Cisco Secure Endpoint: Explicación de los switches de línea de comandos

Contenido

Introducción

Este documento describe los switches de línea de comandos (CLI) disponibles para su uso con Cisco Secure Endpoint.

Antecedentes

Cisco Secure Endpoint contiene muchas funciones y acciones personalizables que se pueden realizar localmente en un terminal mediante switches de línea de comandos. Este documento los muestra.

Switches de línea de comandos para terminales seguros de Cisco

Switches Secure Endpoint Installer

amp_installer.exe

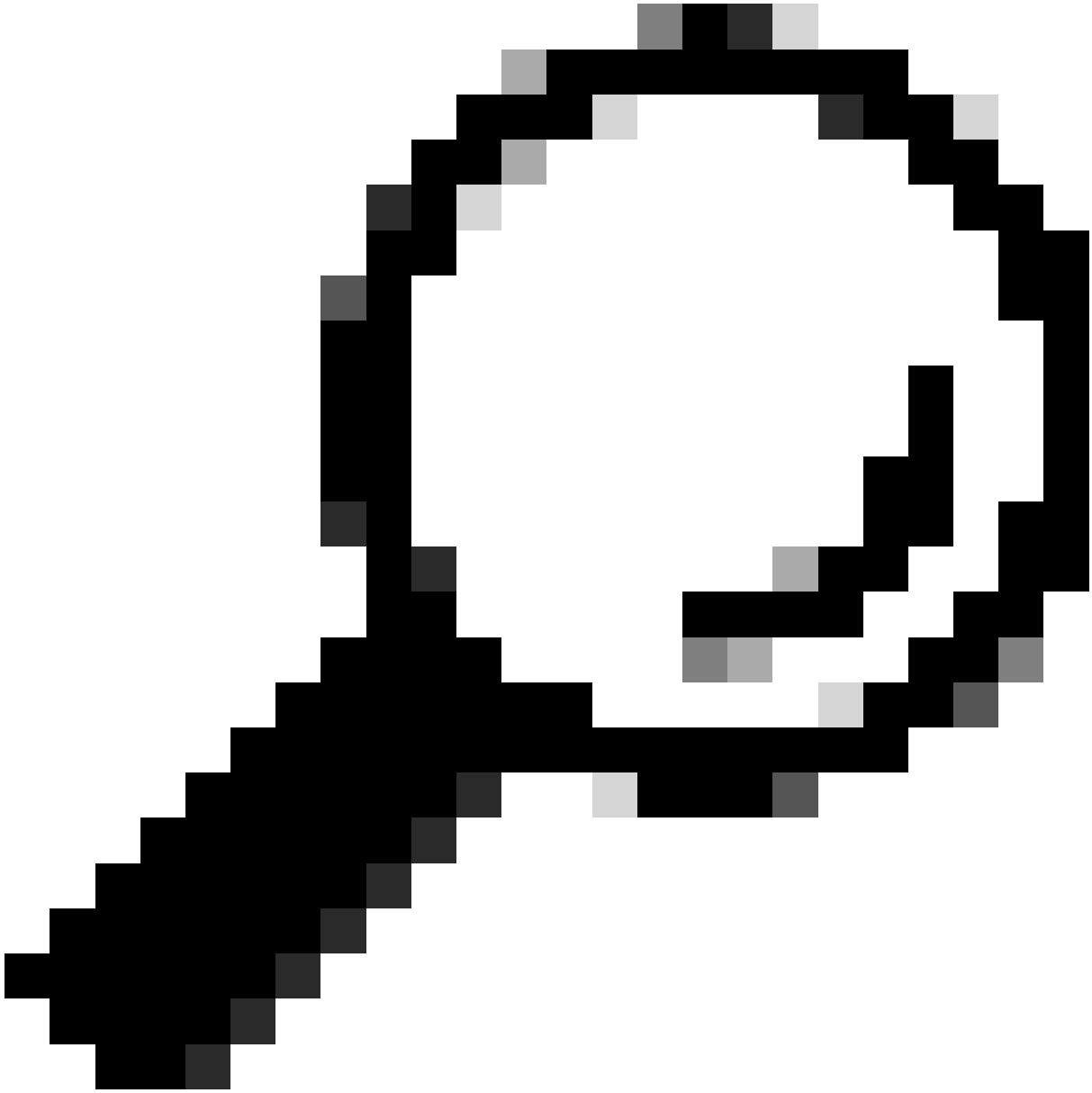
1. Abra el símbolo del sistema en Windows.
2. Vaya a la carpeta en la que se encuentra el instalador en el símbolo del sistema (carpeta Descargas que se utiliza como ejemplo a continuación).

```
cd C:\Users\sysadmin\Downloads
```

