

# Cisco Secure Endpoint: Command Line Switches Explained

## Contents

---

### [Introduction](#)

### [Background Information](#)

#### [Cisco Secure Endpoint Command Line Switches](#)

##### [Secure Endpoint Installer Switches](#)

[amp\\_installer.exe](#)

##### [Secure Endpoint Support Diagnostic Tool Switches](#)

[ipsupporttool.exe](#)

##### [Secure Endpoint UI Switches](#)

[iptraytool.exe](#)

##### [Secure Endpoint SFC Switches](#)

[sfc.exe](#)

### [Related Information](#)

---

## Introduction

This document describes the Command Line (CLI) switches available to use with Cisco Secure Endpoint.

## Background Information

Cisco Secure Endpoint contains many customizable features and actions which can be performed locally on an endpoint using command line switches. This document showcases them.

## Cisco Secure Endpoint Command Line Switches

### Secure Endpoint Installer Switches

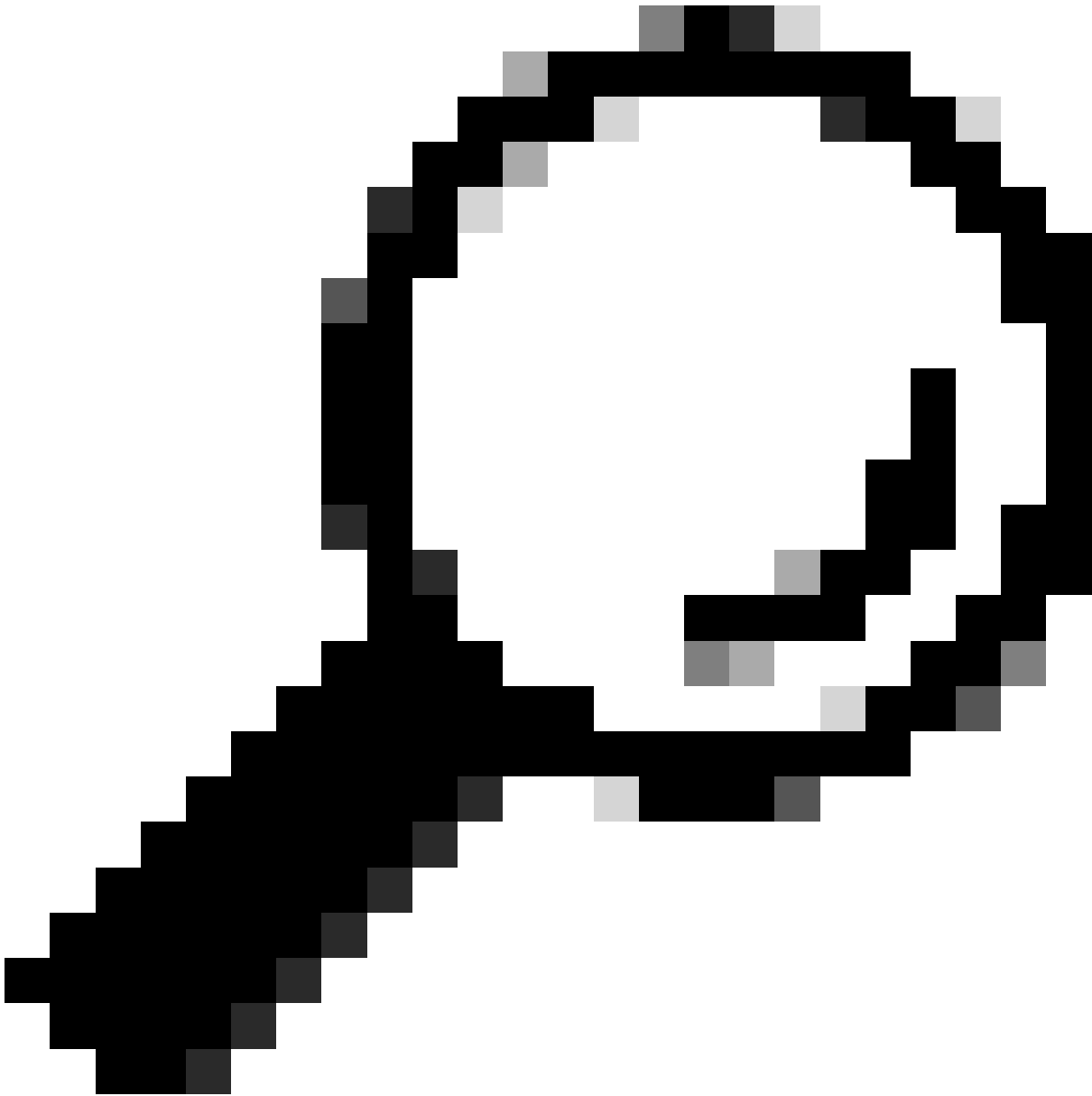
#### amp\_installer.exe

1. Open the command prompt on Windows.
2. Navigate to the folder your installer is located in on the command prompt (Downloads folder used as an example below).  
`cd C:\Users\sysadmin\Downloads`
3. Execute the available switches provided.  
`amp_protect.exe <switch>`



**Note:** No output will be returned after executing the commands.

---



**Tip:** More than one switch can be used at once.

<b>Command Line Switch</b>	<b>Command Description</b>	<b>Special Notes</b>
<b>/S</b>	Used to put the installer into silent mode.	
<b>/temppath</b>	Used to specify a custom temporary location for installation files to be extracted and	<b>/temppath C:\</b>

	executed.	
<b>/desktopicon 0</b>	Used to specify that a desktop icon is not created.	This is the default configuration and does not need to be provided.
<b>/desktopicon 1</b>	Used to specify that a desktop icon is created.	
<b>/startmenu 0</b>	Start Menu shortcuts are not created.	
<b>/startmenu 1</b>	Start Menu shortcuts are created.	This is the default configuration and does not need to be provided.
<b>/contextmenu 0</b>	Disables <b>Scan Now</b> from the right-click context menu.	
<b>/contextmenu 1</b>	Enables <b>Scan Now</b> in the right-click context menu.	This is the default configuration and does not need to be provided.
