Ø¥Ø³ØªØ®Ø¯Ø§Ù… Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ø§Ù„Ø®Ø§Øµ Ø¨Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§Ø©Ø© Ø§Ù„Ø¢Ù…Ù† Mac/Linux

Ø§Ù„Ù…ØØªÙ^ÙŠØ§Øª

Ø§Ù„Ù…Ù‚Ø¯Ù…Ø©

ÙŠØµÙ‰ Ù‡Ø°Ø§ Ø§Ù„Ù…Ø³ØªÙ†Ø¯ Ø£Ù^Ø§Ù…Ø± Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ø§Ù„Ù…ØªÙ^Ù€Ø±Ø© Ù„Ø§Ø³ØªØ®Ø¯Ø§Ù… Ù…Ø¹ Ù…Ù†ØªØ¬ Cisco Secure Endpoint Mac/Linux Ù^ MacOS.

Ù…Ø¹Ù„Ù^Ù…Ø§Øª Ø£Ø³Ø§Ø³ÙŠØ©

ØªÙƒÙ^Ù† Ø£Ù^Ø§Ù…Ø± Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ù…ØªØ§ØØ© Ù„Ø§Ø³ØªØ®Ø¯Ø§Ù… Ù…Ø¹ Ù¬Ù„ Ù†Ù‚Ø·Ø© SØªØ¹ØªÙ…Ø¯ Ø£Ù^Ø§Ù…Ø± OME Ø¹Ù„Ù‰ ØªÙƒÙ^ÙŠÙ† Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ù^/Ø£Ù^ Ø£Ø°Ù^Ù†Ø§Øª Ø§Ù„Ø¬Ø°Ø±. Ù^Ø§Ù„Ø§Ù^Ø§Ù…Ø± Ø§Ù„ØªÙŠ ØªØ¹ØªÙ…Ø¯ Ø¹Ù„Ù‰ ÙŠÙƒÙ´Ù€ Ø¹Ù†Ù‡Ø§ Ù€Ù†Ù Ùƒ Ù‡Ø°Ù‡ Ø§Ù„Ù...Ù‚Ø§Ù„Ø©.

Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ù„ Cisco Secure Endpoint Mac/Linux

Ø§Ù†ØªÙ‚Ù„ Ø¥Ù„Ù‰ Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI)

ØªØªÙ^Ù€Ø± Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ù„Ù†Ø¸Ø§Ù… Ø§Ù„Ù†Ø§ÙØ°Ø© Ø§Ù„Ø«Ø§Ø¨ØªØ© Ø¹Ø¨Ø± Ù^ÙµÙ„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø§Ù„Ø¢Ù…Ù† Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± Ø§Ù„Ù...Ù‚Ø§Ù„Ø© Ø¹Ù„Ù‰ Ù†Ø¸Ø§Ù… Ø§Ù„ØªØ´ØºÙŠÙ„ Ø¹Ù„Ù‰ Ø§Ù„Ù†Ø¸Ø§Ù...:

- Ø§Ù€Ø°Ø Ù†Ø§Ù€Ø°Ø© Ø§Ù„Ù...ØØ·Ø© Ø§Ù„Ø·Ø±Ù€ÙŠØ© Ø¹Ù„Ù‰ Mac/Linux.
- Ø´Ø°Ù„ CLI Ù…Ø¹ Ù‡Ø°Ø§ Ù…Ù…Ø§Ø«Ù„:
  - Ø¹Ù„Ù‰ Linux:`/opt/cisco/amp/bin/ampcli`
  - Ø¹Ù„Ù‰ Mac:`/opt/cisco/amp/ampcli`
- Ø¹Ù†Ø¯ Ø¯Ø¡ Ø´Ø´Ù„ Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI)ØŒ ÙŠØªÙ…

Ø¹Ø±Ø¶ Ù‡Ø°Ù‡ Ø§Ù„Ø±Ø³Ø§Ù„Ø©:

```
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>
```

