

Cisco Secure Endpoint : Commutateurs de ligne de commande expliqués

Table des matières

[Introduction](#)

[Informations générales](#)

[Commutateurs de ligne de commande Cisco Secure Endpoint](#)

[Commutateurs Secure Endpoint Installer](#)

[amp_installer.exe](#)

[Commutateurs d'outils de diagnostic Secure Endpoint Support](#)

[ipsupporttool.exe](#)

[Commutateurs d'interface utilisateur Secure Endpoint](#)

[iptraytool.exe](#)

[Commutateurs SFC pour terminaux sécurisés](#)

[sfc.exe](#)

[Informations connexes](#)

Introduction

Ce document décrit les commutateurs de ligne de commande (CLI) disponibles avec Cisco Secure Endpoint.

Informations générales

Cisco Secure Endpoint contient de nombreuses fonctionnalités et actions personnalisables qui peuvent être exécutées localement sur un terminal à l'aide de commutateurs de ligne de commande. Ce document les présente.

Commutateurs de ligne de commande Cisco Secure Endpoint

Commutateurs Secure Endpoint Installer

amp_installer.exe

1. Ouvrez l'invite de commandes sous Windows.
2. Accédez au dossier dans lequel se trouve votre programme d'installation à l'invite de commandes (dossier Téléchargements utilisé comme exemple ci-dessous).

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

- Exécutez les commutateurs disponibles fournis.
amp_protect.exe <switch>



Remarque : aucune sortie ne sera retournée après l'exécution des commandes.



Conseil : plusieurs commutateurs peuvent être utilisés simultanément.

Commutateur de	Description de	Remarques spéciales
----------------	----------------	---------------------

ligne de commande	commande	
/S	Utilisé pour mettre l'installateur en mode silencieux.	
/temppath	Permet de spécifier un emplacement temporaire personnalisé pour les fichiers d'installation à extraire et à exécuter.	/temppath C:\
/desktopicon 0	Permet de spécifier qu'aucune icône de bureau n'est créée.	Il s'agit de la configuration par défaut et il n'est pas nécessaire de la fournir.
/desktopicon 1	Permet de spécifier la création d'une icône de bureau.	
/startmenu 0	Les raccourcis du menu Démarrer ne sont pas créés.	
/startmenu 1	Les raccourcis du menu Démarrer sont créés.	Il s'agit de la configuration par défaut et il n'est pas nécessaire de la fournir.
/contextmenu 0	Désactive Analyser maintenant à partir du menu	