<b>/remove 0</b>	Uninstalls the connector and leaves files for later reinstallation.	XML files with the UUID remain and allow you to reuse the existing computer object when reinstalling the connector. Log files are preserved as well. If a connector protection password is in use, it must be specified using the <b>/uninstallpassword</b> flag.
<b>/remove 1</b>	Uninstalls the connector and removes all associated files.	If a connector protection password is in use, it must be specified using the <b>/uninstallpassword</b> flag.
<b>/uninstallpassword</b>	Specifies the uninstall password when using the <b>/remove</b> flag. Must be specified if the Connector Protection feature is enabled	Specify the uninstall password after the flag.


<b>/skipdfc 1</b>	Skip installation of the DFC driver.	Any connectors installed with this flag must be in a group with a policy that has the Network engine disabled.
<b>/skiptetra 1</b>	Skip installation of the TETRA driver.	Any connectors installed with this flag must be in a group with a policy that has the Tetra flag unchecked.
<b>/D=[PATH]</b>	Used to specify which directory to perform the install. For example, <b>/D=C:\</b>	<p>This must be specified as the last parameter.</p> <p>For the <b>/D=</b> command line switch, the default installation directory varies from Operating System. Here are the default installation directories on Microsoft Windows XP with Service Pack 3 or later:</p> <p>For x86 Platforms: C:\Program Files (x86)\Cisco\AMP</p> <p>For x64 Platforms: C:\Program Files\Cisco\AMP</p>
<b>/goldenimage 1</b>	Installs connector to prepare for Golden Images.	<p>This flag is designed to help prepare golden images in virtual environments. Using this flag prevents the connector from starting and registering during Golden Image creation. For more information, please see:</p> <p>How To Prepare a Golden Image with Secure Endpoints  <a href="https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html">https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html</a></p>
<b>/skiposcheck 1</b>	Skips the OS check during installation.	This flag can be used to install Secure Endpoint on operating systems it is not compatible with.