Ø£Ù^Ø§Ù…Ø± CLI Ø§Ù„Ù…ØªÙ€Ø±Ø©

Ù…Ù„Ø§ØØ¸Ø©: ÙŠÙ…Ùƒ Ø£ÙŠØ¶Ø§ Øªøºï Ø¹Ø´ØºÙŠÙ„ Ø¬Ù…ÙŠØ¹ Ø£Ù^Ø§Ù…Ø± Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ø§Ù„Ù…Ø¹Ø§Ø§Ø© Ù…Ø¨Ø§Ø´Ø±Ø© Ù…Ù† Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø±Œ Ø¹Ù‰ Ø³Ø¨ÙŠÙŠ Ø§Ù„Ù…Ø«Ø§Ù„ `/opt/cisco/amp/bin/ampcli help` `/opt/cisco/amp/amcli` **ÙŠØ¹Ù…Ù„** Ø§Ù„Ù…Ø§Ø¯Ø© Ø§Ù„Ø·ÙŠØ±Ø§Ù† Ø¹Ø¨Ø± Ø¨Ø¹Ø¶ Ø¹Ø¨Ø¡ Ø¨Ù…Ø« Ø¨Ø¨Ø§ Ù‡Ø§Ø§ Ø¥Ø°Ø§ Ù‡Ø§ Ø¨Ø¹Ø¶ Ù^Ø§Ø¬Ù‡Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù^Ø§Ù…Ø± (CLI) Ù^`runhelp`.

- Ù„Ù„ØØµÙ^Ù„ Ø¹Ù„Ù‰ Ù‚Ø§Ø¦Ù…Ø© Ùƒ§Ù…Ù„Ø© Ù…Ù† Ø£Ù^Ø§Ù…Ø± CLIØŒ ÙŠÙ…Ùƒ Ø§Ø³Ø¨Ø®Ø¯Ø§Ù… Ø§Ù„Ø£Ù^Ø§Ù…Ø± Ø§Ù„ØªØ§Ù„ÙŠØ©:

```
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
```

- Ø§Ù„Ø£Ù^Ø§Ù…Ø± Ù…Ø³Ø¤ÙˆÙ„ØŒ Ø¹Ù„Ù‰ Ø³Ø¨ÙŠÙ„ Ø§Ù„Ù…Ø«Ø§Ù„ØŒ Ø§Ù„Ø£Ù…Ø± `clamav` Ù^ÙŠØªØ¶Ù…Ù† Ø¹Ø¯Ø© Ø¥Ø¬Ø±Ø§Ø¡Ø§Øª Ø¨Ø§Ù„Ù†Ø³Ø¨Ø© Ø¥Ù„Ù‰ Ø§Ù„Ø£Ù…Ø± Ø§Ù„Ø£Ø³Ø§Ø³ÙŠ Ø§Ù„Ø°ÙŠ Ù‚Ø¯ Ù„Ø§ ÙŠÙƒÙˆÙ† Ù…Ø¹Ø±ÙˆÙØ§Ù‹ Ø¨Ø´ÙƒÙ„ Ø¬ÙŠØ¯.

```
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









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
```

Ù…Ù„Ø§ØØ¸Ø©:Ø¥Ø³ØªØ®Ø¯Ø§Ù…Ù…Ø§ Ø§Ù„Ù…Ø§ Ù„Ù„Ù…Ø³ØªØ®Ø¯Ù… Ø§Ù„Ù…Ø¹Ø±Ù Ø§Ù„Ø¹Ø§Ù… Ù„Ø£Ù…Ø± Ø§Ù„Ù‡Ø¬ÙˆÙ… Ø¨Ø§Ø³ØªØ®Ø¯Ø§Ù… Ø§Ù„Ø³Ù„ÙˆÙƒ Ø¨Ø§Ø³ØªØ®Ø¦ Ø§Ù„Ø³Ù„ÙˆÙƒ. Ø¹Ù†Ø¯ Ø§Ù„Ù…Ø³ØªØ¹Ø±Ø§Ø¶Ø© Ø¥Ø§Ø³ØªØ®Ø¯Ø§Ù… Ø£Ù…Ø± CLI (Ù‚Ø§Ø¦Ù…Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù‚Ø§Ù…) Ø§Ù„Ø®Ø§Ø¯Ù… Ø¨Ø§Ù„Ø§Ù‚ØªØ±Ø§Ù† Ù‚Ø§Ø¦Ù…Ø© Ø¹Ù¦Ù…Ø© Ø¨Ø¹Ø¶ Ø§Ù„Ø¹Ø§Ø§Ù„Ø¬Ø§Øª Ø§Ù„Ø¹Ø§Ù…Ø© Ø§Ù„Ù…Ø¹Ø±Ù Ø§Ù„Ø¹Ø§Ù…Ø© Ù„Ø£Ù…Ø± Ø¥Ø¹Ø§Ø¯Ø© Ø¨Ø¯Ø¡ Ø§Ù„Ø®Ø¯Ù…Ø© Ø§Ù„Ø¹Ø§Ù…Ø© Ø§Ù„Ø¹Ø§Ù…Ø© Ø§Ù„Ø¹Ø§

```
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
```

