Cisco Secure Endpoint: spiegazione degli switch della riga di comando

Sommario

Introduzione

In questo documento vengono descritte le opzioni della riga di comando (CLI) disponibili per l'utilizzo con Cisco Secure Endpoint.

Premesse

Cisco Secure Endpoint contiene molte funzionalità e azioni personalizzabili che possono essere eseguite localmente su un endpoint tramite opzioni della riga di comando. Nel documento vengono mostrati.

Switch della riga di comando per Cisco Secure Endpoint

Switch Secure Endpoint Installer

amp_installer.exe

1. Aprire il prompt dei comandi in Windows.

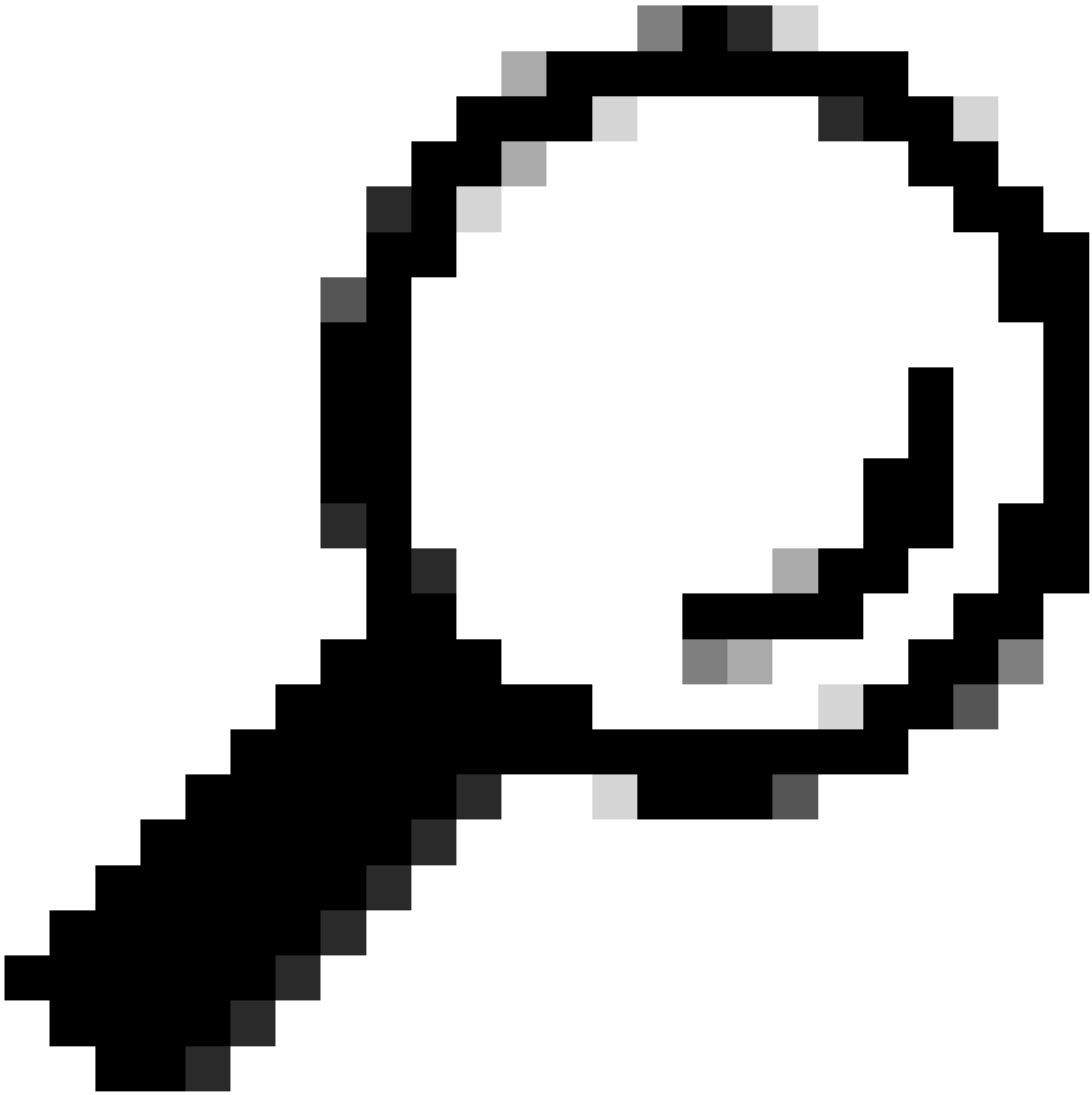
2. Passare alla cartella in cui si trova il programma di installazione al prompt dei comandi (cartella Download utilizzata come esempio di seguito).