## Secure Endpoint Support Diagnostic Tool Switches

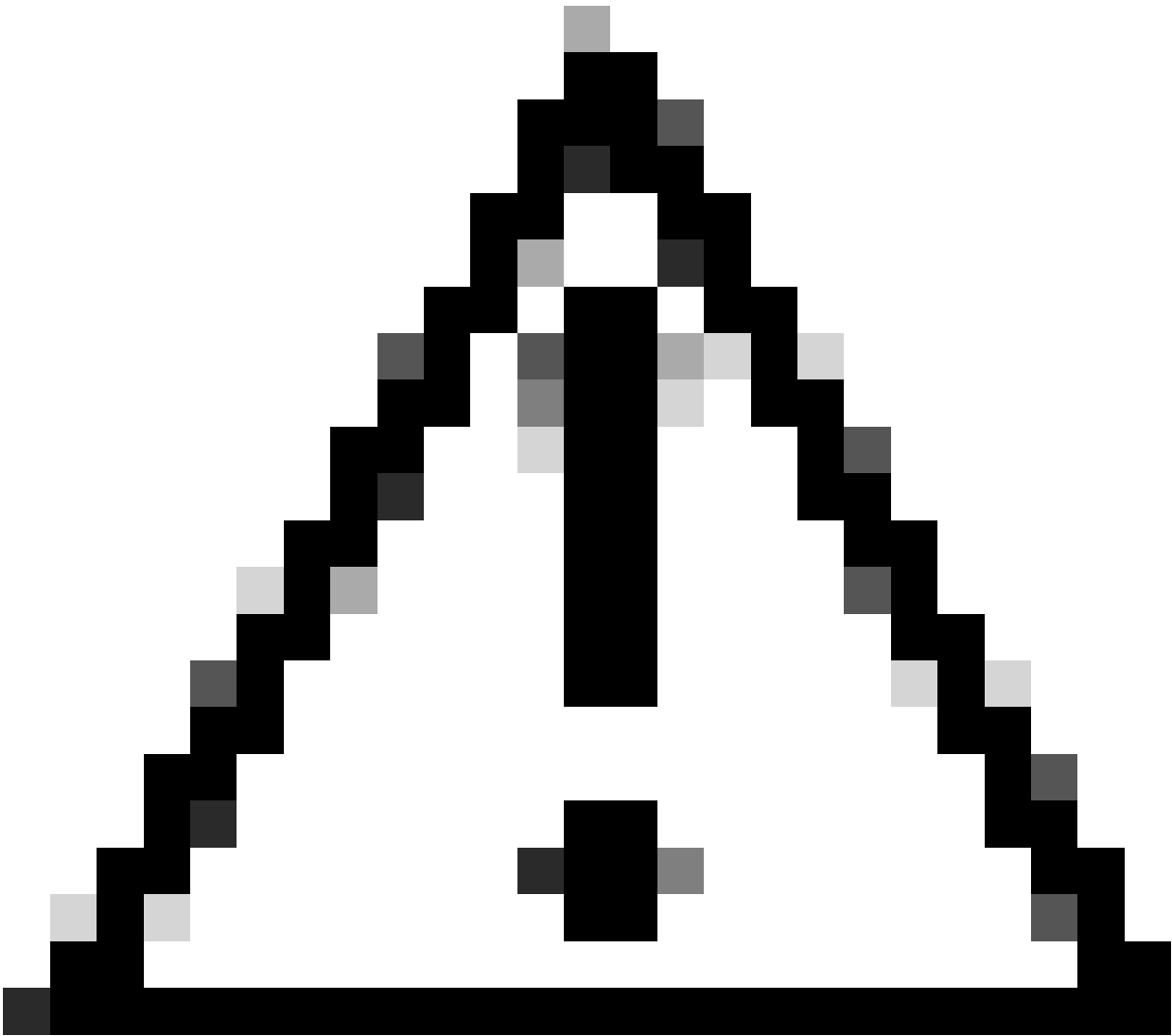
### ipsupporttool.exe

1. Open the command prompt on Windows.
2. Navigate to the folder on the command prompt. Default path: **C:\Program Files\Cisco\AMP\X.X.X\**, the X.X.X denotes the version number).  
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
3. Execute the available switches provided.  
ipsupporttool.exe <switch>

---

 **Note:** On execution of switches, there will be no output returned.

---



