Best Practices

Endpoint Security – Apex One & Apex Central

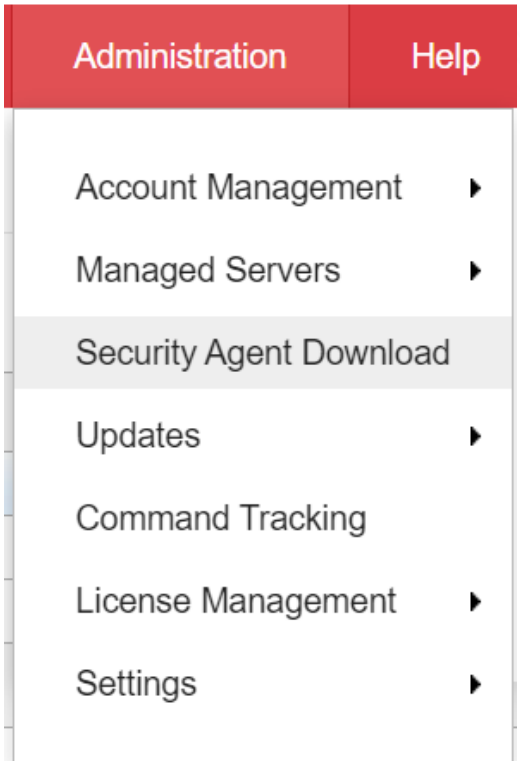
EDSI Trend Argentina S.A
Abril 2023

Introducción

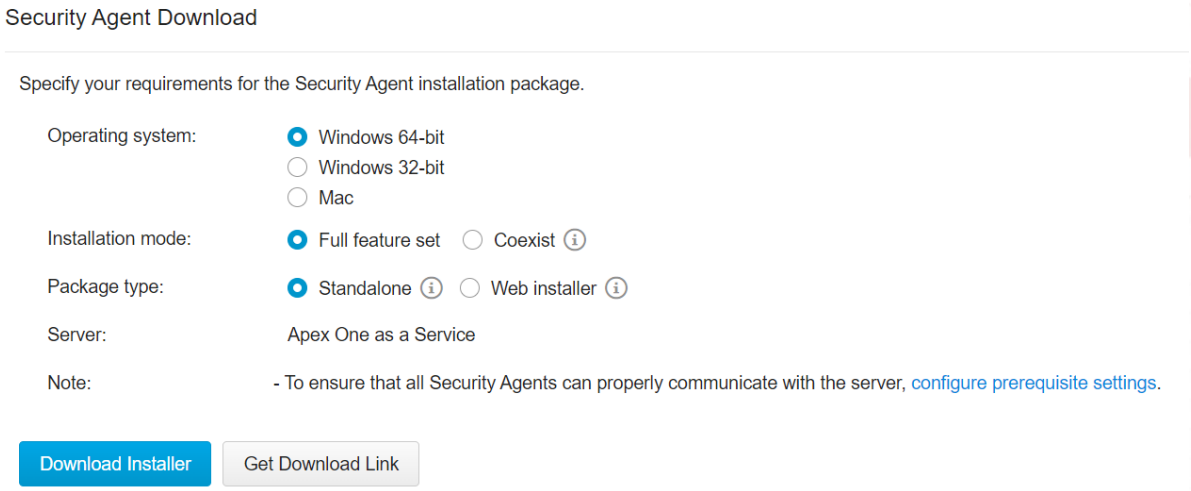
El presente documento busca ofrecer utilidades básicas a los administradores de las consolas de Apex One & Apex Central, recopilando las mejores prácticas, guías e instructivos, con el objetivo de asistir a lo usuarios en el uso de las consolas.

Instalación Agente Software as a Service

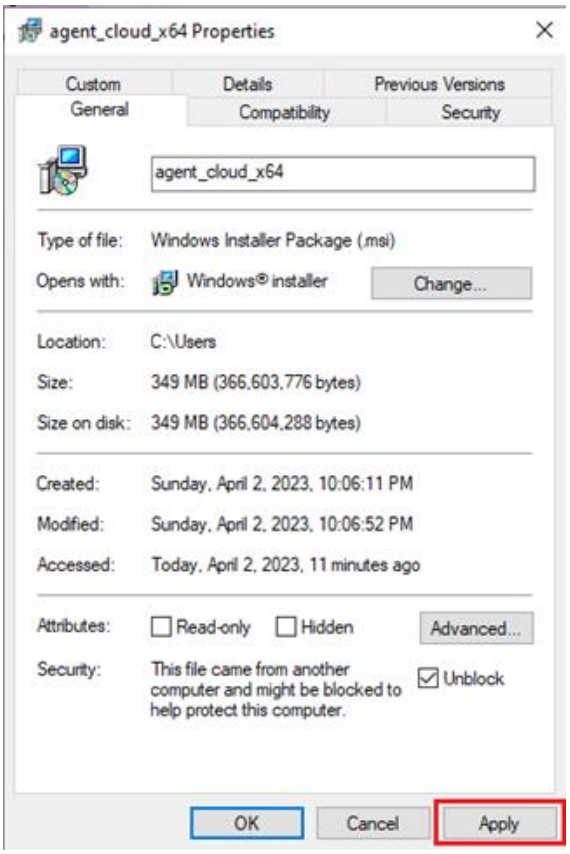
Para instalar el agente será necesario iniciar sesión en la consola de Apex Central. Allí, desde el módulo de Administration, cliquearemos en “Security Agent Download”.