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

- Eseguire gli switch disponibili in dotazione.

amp_protect.exe <switch>

Nota: dopo l'esecuzione dei comandi non verrà restituito alcun output.



Suggerimento: è possibile utilizzare più switch contemporaneamente.

Opzione della riga	Descrizione	Note speciali

di comando	comando	
/S	Utilizzato per impostare la modalità invisibile all'utente.	
/temppath	Consente di specificare un percorso temporaneo personalizzato per i file di installazione da estrarre ed eseguire.	/temppath C:\
/desktopicon 0	Utilizzato per specificare che non viene creata un'icona del desktop.	Questa è la configurazione predefinita e non deve essere fornita.
/desktopicon 1	Utilizzato per specificare la creazione di un'icona del desktop.	
/startmenu 0	I collegamenti del menu Start non vengono creati.	
/menu Start 1	Vengono creati i collegamenti del menu Start.	Questa è la configurazione predefinita e non deve essere fornita.
/contextmenu 0	Disabilita Scan Now dal menu di scelta rapida visualizzato	

	facendo clic con il pulsante destro del mouse.	
/contextmenu 1	Abilita Scan Now nel menu di scelta rapida visualizzato facendo clic con il pulsante destro del mouse.	Questa è la configurazione predefinita e non deve essere fornita.
/remove 0	Disinstalla il connettore e lascia i file per una successiva reinstallazione.	I file XML con l'UUID rimangono e consentono di riutilizzare l'oggetto computer esistente durante la reinstallazione del connettore. Vengono conservati anche i file di registro. Se è in uso una password di protezione del connettore, è necessario specificarla utilizzando il flag /uninstallpassword.
/remove 1	Disinstalla il connettore e rimuove tutti i file associati.	Se è in uso una password di protezione del connettore, è necessario specificarla utilizzando il flag /uninstallpassword.
/uninstallpassword	Specifica la password di disinstallazione quando si utilizza il flag /remove. È necessario specificare se la funzionalità Protezione connettore è abilitata	Specificare la password di disinstallazione dopo il contrassegno.
/skipdfc 1	Ignora l'installazione del driver DFC.	Tutti i connettori installati con questo flag devono appartenere a un gruppo con un criterio in cui il motore di rete è disabilitato.
/skiptetra 1	Ignorare l'installazione del driver TETRA.	Tutti i connettori installati con questo flag devono essere in un gruppo con un criterio che ha il flag Tetra deselezionato.

/D=[PERCORSO]	Consente di specificare la directory in cui eseguire l'installazione. Ad esempio, /D=C:\	Deve essere specificato come ultimo parametro. Per lo switch da riga di comando /D=, la directory di installazione predefinita varia a seconda del sistema operativo. Di seguito sono elencate le directory di installazione predefinite in Microsoft Windows XP con Service Pack 3 o versione successiva: Per le piattaforme x86: C:\Program Files (x86)\Cisco\AMP Per le piattaforme x64: C:\Program Files\Cisco\AMP
/goldenimage 1	Installa il connettore per preparare le immagini dorate.	Questo flag è progettato per aiutare a preparare immagini dorate in ambienti virtuali. L'uso di questo flag impedisce l'avvio e la registrazione del connettore durante la creazione dell'immagine dorata. Per ulteriori informazioni, vedere: Come preparare un'immagine dorata con endpoint sicuri 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	Ignora il controllo del sistema operativo durante l'installazione.	Questo flag può essere utilizzato per installare Secure Endpoint nei sistemi operativi in cui non è compatibile.

