

Gebruik de Secure Endpoint Mac/Linux CLI

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Cisco Secure Endpoint voor Mac/Linux-CLI](#)

[Naar de CLI navigeren](#)

[Beschikbare CLI-opdrachten](#)

[CLI-opdrachtgebruik](#)

[Aanvullende informatie](#)

Inleiding

Dit document beschrijft de opdrachten van de Command Line Interface (CLI) die beschikbaar zijn voor gebruik met de Secure Endpoint-connector op Linux en MacOS.

Achtergrondinformatie

De CLI-opdrachten zijn beschikbaar voor gebruik door alle gebruikers op een systeem. Sommige opdrachten zijn afhankelijk van beleidsconfiguratie en/of root-machtigingen. De opdrachten die hiervan afhangen, worden in dit artikel openbaar gemaakt.

Cisco Secure Endpoint voor Mac/Linux-CLI

Naar de CLI navigeren

De Secure Endpoint CLI is beschikbaar wanneer de Secure Endpoint-connector is geïnstalleerd en op het systeem actief is:

- Open het Terminalvenster op Mac/Linux.
- Voer de CLI met deze paden uit:
 - op Linux: `/opt/cisco/amp/bin/ampcli`
 - op Mac: `/opt/cisco/amp/ampcli`
- Wanneer de CLI wordt gestart, wordt dit bericht weergegeven:

```
ampcli - Cisco Secure Endpoint Connector Command Line Interface
Interactive mode
```

```
Enter 'q' or Ctrl+c to Exit
```

```
[logger] Set minimum reported log level to notice
Trying to connect...
Connected.
ampcli>
```

Beschikbare CLI-opdrachten

OPMERKING: alle beschikbare CLI-opdrachten kunnen ook direct vanaf de opdrachtregel worden uitgevoerd, bijvoorbeeld `/opt/cisco/amp/bin/ampcli help` of `/opt/cisco/amp/ampcli help` werkt hetzelfde als wanneer u de CLI en `runhelp` start.

- Voor een volledige lijst met CLI-opdrachten kan de gebruiker `help` uitvoeren:

```
ampcli> help
  about          About Cisco Secure Endpoint connector
  definitions    Show virus definitions
  defupdate     Update virus definitions
  exclusions    List custom exclusions
  history       Show event history
               * See 'history help' for more.
  notify        Toggle notifications
  policy        Show policy
  quarantine    List/restore quarantined file(s)
               * See 'quarantine help' for more.
  quit (or q)   Quit ampcli interactive mode
  scan          Initiate/pause/stop a scan
               * See 'scan help' for more.
  status        Get ampd daemon status
               * See 'status help' for more.
  sync          Sync policy
  verbose       Toggle verbose mode
```

- De opdrachten `aftasten`, `historie`, en `quarantaine` neem extra parameters, die worden beschreven als de gebruiker de opdracht samen met `assistentie`:

```
ampcli> scan help
Supported scan parameters:
  flash      Perform a flash scan
  full       Perform a full scan
  custom     Perform a custom scan on a file or directory (recursive)
             e.g. '...> scan custom file_or_directory_to_scan'
  pause      Pause a running scan
  resume     Resume a paused scan
  cancel     Cancel a running scan
  list       List scheduled scans
```

```
ampcli> history help
Supported history parameters:
  list       List history
             * Listing starts at page 1. Each time 'list' is run we move to
               the next page. Specify a page number to jump directly to
               that page.
  pagesize   Set history page size (max: 12)
             * e.g. 'ampcli> history pagesize 10'
```

```
ampcli> quarantine help
Supported quarantine parameters:
```

```
list          List currently quarantined files
* Listing starts at page 1. Each time 'list' is run we move to
  the next page. Specify a page number to jump directly to
  that page.
restore       Restore file by quarantine id
e.g. '...> quarantine restore
```

```
' run 'quarantine list' first to find
```

```
in listing
```

OPMERKING: Gebruik de `help` parameter om de ondersteunde inputparameters voor een bepaald commando te leveren, met uitzondering van de status `help`. Wanneer hulp wordt uitgegeven met de status CLI opdracht, het toont een lijst van alle ondersteunde connector staten, met een korte beschrijving en mogelijke redenen voor elke status. De status van de huidige connector wordt in de tabel ****** aangegeven.