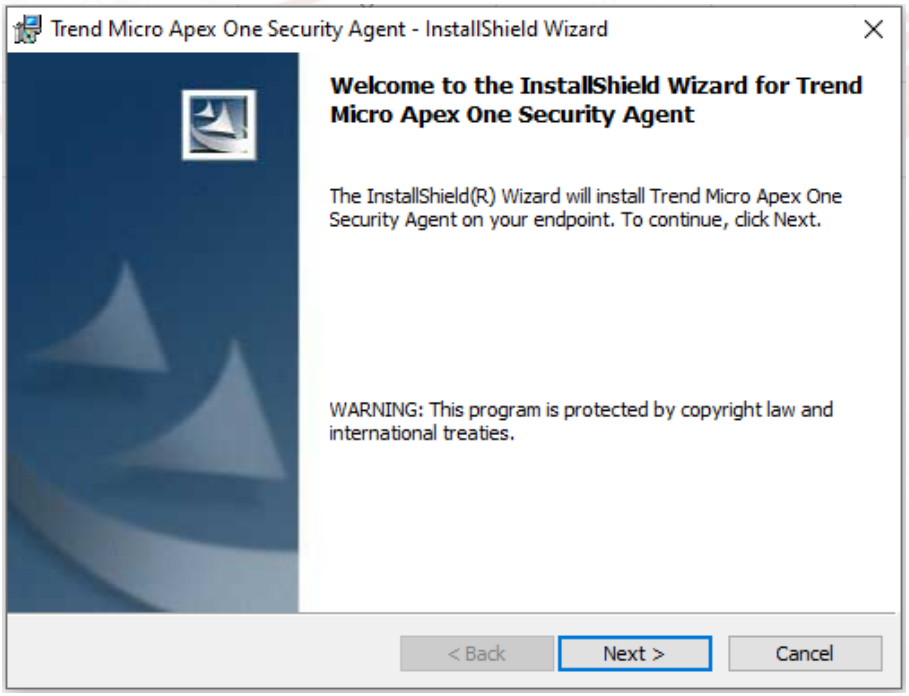
Posteriormente nos figurará la siguiente pantalla en la que podremos especificar los requerimientos de sistema operativo, si necesitamos un agente completo e individual o que coexista con otro antivirus y elegir el tipo de paquete.



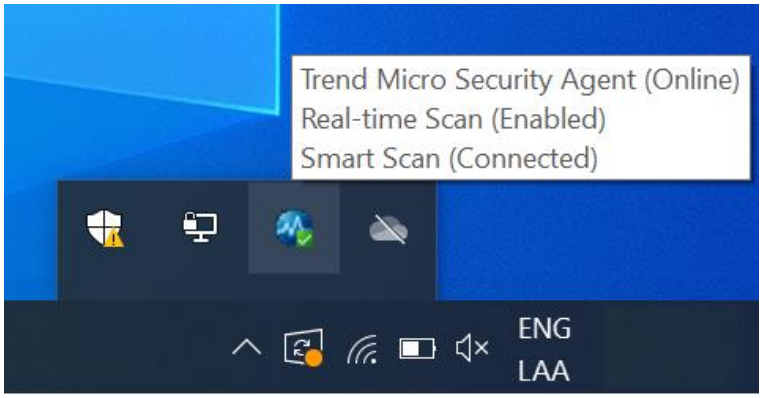
Una vez que tengamos el instalador descargado en el equipo a proteger, será necesario desbloquearlo desde Propiedades.



Luego, ejecutar el instalador como administrador. Aparecerá el InstallShield Wizard, y procederemos a presionar siguiente hasta que comience la instalación.



Una vez instalado, nos figurará en la barra de tareas el Notifier. De no ser así, abrir la aplicación desde la búsqueda de Windows.



