El último comando elimina todos los archivos de la carpeta temporal de Windows.
	c. Reinicie el endpoint en modo normal.
	3. En caso de que el archivo infectado se encuentre en la carpeta temporal de Internet Explorer:
	a. Abra el símbolo del sistema y vaya a la carpeta temporal de Internet Explorer (ubicada de forma predeterminada en `C:\Documents and Settings\<Su nombre de usuario>\Configuración local\Archivos temporales de Internet` para endpoints con Windows XP o Windows Server 2003).
	b. Escriba lo siguiente para eliminar los archivos:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`

ARCHIVO QUE NO SE PUEDE LIMPIAR	EXPLICACIÓN Y SOLUCIÓN
	El último comando elimina todos los archivos de la carpeta temporal de Internet Explorer. c. Reinicie el endpoint en modo normal.
Archivos comprimidos con un formato de compresión no admitido	Solución: descomprima los archivos.
Archivos bloqueados o archivos actualmente en ejecución	Solución: desbloquee los archivos o espere hasta que se hayan ejecutado.
Archivos dañados	Solución: borre los archivos.

Archivos infectados con troyanos

Los troyanos son programas que ejecutan acciones imprevistas o no autorizadas, por lo general malintencionadas como, por ejemplo, mostrar mensajes, eliminar archivos o formatear discos. Los troyanos no infectan los archivos, por lo que no es necesario limpiarlos.

Solución: OfficeScan usa el motor de Damage Cleanup y la plantilla de Damage Cleanup para eliminar troyanos.

Archivos infectados con gusanos

Un gusano es un programa (o conjunto de programas) completo capaz de propagar a otro endpoint copias funcionales de sí mismo o de sus segmentos. La propagación suele efectuarse a través de conexiones de red o archivos adjuntos de correo electrónico. Los gusanos no se pueden limpiar porque el archivo en sí es un programa completo.

Solución: Trend Micro recomienda eliminar los gusanos.

Archivos protegidos contra escritura

Solución: quite la protección contra escritura para que OfficeScan pueda limpiar el archivo.

Archivos protegidos mediante contraseña

Incluye los archivos comprimidos o archivos de Microsoft Office protegidos mediante contraseña.

Solución: quite la protección con contraseña para que OfficeScan pueda limpiar los archivos.

Archivos de copia de seguridad

Los archivos con las extensiones RB0~RB9 son copias de seguridad de los archivos infectados. OfficeScan crea una copia de seguridad del archivo infectado por si el virus/malware daña el archivo original durante el proceso de limpieza.

Solución: si OfficeScan consigue limpiar el archivo infectado correctamente, no es necesario conservar la copia de seguridad. Si el endpoint funciona con normalidad, puede borrar el archivo de copia de seguridad.

Índice

A

acción en los sucesos del sistema supervisado, 9-8
acciones
    Prevención de pérdida de datos, 11-41
Acciones de exploración, 7-38
    spyware/grayware, 7-52
    virus/malware, 7-80
ActiveAction, 7-39
Active Directory, 2-42–2-44, 2-61, 2-66, 5-17, 5-35
    administración de servidores externos, 2-42
    agrupación de agentes, 2-61
    alcance y consulta, 15-77
    credenciales, 2-43
    duplicar estructura, 2-66
    grupos de agentes personalizados, 2-42
    integración, 2-42
    Sincronización, 2-44
ActiveSync, 11-40
actualización del agente
    activada por suceso, 6-42
    actualización programada, 6-43
    actualización programada con NAT, 6-45
    Automático, 6-41
    derechos, 6-50
    desactivado, 6-51
    desde el servidor ActiveUpdate, 6-50
    fuente estándar, 6-34
    fuente personalizada, 6-35
    manual, 6-48
Actualización del servidor
    actualización manual, 6-27
    actualización programada, 6-28
    configuración del proxy, 6-20
    Duplicación de componentes, 6-22
    métodos de actualización, 6-27
    registros, 6-29
actualización de OfficeScan, 6-13
Actualizaciones, 4-19, 4-20
    Agente de actualización, 6-59
    agentes, 6-30
    aplicar, 6-56
    Servidor de OfficeScan, 6-16
    Smart Protection Server integrado, 4-19, 4-20
actualizar
    Smart Protection Server, 6-15, 6-29
Actualizar ahora, 6-51
administración de servidores externos, 2-42, 15-76
    consulta programada, 15-81
    registros, 18-9
    resultados de la consulta, 15-80
administrador de cuarentena, 14-65
Agente de actualización, 5-4, 5-7, 6-59
    asignación, 6-59
    Duplicación de componentes, 6-65
    fuente de actualización estándar, 6-62
    informe analítico, 6-67
    métodos de actualización, 6-66
    requisitos de sistema, 6-59
agente de OfficeScan
    procesos, 15-17
Agente de OfficeScan
    agentes inactivos, 15-27
    archivos, 15-15