- Ejecute los switches disponibles proporcionados.

amp_protect.exe <switch>

Nota: No se devolverá ninguna salida después de ejecutar los comandos.



Sugerencia: se puede utilizar más de un switch a la vez.

Switch de línea de comandos	Descripción del comando	Notas especiales
/S	Se utiliza para poner el instalador en modo silencioso.	
/temppath	Se utiliza para especificar una ubicación temporal personalizada para los archivos de instalación que se van a extraer y ejecutar.	/temppath C:\
/desktopicon 0	Se utiliza para especificar que no se crea un icono de escritorio.	Ésta es la configuración predeterminada y no es necesario proporcionarla.
/desktopicon 1	Se utiliza para especificar que se crea un icono de escritorio.	
/startmenu 0	No se crean los accesos directos del menú Inicio.	
/startmenu 1	Se crean accesos directos al menú Inicio.	Ésta es la configuración predeterminada y no es necesario proporcionarla.
/contextmenu 0	Deshabilita la	

	opción Analizar ahora en el menú contextual del botón derecho.	
/contextmenu 1	Habilita Scan Now en el menú contextual del botón derecho.	Ésta es la configuración predeterminada y no es necesario proporcionarla.
/remove 0	Desinstala el conector y deja los archivos para su posterior reinstalación.	Los archivos XML con el UUID permanecen y permiten reutilizar el objeto de equipo existente al reinstalar el conector. Los archivos de registro también se conservan. Si se está utilizando una contraseña de protección del conector, se debe especificar mediante el indicador /uninstallpassword.
/remove 1	Desinstala el conector y quita todos los archivos asociados.	Si se está utilizando una contraseña de protección del conector, se debe especificar mediante el indicador /uninstallpassword.
/uninstallpassword	Especifica la contraseña de desinstalación cuando se utiliza el indicador /remove. Se debe especificar si la función de protección de conectores está habilitada	Especifique la contraseña de desinstalación después del indicador.
/skipdfc 1	Omitir la instalación del controlador DFC.	Todos los conectores instalados con este indicador deben pertenecer a un grupo con una directiva que tenga el motor de red deshabilitado.

/skiptetra 1	Omita la instalación del controlador TETRA.	Todos los conectores instalados con este indicador deben estar en un grupo con una política que tenga el indicador Tetra desactivado.
/D=[RUTA]	Se utiliza para especificar el directorio que se va a instalar. Por ejemplo, /D=C:\	Se debe especificar como el último parámetro. Para el modificador de línea de comandos /D=, el directorio de instalación predeterminado varía según el sistema operativo. Estos son los directorios de instalación predeterminados en Microsoft Windows XP con Service Pack 3 o posterior: Para plataformas x86: C:\Program Files (x86)\Cisco\AMP Para plataformas x64: C:\Program Files\Cisco\AMP
/goldenimage 1	Instala el conector para prepararse para las imágenes doradas	Este indicador está diseñado para ayudar a preparar imágenes doradas en entornos virtuales. El uso de este indicador evita que el conector se inicie y registre durante la creación de la imagen dorada. Para obtener más información, visite: Cómo preparar una imagen dorada con terminales seguros https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html
/skiposcheck 1	Omite la comprobación del sistema operativo durante la instalación.	Este indicador se puede utilizar para instalar Secure Endpoint en sistemas operativos con los que no es compatible.