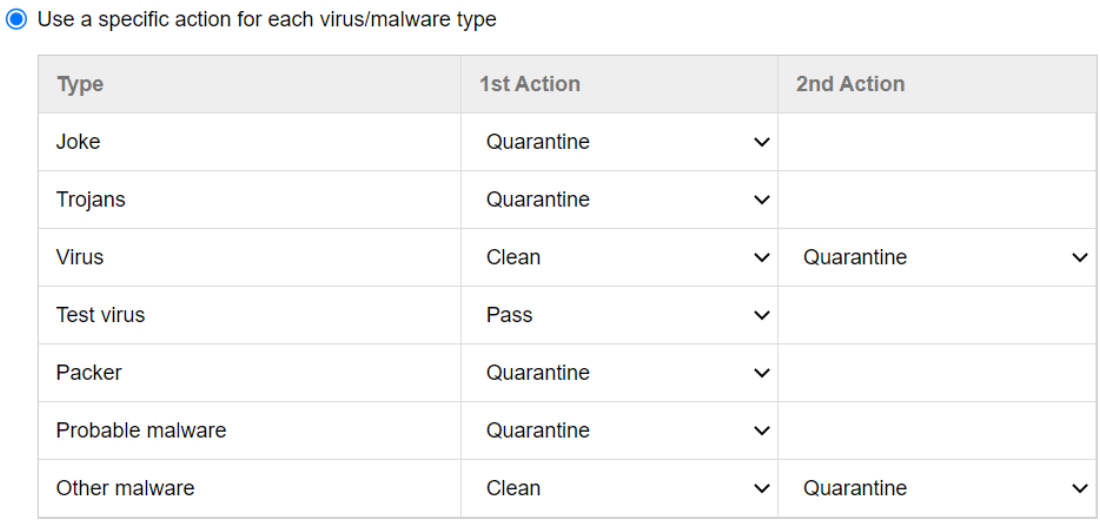
Políticas: Configuraciones Recomendadas

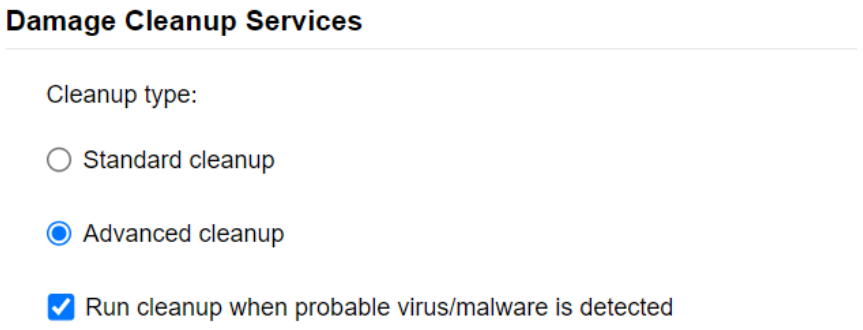
General

- ✓ Activar 2FA
- ✓ Mantener los roles de los usuarios controlados

Anti-Malware Scans

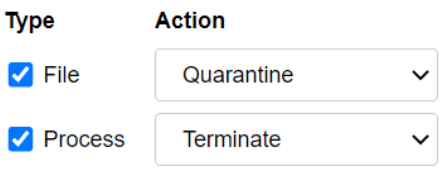
- ✓ Real-Time Scan y Scheduled Scan habilitados con Spyware y Grayware Scan, para todos los archivos escaneables.
- ✓ Configurar un escaneo semanal.
- ✓ Realizar excepciones de aquellos archivos/directorios/extensiones que no requieran análisis.
- ✓ Configurar las acciones de la siguiente manera.



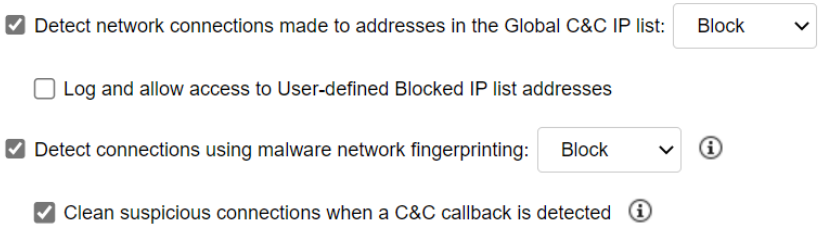


Advanced Threat Protection

- ✓ Habilitar Behaviour Monitoring, protegiendo los documentos de la encripción no autorizada y bloqueando procesos comúnmente asociados a Ransomware. Recomendamos activar a su vez “Program Inspection”.
- ✓ Habilitar Predictive Machine Learning, determinando las siguientes opciones:



- ✓ Habilitar Web Reputation, marcando la característica “Browser Exploit Prevention”, permitiendo páginas web internas y válidas para agilizar su funcionamiento.
- ✓ Habilitar Suspicious Connection, determinando las siguientes opciones:



- ✓ Habilitar Vulnerability Protection en el modo recomendado, realizando excepciones o cambiando los modos desde Policy Resources > Intrusion Prevention Rules.
- ✓ Habilitar Device Control y Application Control en base a las necesidades de la organización.

Exceptions

- ✓ En Trusted Program List excluir los programas requeridos de los escaneos de Application Control, Behavior Monitoring, Device Control, Endpoint Sensor y Real-time Scan.