claves de registro, 15-17
conexión con el servidor de OfficeScan, 15-28, 15-44
conexión con el Smart Protection Server, 15-45
desinstalación, 5-78
espacio de disco reservado, 6-52
importar y exportar configuración, 15-61
información detallada sobre los agentes, 15-60
métodos de instalación, 5-13
agentes, 2-61, 2-68, 2-70, 4-32, 5-2
agrupamiento, 2-61
características, 5-3
conexión, 4-32
configuración del proxy, 4-32
eliminar, 2-68
instalación, 5-2
mover, 2-70
ubicaciones, 4-32
agentes inactivos, 15-27
Agentes independientes, 5-7, 5-10
agentes no accesibles, 15-49
agent mover, 15-24
Agent Packager, 5-17, 5-29, 5-33, 5-35, 5-37
configuración, 5-32
implementación, 5-30
agrupación automática de agentes, 2-62, 2-63
agrupación de agentes, 2-61–2-63, 2-65–2-70
Active Directory, 2-61, 2-65
añadir un dominio, 2-68
Automático, 2-62, 2-63
cambiar el nombre de un dominio, 2-69
direcciones IP, 2-66
DNS, 2-61
eliminar un dominio o agente, 2-68
grupos personalizados, 2-62
manual, 2-61, 2-62
métodos, 2-61
mover agentes, 2-70
NetBIOS, 2-61
tareas, 2-67
agrupación manual de agentes, 2-61, 2-62
amenazas desconocidas, 8-11
registros, 8-11
amenazas web, 12-2
Aplicaciones de MI, 11-29
árbol de agentes, 2-45, 2-49–2-52, 2-56–2-59
acerca de, 2-45
búsqueda avanzada, 2-50, 2-51
filtros, 2-50
tareas específicas, 2-52, 2-56–2-59
actualizaciones manuales de componentes, 2-57
administración de agentes, 2-52
Prevención de epidemias, 2-56
recuperar actualizaciones de componentes, 2-58
registros de riesgos de seguridad, 2-59
tareas generales, 2-49
vistas, 2-50
archivos cifrados, 7-48
archivos comprimidos, 7-30, 7-80
reglas de descompresión, 11-45
archivos de patrones
Lista de bloqueo Web, 4-9
smart protection, 4-8
Smart Scan Agent Pattern, 4-9
Smart Scan Pattern, 4-9
Archivos Hotfix, 6-11, 6-57

ARP en conflicto, 13-5
Ataque con fragmentos pequeños, 13-5
Ataque LAND, 13-6
atributos de archivo, 11-6, 11-11, 11-13, 11-14
    comodines, 11-13
    crear, 11-13
    importación, 11-14
    predefinidas, 11-12
AutoPcc.exe, 5-15, 5-16, 5-26, 5-27
autoprotección del agente, 15-13