Switch degli strumenti di diagnostica Secure Endpoint Support

ipsupporttool.exe

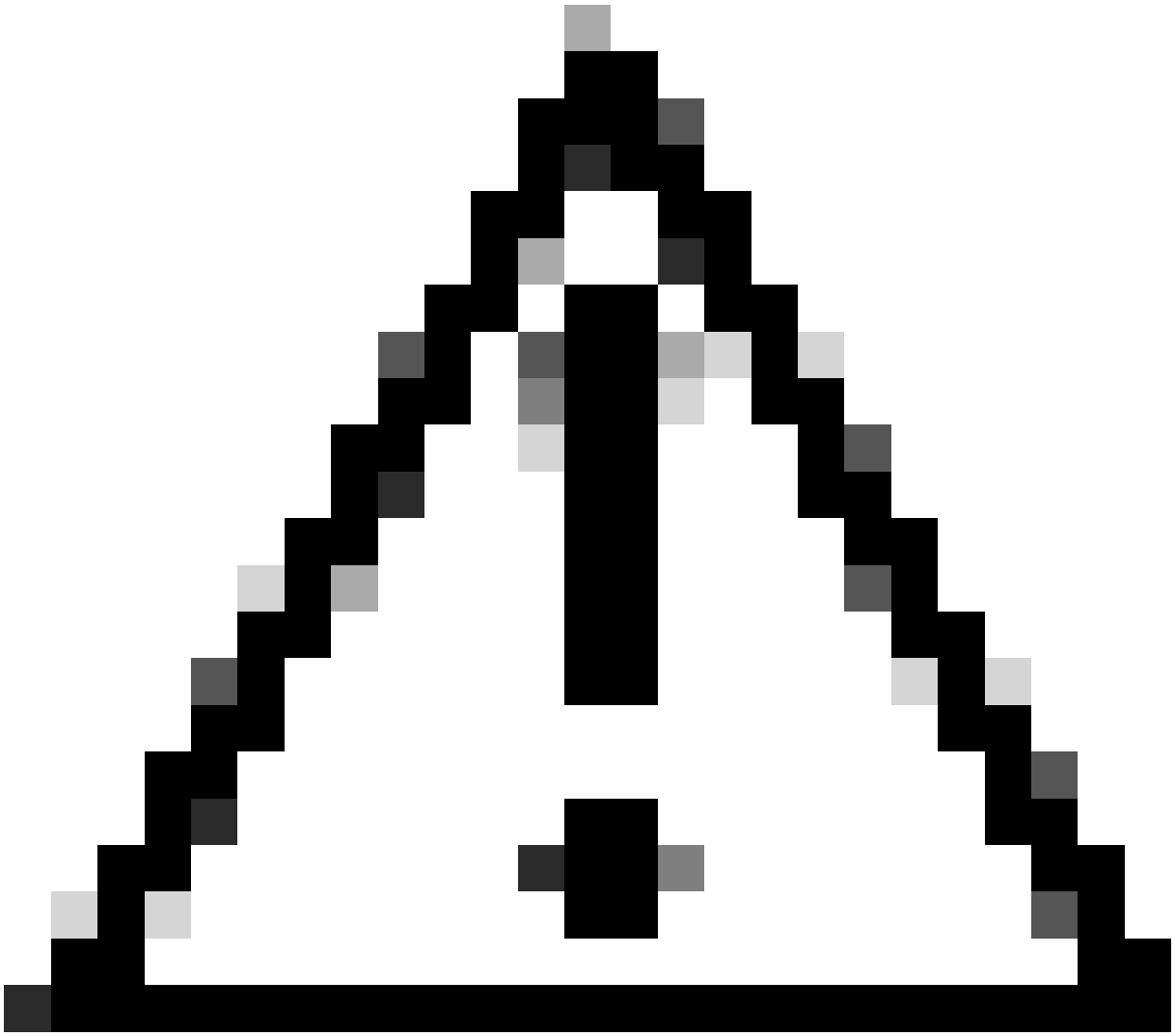
- Aprire il prompt dei comandi in Windows.