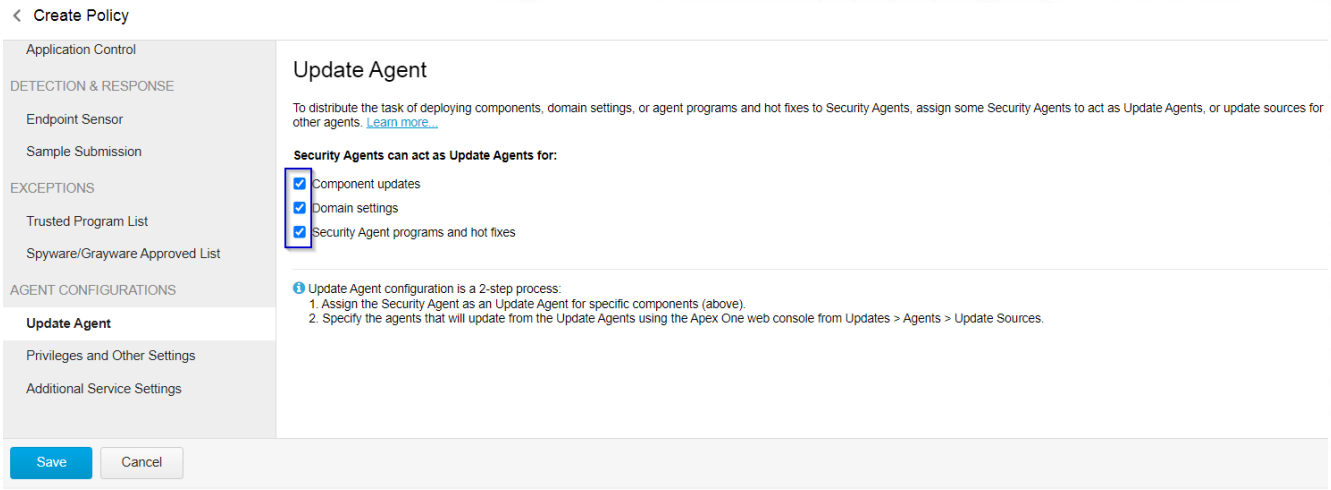
Agent Configurations

- ✓ Habilitar Unauthorized Change Prevention Service, Suspicious Connection Service, Data Protection Service y Advanced Protection Service. Generar contraseña de Upload/Uninstall.

Creación de Update Agent

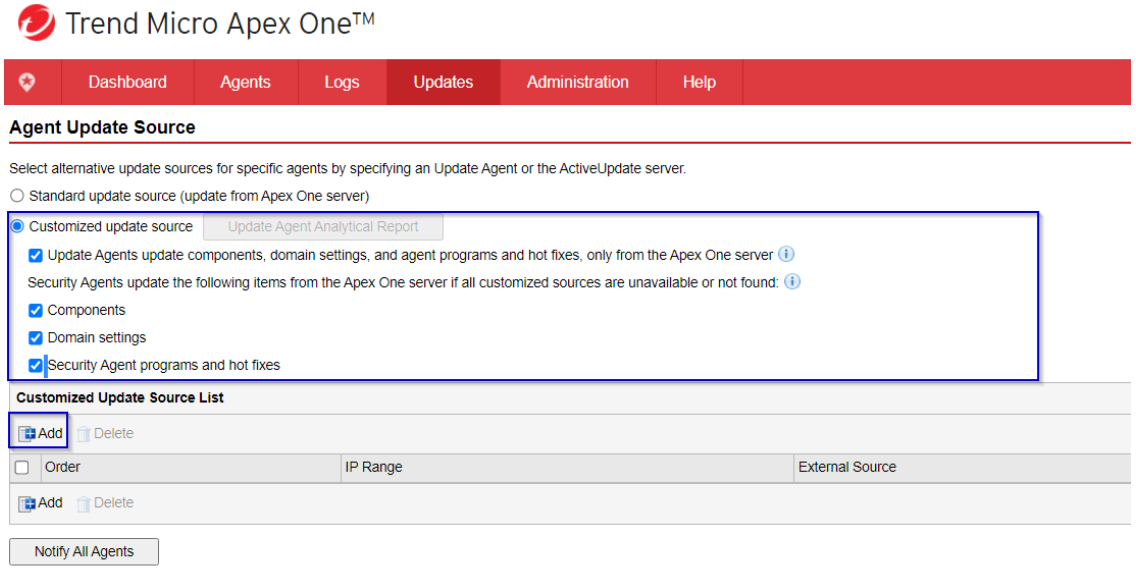
1. En primera instancia debemos modificar/crear una política en Apex Central que apunte a un agente el cual será el que actúe como Update agent.

   Policies > Policy Management > Modulo Update Agent.