B

Bloqueo de comportamiento de malware, 9-2
bloqueo de puertos, 7-121

C

caché de exploración, 7-70
caché de la exploración bajo petición, 7-72
caché de la firma digital, 7-71
canales de aplicaciones y sistemas, 11-26, 11-34, 11-35, 11-38–11-41
    almacenamiento extraíble, 11-39
    CD/DVD, 11-35
    Cifrado PGP, 11-38
    Cloud Storage Service, 11-34
    impresora, 11-38
    Portapapeles de Windows, 11-41
    programas Peer To Peer (P2P), 11-38
    software de sincronización, 11-40
canales de red, 11-26, 11-27, 11-29–11-31, 11-33, 11-34, 11-44
    alcance de la transmisión, 11-34
        conflictos, 11-34
        todas las transmisiones, 11-31
        transmisiones externas, 11-33
    Aplicaciones de MI, 11-29
    clientes de correo electrónico, 11-27
    correo electrónico Web, 11-31
    destinos no supervisados, 11-34, 11-44
    destinos supervisados, 11-34, 11-44
    destinos y alcance de la transmisión, 11-31
    FTP, 11-29
    HTTP y HTTPS, 11-29
    Protocolo SMB, 11-30
Código malicioso ActiveX, 7-4
Código malicioso Java, 7-4
comodines, 11-13
    atributos de archivo, 11-13
    control de dispositivos, 10-10
Compatibilidad con IPv6, A-2
    limitaciones, A-3, A-4
    visualización de direcciones IPv6, A-7
componentes, 2-8, 2-22–2-26, 2-28, 2-30–2-32, 2-34–2-37, 5-77, 6-2, 17-3
    Actualizaciones del agente, 2-36
    Agentes conectados a Edge Relay Server, 2-34
    Conectividad del agente antivirus, 2-32
    Conectividad entre agente y servidor, 2-37
    derechos y configuración de actualización, 6-50
    Detección de riesgos de seguridad, 2-30
    en el agente, 6-30
    en el agente de actualización, 6-59
    en el servidor de OfficeScan, 6-16
    Epidemias, 2-35
    Eventos de rellamada de C&C, 2-28
    Fuentes de amenazas principales de la reputación Web, 2-24
    Mapa de amenazas de la reputación de ficheros, 2-22

OfficeScan y Plug-ins Mashup, 2-31
Prevención de pérdida de datos - Detecciones durante un tiempo, 2-25
Prevención de pérdida de datos - Detecciones más importantes, 2-26
resumen de la actualización, 6-68
Usuarios con amenazas principales de la reputación Web, 2-23
Comprobación de la conexión, 15-47
condiciones, 11-22
configuración de DHCP, 5-52
Configuración de inicio de sesión, 5-15, 5-16, 5-26, 5-27
configuración de la caché para las exploraciones, 7-70
configuración del proxy, 4-32
agentes, 4-32
configuración automática del proxy, 15-59
derechos, 15-57
para la actualización de componentes del servidor, 6-20
para la conexión externa, 15-55
para la conexión interna, 15-54
Configuración de servicios adicionales, 15-7
Conformidad con las normas de seguridad, 15-62
administración de servidores externos, 2-42, 15-76
aplicar, 15-77
aplicar actualización, 6-56
componentes, 15-66
Configuración, 15-70
Explorar, 15-68
instalación, 5-68
registros, 18-9
servicios, 15-64
valoraciones programadas, 15-75
conocimiento de ubicación, 15-2
consola del agente
restricción de acceso, 15-18
consola Web, 1-7, 2-2–2-4
acerca de, 2-2
actualización, 2-3
banner, 2-4
contraseña, 2-4
cuenta de inicio de sesión, 2-4
URL, 2-3
continuidad de protección, 4-11
contraseña, 14-64
Contrato de licencia para usuario final (EULA), E-4
Controlador de consultas de inteligencia contextual, 6-6
Controlador de la exploración antivirus, 6-3
Controlador de la supervisión de comportamiento, 6-8
Controlador del cortafuegos habitual, 6-8
control de dispositivos, 10-2, 10-4, 10-6–10-13, 10-15
actualización, 10-2
administración del acceso, 10-11, 10-15
comodines, 10-10
dispositivos de almacenamiento, 10-4, 10-6, 10-7
dispositivos externos, 10-11, 10-15
dispositivos sin almacenamiento, 10-11
dispositivos USB, 10-13
Lista de permitidos, 10-13
permisos, 10-4, 10-6, 10-7, 10-9, 10-11
ruta y nombre de programa, 10-9
permisos avanzados, 10-12