CLI-opdrachtgebruik

- `aftasten`
 - `scan flitser` - voer een flitsscan van het systeem uit.
 - `scan volledig` - voer een volledige scan van het systeem uit.
 - `scannen, aangepast <pad_to_scan>` - een opgegeven bestand of map scannen.
 - `scanpauze` - onderbreek de huidige scans.
 - `scanonderbreking` - hervat alle momenteel gepauzeerde scans.
 - `scannen annuleren` - alle momenteel actieve scans te annuleren.
 - `scanlijst` - een lijst van alle geplande scans die op het systeem moeten worden uitgevoerd.
- `status` - geeft de huidige status van de connector op het systeem aan.
 - `status help` - toon een tabel van alle connector statussen, de huidige connector status, met beschrijvingen van elke status status, en redenen voor een bepaalde staat.

```
ampcli> status
Status:      Connected
Mode:        Normal
Scan:        Ready for scan
Last Scan:   2020-01-22 03:57 PM
Policy:      Audit Policy for Cisco Secure Endpoint (#5755)
Command-line: Enabled
Faults:      None
```

Als een eindpunt aanwezige fouten heeft, toont het veld Faults het aantal aanwezige fouten voor elk prioriteitsniveau (Critical/Major/Minor). Vanaf connector versie 1.12.3 toont de CLI een Fault-ID™s Dit veld geeft de foutcodes weer voor elke fout die op het eindpunt is veroorzaakt. De CLI outputbegeleiding met betrekking tot elke fout die op het eindpunt aanwezig is.

Bijvoorbeeld:

```
Faults:      1 Critical, 1 Major
Fault IDs:   1, 3
  ID 1 - Critical: The system extensions failed to load. Approve the system extensions in Security
  ID 3 - Major: Full Disk Access not granted. Grant access to the ampd daemon executable in Security
```

```
ampcli> status help
  Status      Description      Reason(s)
=====
| Initializing... | Program starting/loading. | --
| Provisioning... | Endpoint identity | --
| enrollment/subscription. |
| Provisioning | Endpoint identity | Cannot reach AMP services.
| failed, retrying | enrollment/subscription failed. | Missing SSL certificates.
| Connector will retry. |
| Registering... | Registering endpoint identity. | --
| Registration | Endpoint identity registration | Cannot reach AMP services.
| failed, retrying | failed. Connector will retry. | Missing SSL certificates.
| Connecting... | Registering with disposition | --
| service. |
| Connection failed, | Registration with disposition | Cannot reach AMP services.
| retrying | service failed. Connector will | Missing SSL certificates.
| retry. |
| ** Connected | Enrollment and registration | --
| succeeded. Connected to AMP |
| services. Connector is operating |
| normally. |
| Disabled | Connector is not operational. | AMP subscription is invalid
| or has expired.
| Disconnected, | Lost connection to the disposition | Network connection to the
| retrying | service after an initial | disposition service has been
| connection was established. | interrupted.
| Connector will attempt to |
| reconnect. |
| Offline (the | The local network has been | Cable disconnected.
| network is down) | disconnected. | The network interface is
| disabled.
```

** indicates the current status of the Connector

Voor Mac-connector versies 1.16.0 en nieuwer en voor Linux-connector versies 1.17.0 en nieuwer, omvat de status de huidige status van Orbital op de computer:

Orbital: Enabled (Running)

Er zijn drie waarden voor de status van de orbitaal:

1. Ingeschakeld (actief): geeft aan dat het huidige beleid Orbital heeft ingeschakeld en dat de Orbital-service momenteel op de computer wordt uitgevoerd.
2. Ingeschakeld (niet actief): geeft aan dat het huidige beleid Orbital ingeschakeld heeft, maar dat de Orbital-service momenteel niet op de computer actief is.
3. Uitgeschakeld: geeft aan dat het huidige beleid Orbital niet heeft ingeschakeld.

Voor Mac-connector versies 1.21.0 en nieuwer (niet op Linux) omvat de status de huidige status van Endpoint Isolation op de computer:

Isolation: Isolated

Er zijn drie waarden voor de status van de orbitaal:

1. Geïsoleerd: geeft aan dat het huidige beleid Endpoint Isolation heeft ingeschakeld en dat de computer is geïsoleerd van het netwerk.
 2. Niet geïsoleerd: geeft aan dat het huidige beleid Endpoint Isolation heeft ingeschakeld en dat de computer niet is geïsoleerd.
 3. Uitgeschakeld in beleid: geeft aan dat het huidige beleid de eindpuntisolatie niet heeft ingeschakeld.
- synchroniseren - synchroniseer de connector met de Cloud om te zorgen voor het nieuwste beleid.
 - beleid - toont het huidige beleid voor de connector:

```
ampcli> policy
Quarantine Behavior:
  Quarantine malicious files.
Protection:
  Monitor program install.
  Monitor program start.
  Passive on-execute mode.
Proxy:      NONE
Notifications: Do not display cloud notifications.
Policy:      Audit Policy for Cisco Secure Endpoint (#5755)
Last Updated: 2020-01-08 04:49 PM
Definition Version: ClamAV(bytecode.cvd: 331, daily.cvd: 25721, main.cvd: 59)
Definitions Last Updated: 2020-01-08 05:09 PM
```

Voor Mac-connector versies 1.16.0 en nieuwer en voor Linux-connector versies 1.17.0 en nieuwer, omvat het beleid de beleidsstatus voor Orbital:

Orbital: Enabled

Er zijn twee waarden voor de Orbital policy setting:

1. Ingeschakeld: Orbital is mogelijk gemaakt via beleid.
2. Gehandicapt: Orbitaal is gehandicapt via beleid.

Voor Mac-connector versies 1.21.0 en nieuwer (niet op Linux) bevat het beleid de beleidsstatus voor Endpoint Isolation:

Isolation: Enabled

Er zijn twee waarden voor de instelling van het isolatiebeleid:

1. Ingeschakeld: Endpoint Isolation is mogelijk via beleid.
2. Uitgeschakeld: Endpoint Isolation is uitgeschakeld via beleid.

- uitsluitingen - de huidige uitsluitingen voor de connector tonen:
 - Deze instelling moet ook zijn ingeschakeld in het aansluitbeleid zodat uitsluitingen kunnen worden weergegeven.

```
ampcli> exclusions
Exclusions:
Path          /home
Path          /mnt/hgfs
Regular Expression /var/log/.*\log
```

- historie
 - geschiedenislijst - geef een lijst van de geschiedenis van connectoractiviteit (scans, quarantaine, etc.)
 - history pagesize <numeric_value> - stelt de pagina-grootte in voor de geschiedenisweergave (max. 12)

```
ampcli> history pagesize 12
Page size set to 12
```

- quarantaine(*Deze optie is alleen beschikbaar voor gebruikers met basisrechten.*)
 - quarantainelijst - een lijst van de in quarantaine geplaatste goederen op het systeem.
 - quarantaine herstellen <quarantaine_id> - herstel een quarantaine bestand via de quarantaine-id, die kan worden gevonden via de quarantaine-listcommando.

- isoleren (*Deze optie is alleen beschikbaar voor Mac-connectorversies 1.21.0 en hoger (niet voor Linux)*)
 - stop <token> - stop de isolatiesessie voor endpoints met het token dat wordt gebruikt om de isolatiesessie te starten
- About - geeft informatie, zoals versie en GUID van de connector.

```
ampcli> about
Cisco Secure Endpoint Connector v1.16.0.123
Copyright (c) 2013-2021 Cisco Systems, Inc. All rights reserved.
This product incorporates open source software; refer to
/opt/cisco/amp/doc/acknowledgement.txt for details.
```

```
[ 22b608b3-b20e-4bd3-8b53-def824acce8a ]
```

- defupdate - een verzoek naar de Cloud te sturen om Virus Definitions bij te werken.
- houding - toon schakelaarhouding in formaat JSON
 - postuur prettyprint - print postuur met mooie print JSON formaat

```
ampcli> posture
{"running": true, "connected": true, "connector_version": "1.19.1.1419", "agent_uuid": "e03ecde8-1aee-40
```

- meldingen via een schakelaar in de CLI aan/uit.
 - Deze instelling moet ook zijn ingeschakeld in het aansluitbeleid.
 - Op Mac heeft dit geen invloed op meldingen in de UI.

```
ampcli> notify
Notifications set to on
```

```
ampcli> notify
Notifications set to off
```

- breedvoerig - de omgekeerde logbestanden voor de CLI in- en uitschakelen.

```
ampcli> verbose
Verbose mode set to on
```

```
ampcli> verbose
Verbose mode set to off
```

- opgeven (of q) - Sluit de Secure Endpoint Mac/Linux-connector CLI af.

Aanvullende informatie

[Technische ondersteuning en documentatie â€™ Cisco Systems](#)

[Cisco Secure Endpoint - gebruikershandleiding](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.