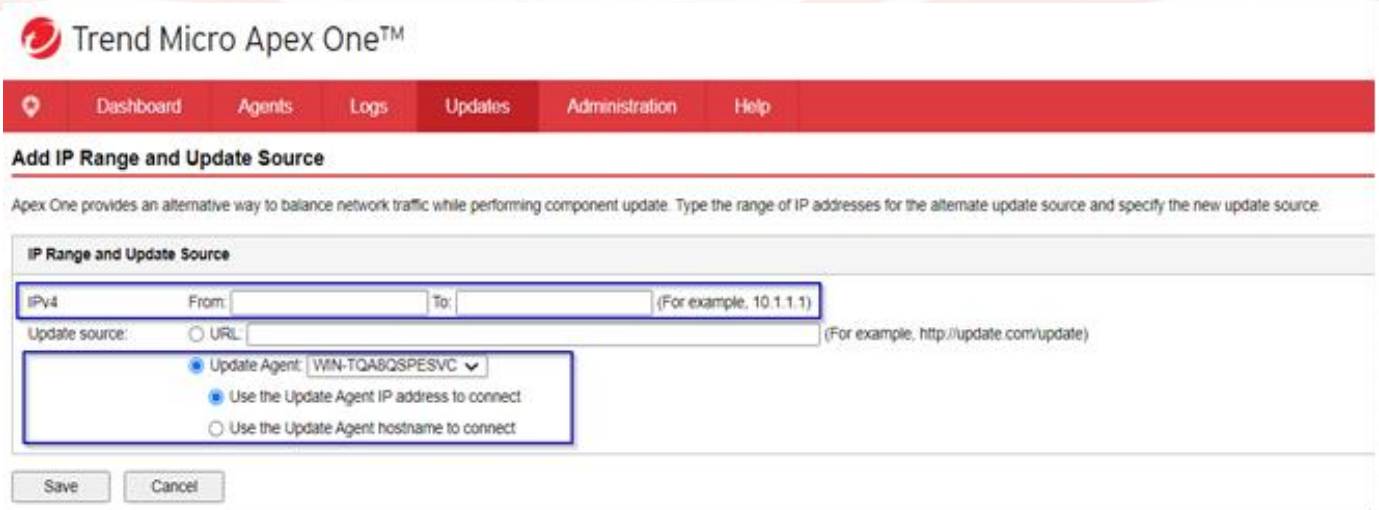


2. En segunda Instancia debemos ir a Apex One y entrar.
   Update > Agents > Update source.

Tildamos las opciones correspondientes.



3. Agregamos el rango de IPv4 al cual le va a aplicar dicha configuración y luego seleccionamos el Update agent y selecionamos como queremos que se conecte por IP o hostname.

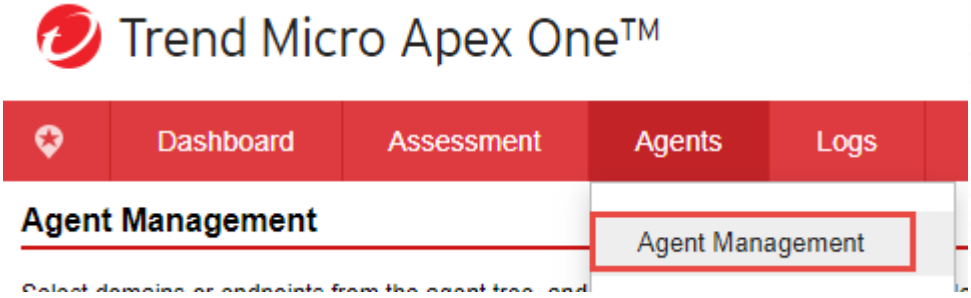


Exclusiones de Escaneo

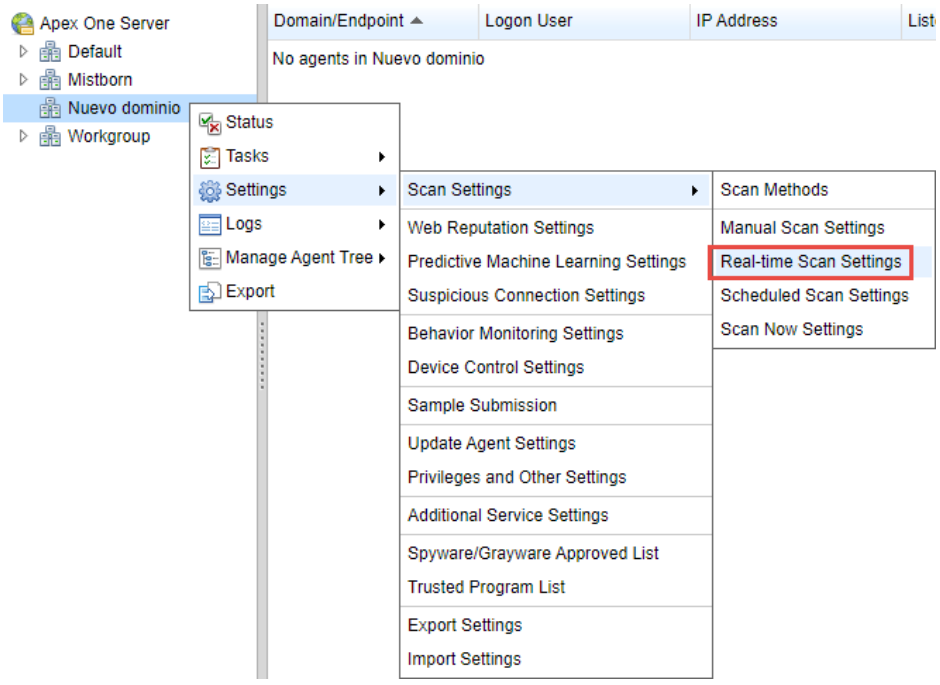
A continuación, se describirán los pasos a realizar para crear exclusiones de escaneo de Real-Time Scan. Tenga en cuenta que, de ser necesario se deberá extender las mismas a los otros tipos de escaneo.