configurar, 10-12
Proveedor de firmas digitales, 10-8
Control de dispositivos, 1-9
Notificaciones, 10-19
registros, 10-19, 18-10
control de dispositivos;lista de control de dispositivos;lista de control de dispositivos:adición de programas, 10-17
control del rendimiento, 7-31
Control Manager
integración con OfficeScan, 14-26
registros del Agente de MCP, 18-11
copia de seguridad de la base de datos, 14-50
correo electrónico Web, 11-31
Cortafuegos, 5-4, 5-8, 13-2
derechos, 13-6, 13-24
desactivar, 13-6
excepciones de las políticas predeterminadas, 13-14, 13-15
excepciones de políticas, 13-13
perfiles, 13-4, 13-17
políticas, 13-9
probar, 13-34
supervisor de epidemias, 13-6
tareas, 13-8
ventajas, 13-2
criterios
expresiones personalizadas, 11-8, 11-9
palabras clave, 11-17, 11-18
criterios de epidemia, 7-114, 12-20, 13-32
criterios de exploración
Actividad del usuario en los archivos, 7-28
archivos para explorar, 7-29
compresión de archivos, 7-30
programa, 7-32
Uso de la CPU, 7-31
cuentas de usuario, 2-5
panel, 2-5

D

Damage Cleanup Services, 1-8, 5-4, 5-8
derechos
derecho de descarga, 15-19
Derecho del modo independiente, 15-20
Derechos de exploración, 7-59
derechos de exploración del correo, 7-68
Derechos de exploración programada, 7-62
derechos de la configuración del proxy, 15-57
derechos del cortafuegos, 13-24, 13-26
Derechos de exploración, 7-59
Desbordamiento SYN, 13-5
desinstalación, 5-78
desde la consola Web, 5-79
Plug-in Manager, 17-12
programa de complemento, 17-12
Protección de datos, 3-15
uso del programa de desinstalación, 5-79
desinstalación del agente, 5-78
destinos no supervisados, 11-31, 11-33
destinos supervisados, 11-32, 11-33
Detección de rootkits, 6-8
dirección IP del gateway, 15-3
Dirección MAC, 15-3
directorio de cuarentena, 7-42, 7-48
dispositivos de almacenamiento
permisos, 10-4
permisos avanzados, 10-6, 10-7
dispositivos externos
administración del acceso, 10-11, 10-15

dispositivos sin almacenamiento
permisos, 10-11
dispositivos USB
Lista de permitidos, 10-13
configurar, 10-13
documentación, xiv
dominios, 2-61, 2-68, 2-69
agregar, 2-68
agrupación de agentes, 2-61
cambiar el nombre, 2-69
eliminar, 2-68
dominios de correo electrónico, 11-27
dominios de correo electrónico no supervisados, 11-27
Driver del Cortafuegos común, 18-21
DSP, 10-8
Duplicación de componentes, 6-22, 6-65

E

Early Boot Cleanup Driver, 6-7
Enciclopedia de virus, 7-5
escaneo de cookies, 7-84
Estadísticas de los 10 principales riesgos de seguridad para los endpoints en red, 2-35
Evaluación de la documentación, 19-6
exclusiones de la exploración, 7-33
archivos, 7-36
directorios, 7-34
extensiones de los archivos, 7-37
exploración convencional, 7-10, 7-11
cambiar a Smart Scan, 7-11
Exploración de correo, 7-68
exploración de la base de datos, 7-79
Exploración del servidor de Microsoft Exchange, 7-79
exploración de prueba, 5-77
Exploración de spyware/grayware
acciones, 7-52
Lista de permitidos, 7-53
resultados, 7-108
Exploración de virus/malware
configuración general, 7-75
resultados, 7-99
Exploración en tiempo real, 7-16
Exploración manual, 7-19
acceso directo, 7-77
Exploración programada, 7-21
detener automáticamente, 7-86
omitir y detener, 7-63, 7-86
posponer, 7-85
reanudar, 7-86
recordatorio, 7-85
Explorar ahora, 7-24
Exportar configuración, 15-61
expresiones, 11-6
Personalizado, 11-7, 11-11
criterios, 11-8, 11-9
predefinidas, 11-6, 11-7
expresiones personalizadas, 11-7–11-9, 11-11
criterios, 11-8, 11-9
importación, 11-11
Expresiones predefinidas, 11-6
ver, 11-7
Expresiones regulares compatibles con Perl, 11-8

F

Falso antivirus, 7-45
file reputation, 4-3
filtro de aplicaciones, 13-3
Fragmento demasiado grande, 13-4
FTP, 11-29
fuente de actualización
agentes, 6-33

Agentes de actualización, 6-61
Servidor de OfficeScan, 6-19
función de usuario
administrador, 14-10
Usuario avanzado de Trend, 14-11
usuario invitado, 14-11