**Caution:** Any switch that references a folder choice requires that the the folders already be present.

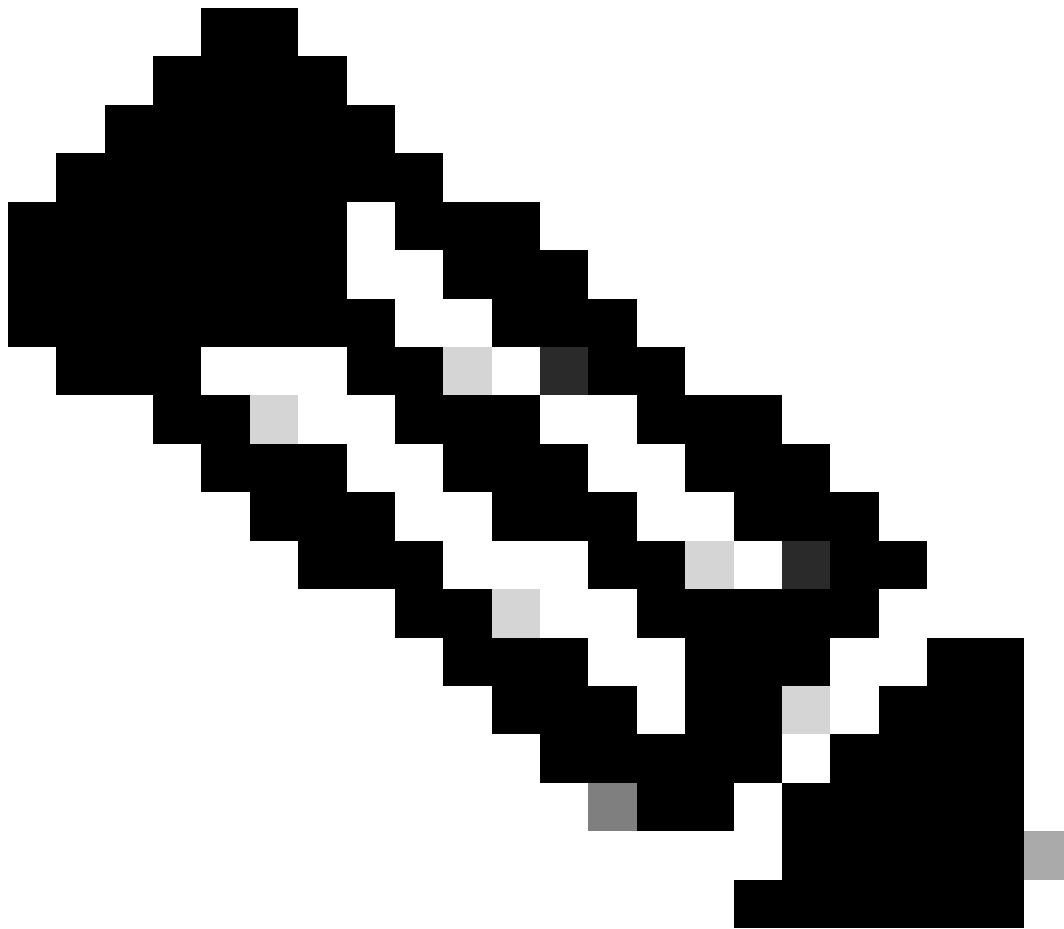
Command Line Switch	Command Description	Special Notes
<b>-o &lt;path&gt;</b>	Specifies the output folder for the Support Tool.	Defaults to the desktop if this option is not specified.
<b>-d &lt;install_path&gt;</b>	Specifies the folder that the Windows Support Tool can retrieve files from.	Defaults to the default installation directory of Secure Endpoint if not specified.
<b>-t &lt;minutes&gt;</b>	Runs a Timed debug level	

