Use the Secure Endpoint Mac/Linux CLI

Contents

Introduction

This document describes the Command Line Interface (CLI) commands available for use with the Secure Endpoint connector on Linux and MacOS.

Background Information

The CLI commands are available for use by all users on a system; however, some commands depends on policy configuration and/or root permissions. The commands dependent on this are disclosed throughout this article.

Cisco Secure Endpoint Mac/Linux CLI

Navigate to the CLI

The Secure Endpoint CLI is available when the Secure Endpoint connector is installed and running on the system:

- Open the Terminal window on Mac/Linux.
- Run the CLI with these paths:
  - on Linux:`/opt/cisco/amp/bin/ampcli`
  - on Mac:`/opt/cisco/amp/ampcli`
- When the CLI starts, this message is displayed:

```
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>
```

Available CLI Commands

NOTE: all of the available CLI commands can also be run directly from the command line, for example`/opt/cisco/amp/bin/ampcli help`or`/opt/cisco/amp/ampcli help`works the same as if you start the CLI and run`help`.

- For a full list of CLI commands, the user can run`help`:

```
ampcli> help
    about               About Cisco Secure Endpoint connector
    bp                  Show and sync behavioral protection signatures
                         * See 'bp help' for more.
    clamav              Show and sync ClamAV definitions
                         * See 'clamav help' for more.
    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 ampdaemon status
                         * See 'status help' for more.
    sync                Sync policy
    verbose             Toggle verbose mode
```

- The commands `scan`, `history`, `quarantine` , `clamav`, and`bp`take additional parameters, which are described if the user runs the command along with `help`:

```
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 <quarantine id>'
          run 'quarantine list' first to find <quarantine id> in listing
```

```
ampcli> clamav help
Supported clamav parameters:
  status        Display engine and definition information
  sync          Synchronizes ClamAV definitions
```

```
ampcli> bp help
Supported bp parameters:
  status        Display engine and definition information
  sync          Synchronizes BP signatures
```

NOTE: Use the `help`parameter to provide the supported input parameters for a given command, with the exception of `status help`. When `help`is issued with the status CLI command, it displays a list of all supported connector states, with a short description and possible reasons for each status. The current connector status is indicated in the table by **.

CLI Command Usage

- `about` - provides information, such as version and GUID of the 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 ]
```

- `bp`*(This option is only available for Linux connector versions 1.22.0 and higher (not on Mac))*
  - `status` - display Behavioral Protection engine and definition information
    - If Behavioral Protection is not enabled then no additional engine or signature information is provided:

```
ampcli> bp status
Behavioral Protection is not enabled
```

    - If Behavioral Protection is enabled then the engine, mode, and signature information is displayed:

```
ampcli> bp status
APDE Engine Version:              3.1.0.0
BP Mode:                          Protect
BP Signature Serial Number:       8071
BP Signature Last Loaded:         2023-05-02 05:44:09 PM
```

    - `sync` - synchronize the Behavioral Protection signatures

- `clamav`
    - `status` - display clamav engine and definition information

```
ampcli> clamav status
Definition Version:       ClamAV(bytecode.cvd: 334, daily.cvd: 26893, main.cvd: 62)
Definitions Published:    bytecode.cvd: 22 Feb 2023 16-33 -0500
                          daily.cvd: 01 May 2023 03-22 -0400
                          main.cvd: 16 Sep 2021 08-32 -0400
Definitions Last Updated: 2023-05-01 04:01:55 PM
```

    - `sync` - synchronize the clamav signatures

- `defupdate` - send a request to the Cloud to update Virus Definitions.

- `exclusions` - show the current exclusions for the connector:
    - This setting must also be enabled in the connector policy for exclusions to be shown.

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

- `history`
    - `history list` - list the history of connector activity (scans, quarantines, and so on)
    - `history pagesize <numeric_value>` - sets the pagesize for the history view (max 12)

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

- `isolate` *(This option is only available for Mac connector versions 1.21.0 and higher (not on Linux))*
    - `isolate stop <token>` - stop endpoint isolation session with the token used to start the isolation session

- `notify` - toggle connector notifications in the CLI on/off.
    - This setting must also be enabled in the connector policy.
    - On Mac, this does not affect notifications in the UI.

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

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

- `policy` - shows the current policy for the 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
```

For Mac connector versions 1.16.0 and newer and for Linux connector versions 1.17.0 and newer, `policy`includes the policy status for Orbital:

```
Orbital: Enabled
```

There are two values for the Orbital policy setting:

1. Enabled: Orbital is enabled via policy.
2. Disabled: Orbital is disabled via policy.

For Mac connector versions 1.21.0 and newer (not on Linux), `policy`includes the policy status for Endpoint Isolation:

```
Isolation: Enabled
```

There are two values for the Isolation policy setting:

1. Enabled: Endpoint Isolation is enabled via policy.
2. Disabled: Endpoint Isolation is disabled via policy.

- `posture` - show connector posture in JSON format
    - `posture prettyprint` - print posture with pretty print JSON format

```
ampcli> posture
{"running": true, "connected": true, "connector_version": "1.19.1.1419", "agent_uuid": "e03ecde8-1aee-4c
```

- `quarantine`(*This option is only available for users with root privileges.*)
    - `quarantine list` - list the quarantined items on the system.
    - `quarantine restore <quarantine_id>` - restore a quarantined file via the quarantine id, which can be found via the `quarantine list`command.

- `quit (or q)` - quit the Secure Endpoint Mac/Linux connector CLI.

- `scan`

    - `scan flash`- perform a flash scan of the system.
    - `scan full`- perform a full scan of the system.
    - `scan custom <path_to_scan>` - scan a specified file or directory.
    - `scan pause` - pause any currently running scans.
    - `scan resume` - resume any currently paused scans.
    - `scan cancel` - cancel any currently running scans.
    - `scan list` - list any scheduled scans to be performed on the system.

- `status` - provides the current status of the connector on the system.
    - `status help`- display a table of all connector statuses, the current connector status, with descriptions of each status state, and reasons for a given state.

```
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
```

If an endpoint has faults present, the Faults field shows the number of faults present for each severity level (Critical/Major/Minor). As of connector version 1.12.3, the CLI shows a`Fault IDs`field, which shows the Fault Codes for each fault raised on the endpoint. The CLI outputs guidance related to each fault present on the endpoint.

ex:

```
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 ampdaemon 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
```

For Mac connector versions 1.16.0 and newer and for Linux connector versions 1.17.0 and newer, `status`includes the current status of Orbital on the computer:

```
Orbital: Enabled (Running)
```

There are three values for the Orbital status:

1. Enabled (Running): indicates the current policy has enabled Orbital and the Orbital service is currently running on the computer.
2. Enabled (Not Running): indicates the current policy has enabled Orbital but the Orbital service is currently not running on the computer.
3. Disabled: indicates the current policy has not enabled Orbital.

For Mac connector versions 1.21.0 and newer (not on Linux), `status`includes the current status of Endpoint Isolation on the computer:

```
Isolation: Isolated
```

There are three values for the Orbital status:

1. Isolated: indicates the current policy has enabled Endpoint Isolation and the computer is isolated from the network.
2. Not Isolated: indicates the current policy has enabled Endpoint Isolation and the computer is not isolated.
3. Disabled in Policy: indicates the current policy has not enabled Endpoint Isolation.

- `sync` - sync the connector with the Cloud to ensure latest policy.
- `verbose` - toggle verbose logs for the CLI on/off.

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

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

Additional Information

Technical Support & Documentation - Cisco Systems

Cisco Secure Endpoint - User Guide