Una vez logueado en la consola web de Apex One:

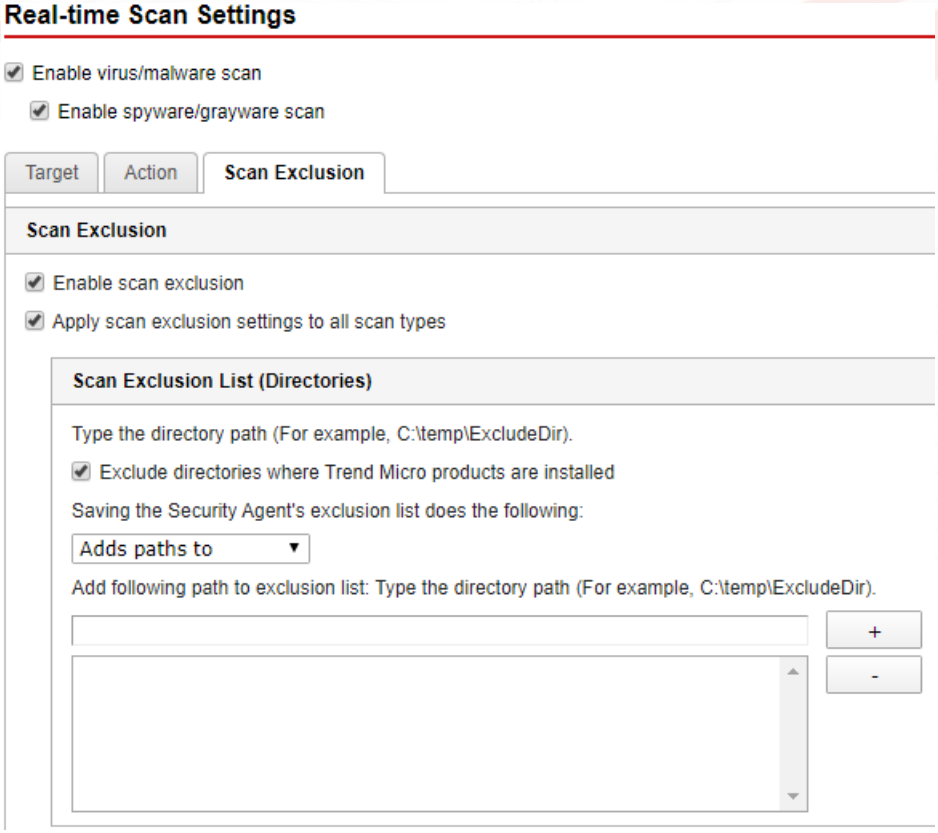
1. Dirigirse al menú **Agents > Agent Management**.



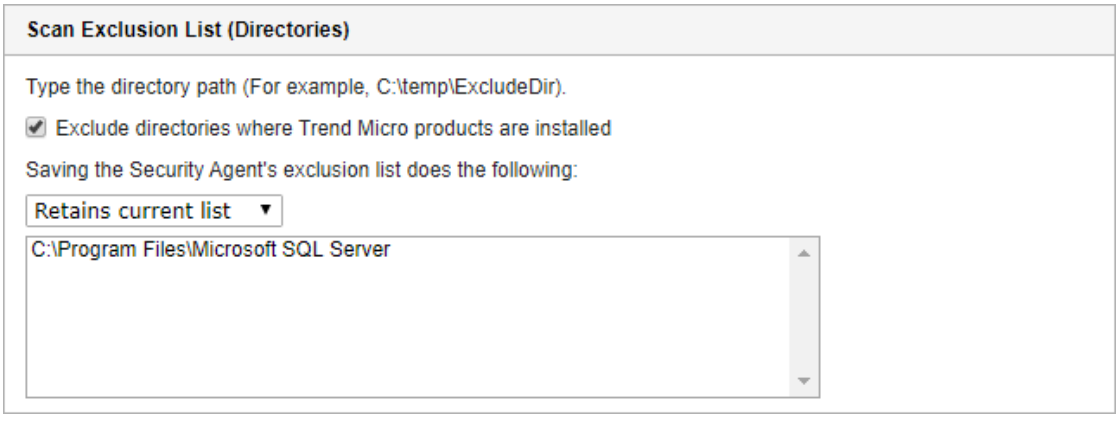
2. Ya allí, seleccionar el dominio al cual se le van a aplicar las exclusiones:



3. En la ventana emergente, se podrán configurar para Directorios, Archivos o Extensiones, según corresponda. Empezando por los directorios:

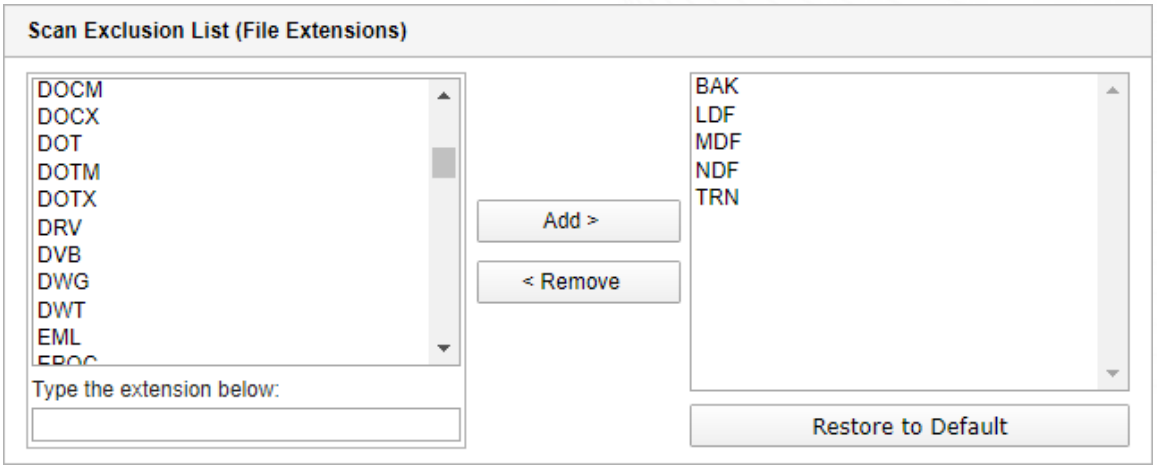


Donde, seleccionando la opción del box Adds paths to, habilitará a añadir una excepción por directorio. La siguiente imagen muestra una exclusión común en servidores con bases de datos SQL:



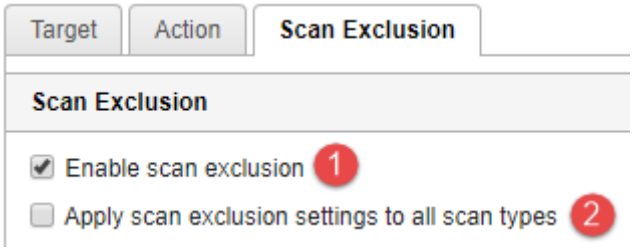
4. El proceso es el exactamente mismo para una exclusión para un archivo en específico en el siguiente recuadro.

5. Por último, el recuadro remanente permitirá seleccionar extensiones de archivos de una lista, o agregarlas para aquellas que se conozcan de acuerdo a las aplicaciones siendo ejecutadas en el equipo. La siguiente es una imagen con exclusiones de extensiones recomendadas para un servidor SQL:



6. Por último, solo restará guardar los cambios realizados presionando el botón Save al final de la página, y de esta forma las exclusiones quedarán aplicadas.

Es importante destacar que las tildes al inicio de la página serán para:



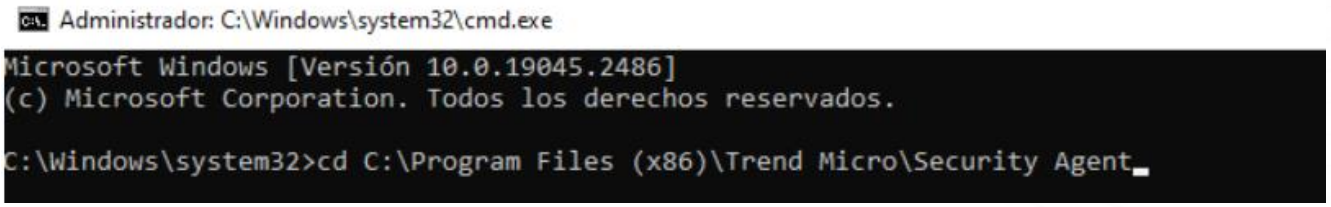
7. Habilitar o no las exclusiones listadas a continuación
8. Aplicar las exclusiones listadas a continuación al resto de tipos de escaneo. No se recomienda si se busca maximizar la seguridad, ya que se estila realizar estas exclusiones en el escaneo en tiempo real, y dejar programado un escaneo en horarios pocos críticos en los cuales se analice todas estas carpetas y archivos excluidos.

Guía de comandos

Los comandos que se describen a continuación serán de utilidad para conseguir información del agente desde el dispositivo; tanto de los archivos escaneados como de sus componentes.