Switches Secure Endpoint Support Diagnostic Tool

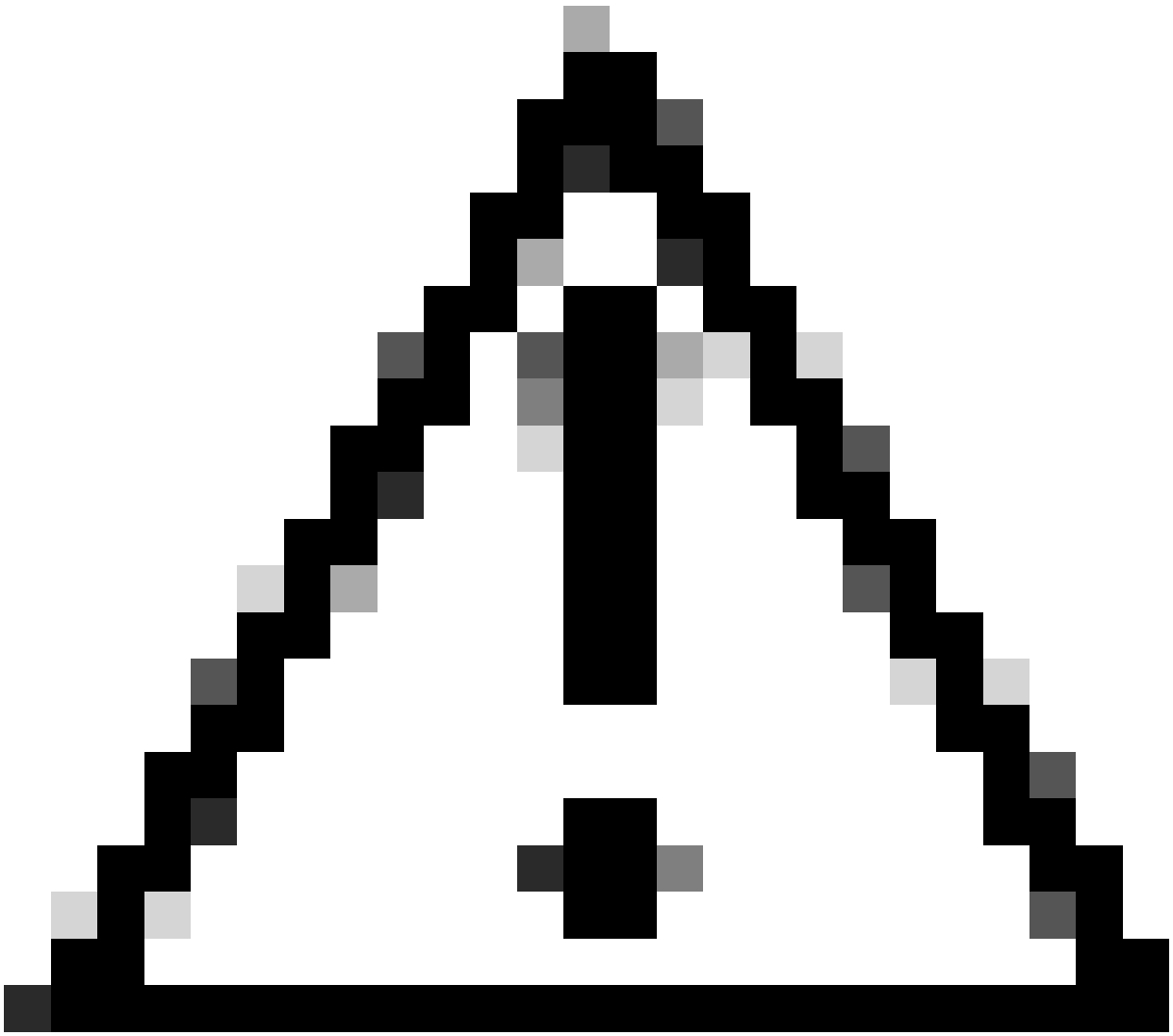
ipsupporttool.exe

- Abra el símbolo del sistema en Windows.