- Passare alla cartella al prompt dei comandi. Percorso predefinito: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica il numero di versione.
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- Eseguire gli switch disponibili in dotazione.

ipsupporttool.exe <switch>

Nota: quando si eseguono gli switch, non viene restituito alcun output.



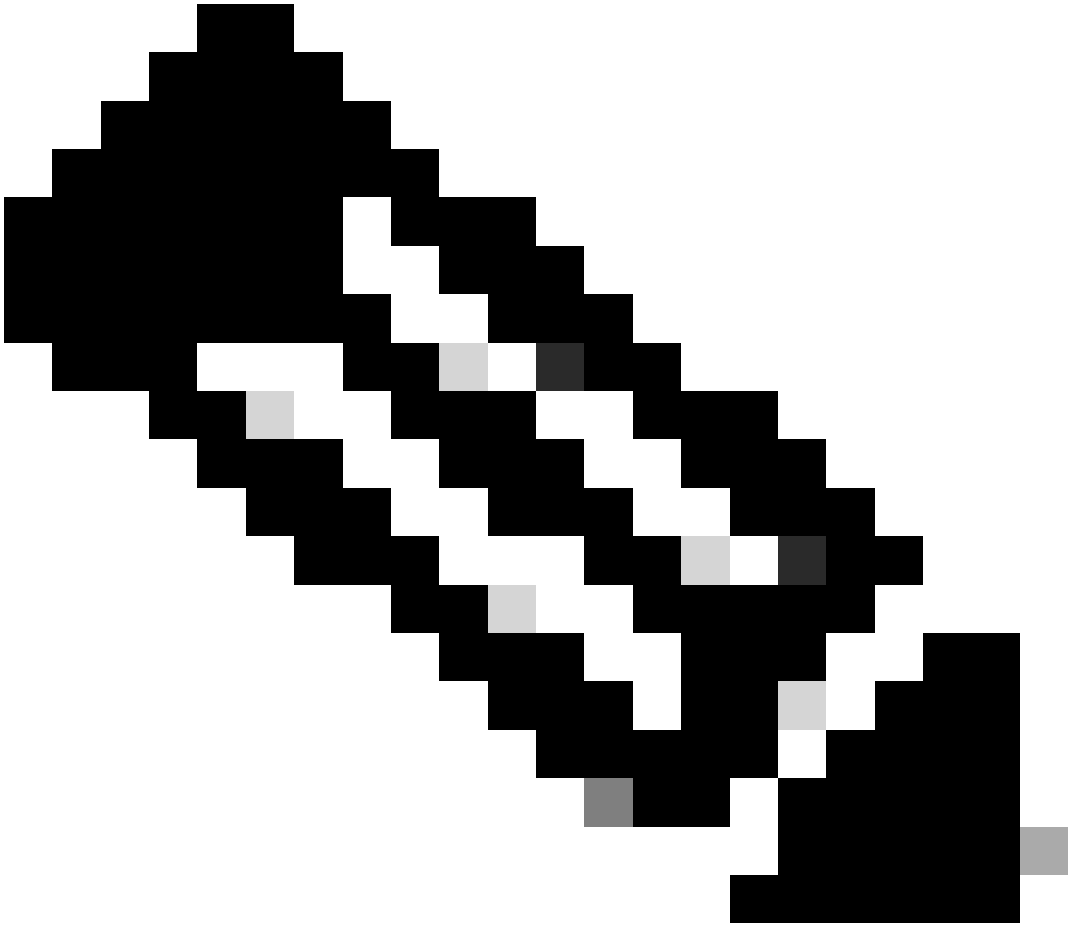
Attenzione: tutte le opzioni che fanno riferimento a una scelta di cartella richiedono che le cartelle siano già presenti.

Opzione della riga di	Descrizione comando	Note speciali

comando		
-o <percorso>	Specifica la cartella di output per lo Strumento di supporto.	Se questa opzione non è specificata, per impostazione predefinita viene visualizzato il desktop.
-d <percorso_installazione>	Specifica la cartella da cui lo Strumento di supporto di Windows può recuperare i file.	Se non specificato, viene utilizzata la directory di installazione predefinita di Secure Endpoint.
-t <minuti>	Esegue una diagnostica a tempo del livello di debug da Strumento di supporto Windows per il tempo specificato. La durata è specificata in minuti.	