G

gateway settings importer, 15-5
grupos de agentes personalizados, 2-42, 2-62
Gusanos, 7-4

H

Herramienta de ajuste del rendimiento, 18-2
Herramienta de creación de plantillas de exploración previa de VDI, 15-93
Herramienta de diagnóstico de casos, 18-2
Herramienta de lista de dispositivos, 10-14
Herramienta de migración de SQL Server, 14-52, 14-55
configurar, 14-52
notificación de alerta, 14-55
herramienta Touch, 6-57
HTTP y HTTPS, 11-29

I

identificadores de datos, 11-6
atributos de archivo, 11-6
expresiones, 11-6
palabras clave, 11-6
IDS, 13-4
IGMP fragmentado, 13-5
imagen de disco de agente, 5-17, 5-42
Importar configuración, 15-61
Infector de archivos COM, 7-4
Infector de archivos EXE, 7-4
información del servidor web, 14-56
Informe de conformidad, 15-63
instalación, 5-2
agente, 5-2
Conformidad con las normas de seguridad, 5-68
Plug-in Manager, 17-3
programa de complemento, 17-5
Protección de datos, 3-2
instalación de agentes, 5-2, 5-27
Agent Packager, 5-29
basada en explorador, 5-22
Configuración de inicio de sesión, 5-26
desde la consola Web, 5-23
desde la página Web de instalación, 5-19
mediante la imagen de disco de agente, 5-42
mediante Vulnerability Scanner, 5-43
posterior a la instalación, 5-75
requisitos de sistema, 5-2
uso de la conformidad con las normas de seguridad, 5-68
instalación remota, 5-16
IntelliScan, 7-29
intranet, 4-13
IPv6, 4-23
soporte, 4-23
IpXfer.exe, 15-24

L

Licencias, 14-47
estado, 2-6
Protección de datos, 3-4
Lista de bloqueo Web, 4-9, 4-21
lista de excepción, 9-10
Supervisión del comportamiento, 9-10
Lista de IP de C&C general, 6-10
Lista de permitidos, 7-53

lista de programas bloqueados, 9-10
lista de programas permitidos, 9-10
Lista de software seguro certificado, 13-3
LogServer.exe, 18-3, 18-15

M

método de exploración, 5-31
    Predeterminado, 7-9
métodos de actualización
    Agente de actualización, 6-66
    agentes, 6-40
    Servidor de OfficeScan, 6-27
Microsoft SMS, 5-17, 5-37
migración
    desde servidores ServerProtect normales, 5-72
    desde software de seguridad de otros fabricantes, 5-71
modo de valoración, 7-83
motor de Damage Cleanup, 6-7
Motor de exploración antivirus, 6-3
Motor de exploración de amenazas avanzadas, 6-6
Motor de exploración de spyware/grayware, 6-7
Motor de filtrado de URL, 6-12
Motor de inteligencia contextual, 6-5

N

NetBIOS, 2-61
Network VirusWall Enforcer, 4-32
notificaciones
    actualización del agente, 6-54
    detección de amenazas web, 12-14
    detección de spyware/grayware, 7-53
    detección de virus o malware, 7-46
    Detecciones de rellamada de C&C, 12-19
    infracciones del cortafuegos, 13-29
    para administradores, 11-56
    para usuarios de agentes, 7-94, 11-60
    patrón de virus obsoleto, 6-55
    reinicio del endpoint, 6-55
Notificaciones
    Control de dispositivos, 10-19
    epidemias, 7-114, 12-20, 13-32
    para administradores, 14-39

O

OfficeScan
    acerca de, 1-2
    actualización de componentes, 5-77
    agente, 1-11
    componentes, 2-36, 6-2
    consola Web, 2-2
    copia de seguridad de la base de datos, 14-50
    documentación, xiv
    exploración de la base de datos, 7-79
    Funciones y ventajas principales , 1-5
    Licencias, 14-47
    Programas, 2-36
    registros, 14-43
    servicios del agente, 15-12
    servidor web, 14-56
operadores lógicos, 11-22