- Vaya a la carpeta en el símbolo del sistema. Ruta predeterminada: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica el número de versión).
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- Ejecute los switches disponibles proporcionados.
ipsupporttool.exe <switch>

Nota: Al ejecutar los switches, no se devolverá ningún resultado.

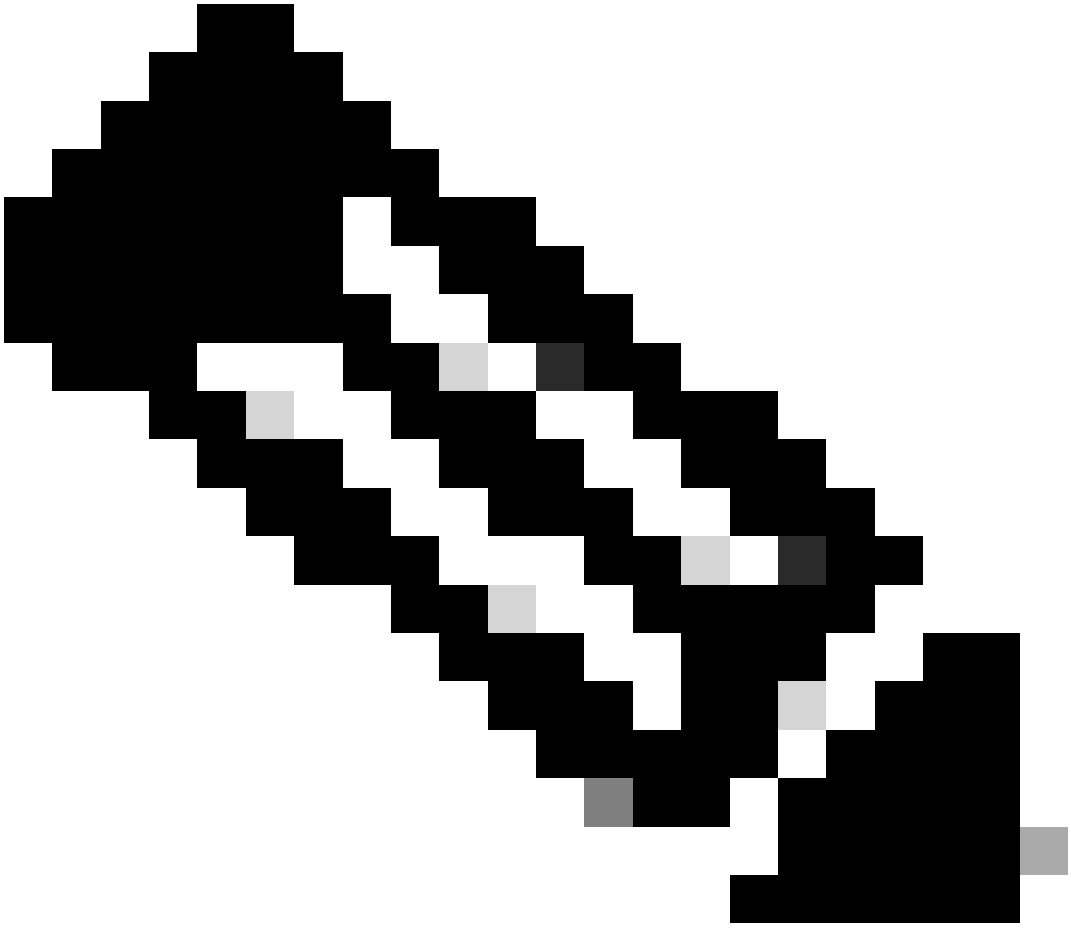


Precaución: cualquier modificador que haga referencia a una opción de carpeta requiere que las carpetas ya estén presentes

Switch de línea de comandos	Descripción del comando	Notas especiales
-o <ruta>	Especifica la carpeta de resultados de la herramienta de soporte técnico.	El valor predeterminado es el escritorio si no se especifica esta opción.
-d <ruta_instalación>	Especifica la carpeta de la que la Herramienta de soporte técnico de Windows puede recuperar archivos.	Si no se especifica, el valor predeterminado es el directorio de instalación predeterminado de Secure Endpoint.
-t <minutes>	Ejecuta un diagnóstico de nivel de depuración programado desde la Herramienta de soporte técnico de Windows durante el tiempo especificado. La duración del tiempo se especifica en minutos.	