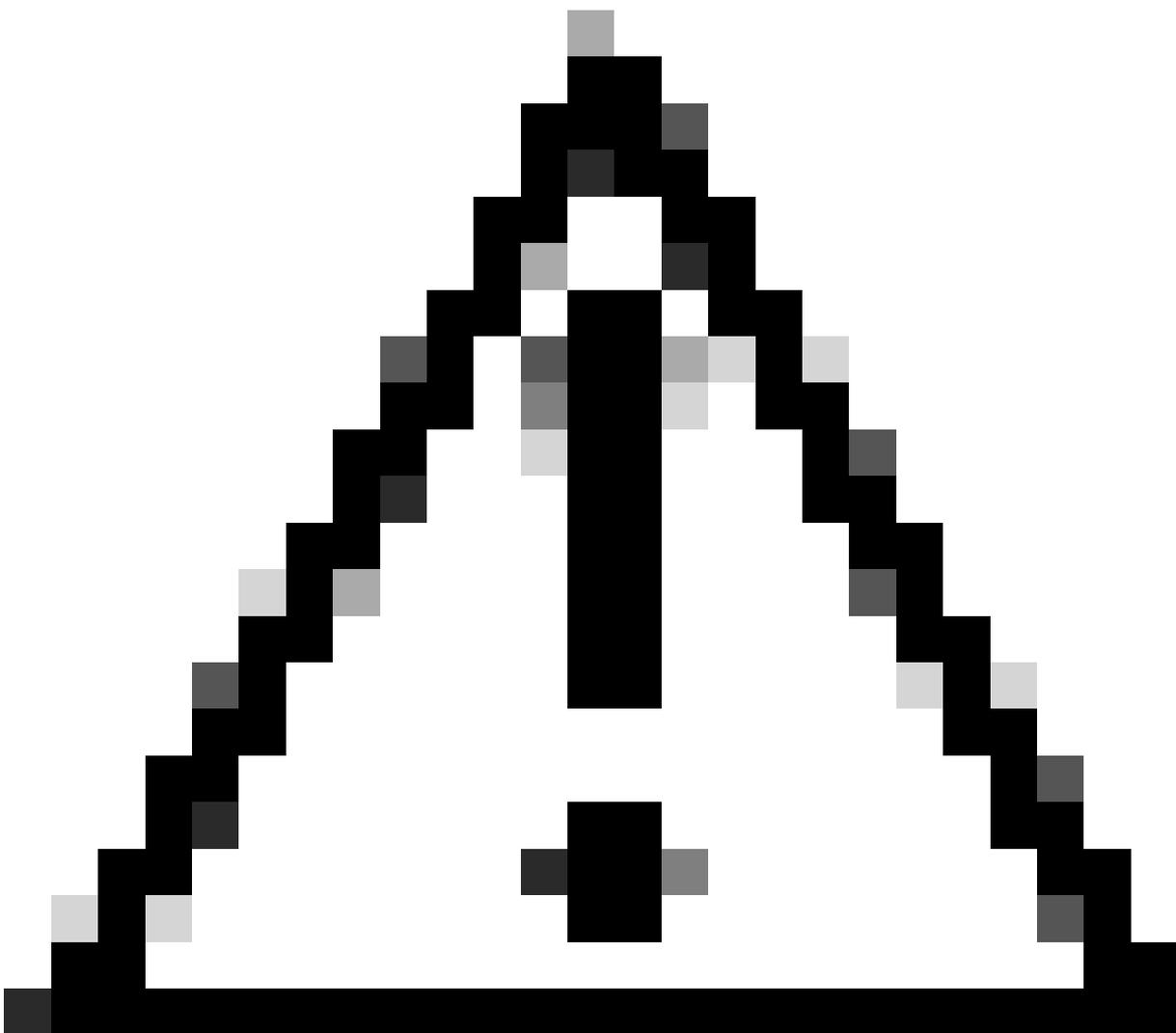
	contextuel accessible par un clic droit.	
/contextmenu 1	Active l'option Analyser maintenant dans le menu contextuel accessible par un clic droit.	Il s'agit de la configuration par défaut et il n'est pas nécessaire de la fournir.
/remove 0	Désinstalle le connecteur et laisse les fichiers pour une réinstallation ultérieure.	Les fichiers XML avec l'UUID restent et vous permettent de réutiliser l'objet ordinateur existant lors de la réinstallation du connecteur. Les fichiers journaux sont également conservés. Si un mot de passe de protection de connecteur est utilisé, il doit être spécifié à l'aide de l'indicateur /uninstallpassword.
/remove 1	Désinstalle le connecteur et supprime tous les fichiers associés.	Si un mot de passe de protection de connecteur est utilisé, il doit être spécifié à l'aide de l'indicateur /uninstallpassword.
/uninstallpassword	Spécifie le mot de passe de désinstallation lors de l'utilisation de l'indicateur /remove. Doit être spécifié si la fonction de protection des connecteurs est activée	Spécifiez le mot de passe de désinstallation après l'indicateur.
/skipdfc 1	Ignorez l'installation du pilote DFC.	Tous les connecteurs installés avec cet indicateur doivent se trouver dans un groupe avec une stratégie dont le moteur réseau est désactivé.

/skiptetra 1	Ignorez l'installation du pilote TETRA.	Tous les connecteurs installés avec cet indicateur doivent faire partie d'un groupe avec une stratégie dont l'indicateur Tetra n'est pas activé.
/D=[CHEMIN]	Utilisé pour spécifier le répertoire dans lequel effectuer l'installation. Par exemple, /D=C:\	<p>Ce paramètre doit être spécifié comme dernier paramètre.</p> <p>Pour le commutateur de ligne de commande /D=, le répertoire d'installation par défaut varie de Operating System. Voici les répertoires d'installation par défaut sous Microsoft Windows XP avec Service Pack 3 ou version ultérieure :</p> <p>Pour les plates-formes x86 :</p> <p>C:\Program Files (x86)\Cisco\AMP</p> <p>Pour les plates-formes x64 :</p> <p>C:\Program Files\Cisco\AMP</p>
/goldenimage 1	Installe le connecteur pour préparer les images dorées.	<p>Ce drapeau est conçu pour aider à préparer des images d'or dans des environnements virtuels. L'utilisation de cet indicateur empêche le connecteur de démarrer et de s'enregistrer lors de la création de l'image dorée. Pour plus d'informations, consultez :</p> <p>Comment préparer une image optimale avec des terminaux sécurisés</p> <p>https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html</p>
/skiposcheck 1	Ignore la vérification du système d'exploitation pendant l'installation.	Cet indicateur peut être utilisé pour installer Secure Endpoint sur les systèmes d'exploitation avec lesquels il n'est pas compatible.

- Ouvrez l'invite de commandes sous Windows.
- Accédez au dossier de l'invite de commandes. Chemin par défaut : **C:\Program Files\Cisco\AMP\X.X.X**, le X.X.X indique le numéro de version).
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- Exécutez les commutateurs disponibles fournis.
ipsupporttool.exe <switch>



Remarque : lors de l'exécution des commutateurs, aucune sortie ne sera retournée.