P

packer, 7-2
página Web de instalación, 5-13, 5-14, 5-19
palabras clave, 11-6, 11-15
    Personalizado, 11-16–11-18, 11-20

predefinidas, 11-15, 11-16
palabras clave personalizadas, 11-16
criterios, 11-17, 11-18
importación, 11-20
palabras clave predefinidas
distancia, 11-16
número de palabras clave, 11-15
panel, 2-5
cuentas de usuario, 2-5
paneles
Resumen, 2-6, 2-8
panel resumen
componentes y programas, 2-36
panel Resumen, 2-6, 2-8
componentes, 2-8
estado de la licencia del producto, 2-6
pestañas, 2-8
Paquete MSI, 5-17, 5-35, 5-37
Patrón de activación de exploración de memoria, 6-9
Patrón de aplicación de políticas, 6-9
Patrón de configuración de la supervisión de comportamiento, 6-8
Patrón de correlación de amenazas avanzadas, 6-6
Patrón de Damage Recovery, 6-9
Patrón de detección de la supervisión de comportamiento, 6-8
Patrón de excepciones de IntelliTrap, 6-4
Patrón de firmas digitales, 6-9, 7-71
Patrón de inteligencia contextual, 6-5
Patrón de IntelliTrap, 6-4
Patrón del cortafuegos habitual, 6-8
Patrón de prevención de explotación del explorador, 6-10
Patrón de regla de relevancia, 6-10
Patrón de spyware y grayware, 6-7
Patrón de supervisión activa de spyware, 6-7
Patrón de supervisión de inspección del programa, 6-9
Patrón de virus, 6-3, 6-55, 6-56
patrones incrementales, 6-22
Patrón unificado del analizador de secuencias de comando, 6-10
PCRE, 11-8
permisos
avanzados, 10-12
dispositivos de almacenamiento, 10-4
dispositivos sin almacenamiento, 10-11
ruta y nombre de programa, 10-9
permisos avanzados
configurar, 10-12
dispositivos de almacenamiento, 10-6, 10-7
pestañas, 2-8
phishing, E-10
Ping de la muerte, 13-4
Plantilla de Damage Cleanup, 6-7
plantillas, 11-21–11-23, 11-25
condiciones, 11-22
operadores lógicos, 11-22
Personalizado, 11-22, 11-23, 11-25
predefinidas, 11-22
plantillas personalizadas, 11-22
crear, 11-23
importación, 11-25
plantillas predefinidas, 11-22
Plug-in Manager, 1-6, 5-7, 5-9, 17-2
administración de las características nativas, 17-4
desinstalación, 17-12
instalación, 17-3

solución de problemas, 17-13
Política, 11-3
Política de prevención de epidemias
archivos ejecutables comprimidos, 7-125
bloquear puertos, 7-121
denegar el acceso a los archivos comprimidos, 7-125
denegar el acceso de escritura, 7-123
exclusiones mutuas, 7-124
gestión de mutex, 7-124
limitar/Denegar el acceso a las carpetas compartidas, 7-120
políticas
Cortafuegos, 13-4, 13-9
Prevención de pérdida de datos, 11-50
reputación Web, 12-5
Portapapeles de Windows, 11-41
Prevención de epidemias, 2-35
desactivar, 7-126
políticas, 7-120
prevención de pérdida de datos
canales de aplicaciones y sistemas, 11-34
canales de red, 11-31, 11-33
Prevención de pérdida de datos, 11-2, 11-3, 11-6
acciones, 11-41
atributos de archivo, 11-11–11-14
canales, 11-26
canales de aplicaciones y sistemas, 11-34, 11-35, 11-38–11-41
canales de red, 11-26, 11-27, 11-29–11-31, 11-34, 11-44
componentes, 2-25, 2-26
expresiones, 11-6–11-9, 11-11
identificadores de datos, 11-6
palabras clave, 11-15–11-18, 11-20
plantillas, 11-21–11-23, 11-25
Política, 11-3
políticas, 11-50
reglas de descompresión, 11-45
Programa de broma, 7-2
Programa de caballo de Troya, 6-7, 7-3
programa de complemento
activar, 3-4, 17-7
desinstalar, 17-12
instalación, 17-5
Programas, 2-36, 6-2
Protección de datos, 11-2
desinstalación, 3-15
estado, 3-9
implementación, 3-6
instalación, 3-2
licencia, 3-4
protección de los dispositivos externos, 6-8
protección inteligente, 4-6
Smart Protection Network, 4-6
Protocolo SMB, 11-30
Proveedor de firmas digitales, 10-8
especificación, 10-8
ptngrowth.ini, 4-18