	diagnostic from the Windows Support Tool for the specified time. Time duration is specified in minutes.	
--	---	--

## Secure Endpoint UI Switches

**iptraytool.exe**

---



**Note:** The iptraytool.exe file is only available on legacy versions of Secure Endpoint.

---

1. Open the command prompt on Windows.
2. Navigate to the folder at the command prompt. Default path: **C:\Program Files\Cisco\AMP\X.X.X\**, the X.X.X denotes the version number).  
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
3. Execute the available switches provided.

iptray.exe <switch>

Command Line Switch	Command Description	Special Notes
<b>-f</b>	Allows for Client User Interface to be made active from command line.	This is only necessary if an endpoint has GUI turned off via Policy with Start Client User Interface unchecked.

## Secure Endpoint SFC Switches

### sfc.exe

1. Open the command prompt on Windows.
2. Navigate to the folder at the command prompt. Default path: **C:\Program Files\Cisco\AMP\X.X.X\**, the X.X.X denotes the version number).  
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
3. Execute the available switches provided  
sfc.exe <switch>

Command Line Switch	Command Description	Special Notes
<b>-s</b>	Start Immuet Protect (Windows Connector) service. The service must already have been registered with SCM to be started.	
<b>-k</b>	Stop Immuet Protect (Windows Connector) service.	If Connector Protection is enabled, input the password after <b>-k</b> in order to successfully stop the service.
<b>-u</b>	Uninstall Immuet Protect (Windows Connector) service. De-register service with Windows Service Control Manager (SCM). This option is used by the de-installer to uninstall the Windows connector service.	
<b>-r</b>	Resets Immuet Protect (Windows Connector) service. This is very similar to <b>-i</b> option but does not install the service. This is useful to fix local.xml corruption.	
<b>-l start</b>	Toggle debug and kernel logging dynamically (The trigger is a lowercase L).	This state remains until toggled off, the service is restarted, or a new policy is configured to change the logging level.

<b>-l stop</b>	Turn off debug and kernel logging dynamically (The trigger is a lowercase L).	
<b>-unblock SHA_of_file</b>	This option unblocks a process from execution. After this command switch is run, the Application can be removed from the local kernel cache of the application blocking list.	This command can be used when an application is blocked because of false positive or mistake, and you want to quickly unblock the application without waiting for 30 minutes or rebooting the machine.
<b>-reregister</b>	This option can clear the uuid and certs from local.xml and registry while the service is running, and triggers a re-enrollment. Local.xml and registry is updated with new values. However, this is blocked if ID Sync is enabled, and the connector gets existing UUID again. This can place the connector in the default group / policy after reregistration if the installation package used for initial install has been modified.	If Connector Protection is enabled, you need to enter the following: <b>sfc.exe -reregister _password_</b>
<b>-forceupdate</b>	This option forces the connector to update the TETRA definitions.	
<b>-forceapdeupdate</b>	This option forces the connector to update the behavioral protection definitions.	You can check the current behavioral protection definitions installed on the endpoint in device trajectory in the Secure Endpoint dashboard.

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)
- [Cisco Secure Endpoint - TechNotes](#)
- [Cisco Secure Endpoint - User Guide](#)
- [Use the Secure Endpoint Mac/Linux CLI](#)