Switch UI per endpoint sicuri

iptraytool.exe



Nota: il file iptraytool.exe è disponibile solo nelle versioni precedenti di Secure Endpoint.

- Aprire il prompt dei comandi in Windows.

- Passare alla cartella al prompt dei comandi. Percorso predefinito: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica il numero di versione.

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

- Eseguire gli switch disponibili in dotazione.

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

Opzione della riga di comando	Descrizione comando	Note speciali
-f	Consente di attivare l'interfaccia utente client dalla riga di comando.	Questa operazione è necessaria solo se l'interfaccia utente di un endpoint è disattivata tramite Criteri e l'opzione Avvia interfaccia utente client è deselezionata.

Switch SFC per endpoint sicuri

sfc.exe

- Aprire il prompt dei comandi in Windows.

- Passare alla cartella al prompt dei comandi. Percorso predefinito: **C:\Program Files\Cisco\AMP\X.X.X**, X.X.X indica il numero di versione.
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- Eseguire gli switch disponibili in dotazione
sfc.exe <switch>

Opzione della riga di comando	Descrizione comando	Note speciali
-s	Avviare il servizio Immunet Protect (Windows Connector). Per avviare il servizio, è necessario che sia già stato registrato con SCM.	
-k	Arrestare il servizio Immunet Protect (Windows Connector).	Se la protezione del connettore è abilitata, immettere la password dopo -k per arrestare correttamente il servizio.
-u	Disinstalla il servizio Immunet Protect (Windows Connector). Annullare la registrazione del servizio con Gestione controllo servizi Windows (SCM). Questa opzione viene utilizzata dal programma di disinstallazione	

	per disinstallare il servizio Connettore di Windows.	
-r	Reimposta il servizio Immunet Protect (Windows Connector). Questa opzione è molto simile all'opzione -i ma non installa il servizio. Questa opzione è utile per correggere il danneggiamento del file local.xml.	
-l inizio	Attiva/disattiva la registrazione dinamica di debug e kernel (il trigger è una L minuscola).	Questo stato rimane attivo fino a quando non viene disattivato, il servizio non viene riavviato o non viene configurato un nuovo criterio per modificare il livello di registrazione.
-l stop	Disattivare dinamicamente la registrazione di debug e kernel (il trigger è un L minuscolo).	
-unblock file_SHA	Questa opzione sblocca l'esecuzione di un processo. Dopo l'esecuzione di questa opzione di comando, è possibile rimuovere l'applicazione dalla cache del kernel locale dell'elenco di blocco delle applicazioni.	Questo comando può essere utilizzato quando un'applicazione viene bloccata a causa di un falso positivo o di un errore e si desidera sbloccare rapidamente l'applicazione senza attendere 30 minuti o riavviare il computer.
-ri-registra	Questa opzione consente di cancellare l'uuid e i certificati dal file local.xml e dal Registro di sistema durante l'esecuzione del servizio e di attivare una nuova registrazione. Local.xml e il Registro di sistema vengono aggiornati con i nuovi valori. Tuttavia, questa condizione viene bloccata se Sincronizzazione ID è abilitata e il connettore ottiene di nuovo l'UUID esistente. In questo modo, il connettore può essere posizionato nel	Se la protezione del connettore è attivata, è necessario immettere quanto segue: sfc.exe -reregister _password_

	gruppo/criterio predefinito dopo la registrazione, se il pacchetto di installazione utilizzato per l'installazione iniziale è stato modificato.	
-forceupdate	Questa opzione forza il connettore ad aggiornare le definizioni TETRA.	
-forceapdeupdate	Questa opzione forza il connettore ad aggiornare le definizioni di protezione comportamentale.	È possibile controllare le definizioni di protezione comportamentale correnti installate sull'endpoint nella traiettoria del dispositivo nel dashboard dell'endpoint sicuro.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- Cisco Secure Endpoint - Note tecniche
- Cisco Secure Endpoint - Guida per l'utente
- Uso della CLI di Secure Endpoint Mac/Linux

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).