R

Recuento de registros del cortafuegos, 13-27
Recursos de solución de problemas, 18-1
registros, 14-43
amenazas desconocidas, 8-11
registros de actualización de los agentes, 6-55
registros de archivos sospechosos, 7-111
registros de Central Quarantine Restore, 7-106
registros de comprobación de la conexión, 15-48

Registros de control de dispositivos, 10-19
registros de exploración, 7-113
registros del cortafuegos, 13-25, 13-26, 13-30
registros de reputación Web, 12-22
registros de restauración de spyware y grayware, 7-111
registros de riesgos de seguridad, 7-98
registros de spyware/grayware, 7-107
registros de sucesos del sistema, 14-41
registros de virus/malware, 7-77, 7-98
sobre, 14-43
Supervisión del comportamiento, 9-18
Registros de depuración
agentes, 18-15
servidor, 18-3
registros del agente
registro de actualizaciones/Hotfix, 18-17
registros de actualización de los agentes, 18-18
registros de conexiones de agentes, 18-18
Registros de Damage Cleanup Services, 18-17
Registros de depuración, 18-15
Registros de depuración de la supervisión de comportamiento, 18-20
registros de depuración de OfficeScan firewall, 18-21
registros de depuración de prevención de epidemias, 18-19
Registros de depuración de protección de datos, 11-67, 18-25
Registros de depuración de TDI, 18-27
registros de exploración de correo, 18-18
registros de instalación nueva, 18-16
Registros del servidor
Registros de Active Directory, 18-6
registros de actualización de componentes, 18-7
registros de administración de servidores externos, 18-9
Registros de Agent Packager, 18-8
registros de agrupación de agentes, 18-7
Registros de conformidad con las normas de seguridad, 18-9
Registros de control de dispositivos, 18-10
Registros de depuración, 18-3
registros de depuración del motor de Escaneo de Virus, 18-19
registros de depuración de ServerProtect Migration Tool, 18-11
registros de depuración de VSEncrypt, 18-11
registros de instalación/actualización local, 18-5
registros de instalación/actualización remota, 18-5
registros del agente MCP de Control Manager, 18-11
registros de reputación Web, 18-10
registros de role-based administration, 18-6
Registros de Soporte de Virtual Desktop, 18-14
reglas de descompresión, 11-45
reinicio del servicio, 15-12
Rellamadas de C&C

componentes, 2-28
configuración general
listas de IP definida por el usuario, 8-6
reputación Web, 1-8, 5-4, 5-8, 12-4
políticas, 12-5
registros, 18-10
requisitos de sistema
Agente de actualización, 6-59
resumen
Actualizaciones, 6-68
panel, 2-6, 2-8
Revisiones, 6-11
Revisiones de seguridad, 6-11
riesgos de seguridad, 7-5–7-7
spyware/grayware, 7-5–7-7
Riesgos de seguridad, 7-2
ataques de phishing, E-10
protección desde, 1-7
role-based administration, 14-3
cuentas de usuario, 14-14
funciones de usuario, 14-3
rootkit, 7-3

S

Secuencia de comandos de prueba EICAR, 5-77, 7-3
ServerProtect, 5-72
Server Tuner, 14-66
Servicio básico de la supervisión de comportamiento, 6-8
Servicio de exploración en tiempo real, 15-44
Servicio de software seguro certificado, 7-76, 9-14, 13-27
Servicios de Command & Control Contact Alert, 12-2
Analizador virtual, 12-3
Lista Analizador virtual, 12-3
Lista Global Intelligence, 12-3
Smart Protection Server, 12-3
Servicios de File Reputation, 4-3
Servicios de reputación Web, 4-3, 4-4
Servidor de OfficeScan, 1-9
funciones, 1-9
servidor de referencia, 14-36
servidor independiente, 4-7
servidor integrado, 4-7
Sistema de detección de intrusiones, 13-4
Smart Feedback, 4-3
smart protection, 4-7, 4-8, 4-10, 4-24
archivos de patrones, 4-8, 4-10
proceso de actualización, 4-10
fuente, 4-7, 4-8
fuentes, 4-24
comparación, 4-7
protocolos, 4-8
ubicaciones, 4-24
Smart Protection, 4-3, 4-4, 4-7, 4-9, 4-13, 4-23
archivos de patrones, 4-9
Lista de bloqueo Web, 4-9
Smart Scan Agent Pattern, 4-9
Smart Scan Pattern, 4-9
entorno, 4-13
fuentes, 4-23
Compatibilidad con IPv6, 4-23
Servicios de File Reputation, 4-3
Servicios de reputación Web, 4-3, 4-4
Smart Protection Server, 4-7
volumen de amenazas, 4-3
Smart Protection Network, 1-2, 4-6
Smart Protection Server, 4-7, 4-14, 4-17–4-21
actualizar, 6-15, 6-29
independiente, 4-7, 4-18