Switches UI de terminal seguro

iptraytool.exe



Nota: iptraytool.exe sólo está disponible en versiones antiguas de Secure Endpoint.

- Abra el símbolo del sistema en Windows.

- Vaya a la carpeta en el símbolo del sistema. Ruta predeterminada: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica el número de versión).

```
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
```

- Ejecute los switches disponibles proporcionados.

```
iptray.exe <switch>
```

Switch de línea de comandos	Descripción del comando	Notas especiales
-f	Permite activar la interfaz de usuario cliente desde la línea de comandos.	Esto sólo es necesario si un terminal tiene la GUI desactivada a través de la política con la opción Iniciar interfaz de usuario cliente desactivada.

Switches SFC de terminales seguros

sfc.exe

- Abra el símbolo del sistema en Windows.

- Vaya a la carpeta en el símbolo del sistema. Ruta predeterminada: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica el número de versión).
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- Ejecutar los switches disponibles proporcionados
sfc.exe <switch>

Switch de línea de comandos	Descripción del comando	Notas especiales
-s	Inicie el servicio Immunet Protect (Conector de Windows). El servicio ya debe estar registrado con SCM para poder iniciarse.	
-k	Detenga el servicio Immunet Protect (Conector de Windows).	Si la protección de conectores está habilitada, ingrese la contraseña después de -k para detener el servicio con éxito.
-u	Desinstale el servicio Immunet Protect (Conector de Windows). Cancele el registro del servicio con el Administrador de control de servicios de Windows (SCM). El desinstalador utiliza esta opción para desinstalar el servicio de conector de Windows.	

-r	Restablece el servicio Immunet Protect (Conector de Windows). Es muy similar a la opción -i, pero no instala el servicio. Esto es útil para corregir la corrupción local.xml.	
-l inicio	Alternar el debug y el registro del kernel dinámicamente (el disparador es una L minúscula).	Este estado permanece hasta que se desactiva, se reinicia el servicio o se configura una nueva directiva para cambiar el nivel de registro.
-l stop	Desactive el registro de depuración y kernel dinámicamente (el disparador es una L minúscula).	
-unblock SHA_of_file	Esta opción desbloquea la ejecución de un proceso. Después de ejecutar este modificador de comandos, la aplicación puede eliminarse de la memoria caché del núcleo local de la lista de bloqueo de aplicaciones.	Este comando se puede utilizar cuando una aplicación se bloquea debido a un falso positivo o error, y desea desbloquear rápidamente la aplicación sin esperar 30 minutos o reiniciar el equipo.
-volver a registrarse	Esta opción puede borrar el uuid y los certificados de local.xml y del Registro mientras el servicio se está ejecutando, y desencadena una reinscripción. Local.xml y el Registro se actualizan con nuevos valores. Sin embargo, se bloquea si la sincronización de ID está activada y el conector vuelve a obtener el UUID existente. Esto puede colocar el conector en el grupo/política predeterminado después del registro si se ha modificado el paquete de instalación utilizado para la instalación inicial.	Si la Protección del conector está habilitada, debe ingresar lo siguiente: sfc.exe -reregister _password_

-forceupdate	Esta opción obliga al conector a actualizar las definiciones de TETRA.	
-forceapdeupdate	Esta opción obliga al conector a actualizar las definiciones de protección del comportamiento.	Puede comprobar las definiciones de protección del comportamiento actuales instaladas en el terminal en la trayectoria del dispositivo en el panel de terminales seguros.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- Terminal seguro de Cisco - Notas técnicas
- Cisco Secure Endpoint - Guía del usuario
- Uso de la CLI de Mac/Linux para terminales seguros

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).