Attention : tout commutateur qui fait référence à un choix de dossier nécessite que les dossiers soient déjà présents.

Commutateur de ligne de commande	Description de commande	Remarques spéciales
-o <chemin>	Spécifie le dossier de sortie de l'outil Support.	La valeur par défaut est le bureau si cette option n'est pas spécifiée.
-d <chemin_installation>	Spécifie le dossier à partir duquel l'outil de support Windows peut récupérer des fichiers.	La valeur par défaut est le répertoire d'installation par défaut de Secure Endpoint si aucune valeur n'est spécifiée.
-t <minutes>	Exécute un diagnostic de niveau de débogage temporisé à partir de l'outil de support Windows pendant la durée spécifiée. La durée est spécifiée en minutes.	

Commutateurs d'interface utilisateur Secure Endpoint

iptraytool.exe



Remarque : le fichier iptraytool.exe n'est disponible que sur les versions héritées de Secure Endpoint.

-
- Ouvrez l'invite de commandes sous Windows.
 - Accédez au dossier à l'invite de commandes. Chemin par défaut : C:\Program Files\Cisco\AMP\X.X.X\, le X.X.X indique le numéro de version).
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
 - Exécutez les commutateurs disponibles fournis.
iptray.exe <switch>

Commutateur de ligne de commande	Description de commande	Remarques spéciales
-f	Permet de rendre l'interface utilisateur du client active à partir de la ligne de commande.	Cela n'est nécessaire que si l'interface utilisateur graphique d'un terminal est désactivée via la stratégie lorsque l'option Démarrer l'interface utilisateur du client est désactivée.

Commutateurs SFC pour terminaux sécurisés

sfc.exe

- Ouvrez l'invite de commandes sous Windows.
- Accédez au dossier à l'invite de commandes. Chemin par défaut : C:\Program Files\Cisco\AMP\X.X.X\, le X.X.X indique le numéro de version).
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- Exécuter les commutateurs disponibles fournis
sfc.exe <switch>

Commutateur de ligne de commande	Description de commande	Remarques spéciales
-s	Démarrez le service Immune Protect (Connecteur Windows). Le service doit déjà avoir été enregistré auprès de SCM pour être démarré.	
-k	Arrêtez le service Immune Protect (Connecteur Windows).	Si la protection du connecteur est activée, entrez le mot de passe après -k afin d'arrêter avec succès le service.
-u	Désinstallez le service Immune Protect (Connecteur Windows). Désinscrire le service avec le Gestionnaire de contrôle des services Windows (SCM). Cette option est utilisée par le programme de désinstallation pour désinstaller	

	le service Connecteur Windows.	
-r	Réinitialise le service Immune Protect (Connecteur Windows). Cette option est très similaire à l'option -i mais n'installe pas le service. Cela est utile pour réparer la corruption local.xml.	
-l début	Basculer dynamiquement le débogage et la journalisation du noyau (le déclencheur est un L minuscule).	Cet état est conservé jusqu'à ce que vous le désactiviez, que le service redémarre ou qu'une nouvelle stratégie soit configurée pour modifier le niveau de journalisation.
-l stop	Désactivez le débogage et la journalisation du noyau dynamiquement (le déclencheur est un L minuscule).	
-unblock SHA_of_file	Cette option débloque l'exécution d'un processus. Une fois ce commutateur de commande exécuté, l'application peut être supprimée du cache du noyau local de la liste de blocage d'application.	Cette commande peut être utilisée lorsqu'une application est bloquée en raison d'un faux positif ou d'une erreur, et que vous souhaitez débloquer rapidement l'application sans attendre 30 minutes ni redémarrer la machine.
reenregistrement	Cette option peut effacer l'uuid et les certificats du fichier local.xml et du registre pendant l'exécution du service, et déclenche une réinscription. Local.xml et le Registre sont mis à jour avec de nouvelles valeurs. Cependant, cette option est bloquée si la synchronisation d'ID est activée et si le connecteur obtient à nouveau l'UUID existant. Cela peut placer le connecteur dans le groupe/la stratégie par défaut après la réinscription si le package d'installation utilisé pour l'installation initiale a été modifié.	Si la protection du connecteur est activée, vous devez entrer ce qui suit : sfc.exe -reregister _password_

-forceupdate	Cette option force le connecteur à mettre à jour les définitions TETRA.	
-forceapdeupdate	Cette option force le connecteur à mettre à jour les définitions de protection comportementale.	Vous pouvez vérifier les définitions de protection comportementale actuelles installées sur le terminal dans la trajectoire du périphérique dans le tableau de bord Secure Endpoint.

Informations connexes

- [Assistance et documentation techniques - Cisco Systems](#)
- [Cisco Secure Endpoint - Notes techniques](#)
- [Cisco Secure Endpoint - Guide de l'utilisateur](#)
- [Utiliser l'interface de ligne de commande Secure Endpoint Mac/Linux](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.