instalación, 4-14
integrado, 4-7, 4-18–4-21
prácticas recomendadas, 4-17
Smart Protection Server independiente, 4-18
ptngrowth.ini, 4-18
Smart Protection Server integrado, 4-18
actualizar, 4-19, 4-20
componentes, 4-20
Lista de bloqueo Web, 4-21
ptngrowth.ini, 4-18
smart scan, 7-10, 7-11
cambiar de la exploración convencional, 7-11
Smart Scan Agent Pattern, 4-9
Smart Scan Pattern, 4-9
software de seguridad de otros fabricantes, 5-69
Solapamiento de fragmentos, 13-5
solución de problemas
Plug-in Manager, 17-13
soporte
solución de problemas más rápida, 19-4
Soporte de sistema de inteligencia, 2-5, 18-2
Soporte de Virtual Desktop, 15-82
spyware/grayware, 7-5–7-7
adware, 7-6
amenazas potenciales, 7-6
aplicaciones de robo de contraseñas, 7-6
herramienta de acceso remoto, 7-6
herramientas de piratería, 7-6
programas de broma, 7-6
programas de marcación, 7-6
protección frente a, 7-7
restaurar, 7-56
spyware, 7-5
subdominios de correo electrónico supervisados, 11-27
sucesos del sistema supervisado, 9-6
Supervisión de eventos, 9-6
Supervisión del comportamiento, 9-18
acción en los sucesos del sistema, 9-8
lista de excepción, 9-10
registros, 9-18

T

tareas previas a la instalación, 5-21, 5-24, 5-68
Teardrop, 13-5
terminología, xvi
tipos de exploración, 5-3, 5-7
Tipos de exploración, 7-15
TMPerftool, 18-2
TMTouch.exe, 6-57
Troyano, 1-8

U

ubicaciones, 4-32
conocimiento, 4-32
Uso de la CPU, 7-31

V

valoraciones programadas, 15-75
VDI, 15-82
registros, 18-14
versión de prueba, 14-47
virus/malware, 7-2–7-5
Código malicioso ActiveX, 7-4
Código malicioso Java, 7-4
Gusanos, 7-4
infector de archivos COM y EXE, 7-4
packer, 7-2
Programa de broma, 7-2
Programa de caballo de Troya, 7-3

rootkit, 7-3
tipos, 7-2–7-5
virus/malware probables, 7-5
Virus de macro, 7-4
Virus de prueba, 7-3
Virus de sector de arranque, 7-4
Virus de VBScript, JavaScript o HTML, 7-4
virus/malware probables, 7-5, 7-101
Virus de macro, 7-4
Virus de prueba, 7-3
virus de red, 7-4
Virus de red, 13-3
Virus de sector de arranque, 7-4
Virus HTML, 7-4
Virus JavaScript, 7-4
Virus VBScript, 7-4
Vulnerability Scanner, 5-18, 5-43
configuración de DHCP, 5-52
configuración del comando ping, 5-65
consulta del producto, 5-59
eficacia, 5-43
protocolos compatibles, 5-61
recuperación de la descripción de Endpoints., 5-62

W

Windows Server Core, B-2
características del agente disponibles, B-6
comandos, B-7
métodos de instalación compatibles, B-2

TREND MICRO INCORPORATED

TREND MICRO España Plaza de las Cortes, 4 – 8º Izq. Madrid, 28014 España

Teléfono: +34 91 369 70 30 Fax: +34 91 369 70 31 reception_es@trendmicro.es

www.trendmicro.com

Item Code: OSSMXG7606/161028