Primero tenemos que ubicarnos en la carpeta de "Security Agent" mediante CMD (Modo Administrador). La ubicación default es la siguiente:

"C:\Program Files (x86)\Trend Micro\Security Agent"



Una vez ubicados en la carpeta escribir "pccntmon –“ y la letra que corresponda. A continuación, se exponen las opciones disponibles:

- **pccntmon -h:** Muestra todos los comandos disponibles.
- **pccntmon -r**: Muestra el ultimo archivo escaneado por el Real-time Monitor y la cantidad de archivos escaneados.
- **pccntmon -v**: lista los componentes del agente y sus versiones.
- **pccntmon -u:** Ejecuta un update de los componentes del agente.
- **pccntmon -c**: Muestra información del **Scan method** que se usa; del **Pattern status** si está en la última versión del update o si está fuera de la última versión; del **Real-time Scan Service** si está funcional, si está deshabilitado o si esta no funcional, si la conexión del agente si esta online, independent u offline; **Web Reputation Services**, si están disponibles o reconectando; **File Reputation Services**, si está disponible o reconectando.
- **pccntmon -m “contraseña_para_desinstalar”:** Desinstala el agente.
- **pccntmon -n "Contraseña_para_desactivar_agente”**: Desactiva el agente.
- **pccnt "path de la carpeta"**: Escanea la carpeta en busca de riesgos de seguridad [no es posible escanear archivos, solo carpetas].

Troubleshooting Apex One SaaS: Agente Offline

Reiniciar servicio “Apex One NT Listener”

1. Ir a “Services”.
2. Click derecho en el servicio.
3. Reiniciar.

Cambiar de dominio al cliente/agente

1. Abrir la consola web de Apex One e ir Agents > Agent Management.
2. Hacer click en Add Domain.
3. Elegirle un nombre al nuevo dominio click OK.
4. Mover al cliente/agente offline al nuevo dominio.
5. En el equipo de cliente/agente, reiniciar el servicio Apex One NT Listener.
6. Desde el equipo del agente, hacer click derecho en el mismo y luego en Update Now.
7. Refrescar la consola para verificar si el cliente/agente ahora aparece correctamente.

Restablecer conexión con IPXfer

1. Descargar ipxfer_x64.exe y OfcNTCer.dat modificando la URL con el nombre del servidor de Apex One SaaS y guardar ambos en una misma ruta.

Para descargar el certificado e IpXfer del servidor Apex One SaaS se deben utilizar las siguientes URL.

- https://<ServidorApexOneSaaS>.manage.trendmicro.com:443/officescan/hotfix_pccnt/Common/OfcNTCer.dat
- https://<ServidorApexOneSaaS>.manage.trendmicro.com:443/officescan/hotfix_admin/utility/ipxfer/ipxfer_x64.exe

2. Abrir CMD desde el equipo con el agente de Apex One a restablecer su conexión y ejecutar desde la ruta donde se encuentran los certificados:

ipxfer_x64.exe -s ServidorApexOneSaaS.manage.trendmicro.com -p 80 -sp 443 -e ofcntcer.dat -pwd ContraseñadeUnload

Parámetros:
-s: Servidor Apex One al cual se va a migrar el agente
-p: Puerto no seguro [80]
-sp: Puerto seguro [443]
-e: Llave pública que utiliza el agente para comunicarse con la consola
-pwd: Contraseña de unload

Troubleshooting Apex One SaaS: Case Diagnostic Tool

Descargar CDT desde el siguiente link:

- https://downloadcenter.trendmicro.com/index.php?regs=nabu&prodid=25

1. Extraiga todo el contenido del archivo zip en un directorio local de su computadora.
2. Ejecutar el CDT.
3. Iniciar la aplicación.
    a. Aceptar el acuerdo.
    b. Haga clic en Inicio. Aparece una ventana que muestra los productos de Trend Micro detectados.
    c. Seleccione los productos instalados.

Si se detecta más de un producto, desplácese hacia abajo para mostrar todos los demás eventos y componentes, y selecciónelos.

5. Depurar Windows. Si es posible reproducir el problema. Si no puede reproducir el problema o no es necesario realizar una depuración, puede hacer clic en Omitir y pasar al Paso 6:
    a. Haga clic en start debug mode.

b. Espere a que el modo de depuración cambie a "ON".

c. En este punto ya está listo para reproducir el problema. Recoge una captura de pantalla de cualquier mensaje que puedas ver en la pantalla.

d. Una vez que se haya reproducido el problema, haga clic en stop debug mode.

6. Recoger los logs.

a. Nombre una carpeta donde serán guardados.

b. Seleccionar "Today's logs".

7. Cliquear Next >.

Cuando se complete la aplicación, se crearán una nueva carpeta y un archivo zip en el directorio que nombró en el Paso 8a.

8. Haga clic en Abrir carpeta para abrir la carpeta donde se guardó el informe CDT.
9. Haga clic en Finalizar para cerrar el CDT.