    - Ø§Ù„Ù…Ø²Ø§Ù…Ù†Ø© - Ù…Ø²Ø§Ù…Ù†Ø© ØªÙ‚ÙˆÙŠØ¹Ø§Øª Ø§Ù„Ø„ØÙ…Ø§ÙŠØ© Ø§Ù„Ø„Ø³Ù„ÙˆÙƒÙŠØ©

- Ùƒ„Ø§Ù…Ø§Ù‹
    - Ø§Ù„Ø„Ø© - Ø¹Ø±Ø¶ Ù…ØØ±Ùƒ Ø§Ù„Ù…Ø·Ø§Ø¨Ù‚Ø© ÙˆÙ…Ø¹Ù„ÙˆÙ…Ø§Øª Ø§Ù„Ø„ØªÙ‡Ø¯ÙŠØ¯

```
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
```

    - Ù…Ø²Ø§Ù…Ù†Ø© - Ù…Ø²Ø§Ù…Ù†Ø© ØªÙ‚ÙˆÙŠØ¹Ø§Øª Ø§Ù„Ù…Ø·Ø§Ø¨Ù‚Ø©

- Ø¯ÙŠÙ†Ø¨ÙˆÙŠØª - Ø¥Ø±Ø³Ø§Ù„ Ø·Ù„Ø¨ Ø¥Ù‰ Ù…Ø¬Ù…Ø¹ Ø§Ù„Ø¯ÙØ¹Ø§Øª Ø§Ù„Ø„Ø¯Ø§Ø®Ù„ÙŠØ© Ø§Ù„Ø„Ø¹ÙŠÙ†Ø© Ø§Ù„Ø„ØªÙ‡Ø¯ÙŠØ¯Ø§Øª.

- Ø§Ù„Ø„Ø³Ø¹Ø¨Ø¹Ø¯Ø¯Ø§Øª - Ø¥Ø¸Ù‡Ø§Ø± Ø§Ù„Ø„Ø³Ø¹Ø¨Ø¹Ø¯Ø¯Ø§Øª Ø§Ù„Ø„Ø§Ù„ÙŠÙ† Ù„Ù„Ù…Ø¹Ø§Ù„Ø¬Ø©:
    - ÙŠØ¬Ø¨ Ø£ÙŠØ¶Ø§ Ø¹Ù…ÙŠÙ† Ù‡Ø°Ø§ Ø§Ù„Ø¥Ø¹Ø¯Ø§Ø¯ Ù„Ù„Ø„Ø¹Ø¯Ø¯Ø§Øª Ø§Ù„Ø„Ø§Ù„ÙŠÙ† Ù„Ù„Ù…Ø¹Ø§Ù„Ø¬Ø© Ø§Ù„Ø„Ø³Ø¹Ø¨Ø¹Ø¯Ø¯Ø§Øª.

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

- Ø¹Ø§Ø±Ø¶
    - Ù‚Ø§Ø¦Ù…Ø© Ø§Ù„Ù…Ø±Ø§Ø¬Ø¹Ø© - Ø³Ø±Ø¯ Ù…Ø±Ø§Ø¬Ø¹Ø§Øª Ù†Ø´Ø§Ø· Ø§Ù„Ø„Ù…Ø±Ø§Ø¬Ø¹ (Ø¹Ù…Ù„ÙŠØ§Øª Ø§Ù„Ù…Ø±Ø§Ø¬Ø¹Ø© Ù‚Ø§Ø¦Ù…Ø© Ø§Ù„Ù…Ø¹Ø±Ø§ Ø§Ù„Ù…Ø§Ø§ Ø¥Ù„Ù‰ Ø°Ù„Ùƒ)
    - ØµÙ‚Ø§Ø¡ Ø§Ù„Ø„Ø³Ù„Ø±Ø© <digital_value> - ÙŠØ¶Ø·Ø± Ø¹Ù„Ù‰... Ø§Ù„Ø„Ø¬Ø§Ø§Ø¹Ø© Ù„Ø·Ø±Ù‚Ù‡ Ø¹Ø¹Ø¹Ø¹ (12 Ùƒ Ø£Ù‚Ù‰)

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

- Ù†Ø¹Ø²Ù„ *(ÙŠØªÙˆÙ‹Ø± Ù‡Ø°Ø§ Ø§Ù„Ø®ÙŠØ§Ø± Ù‹Ù,Ø· Ù„Ø¥Øµ Ø¯Ø§Ø±Ø§ Ù…Ù„ Mac 1. 21. 0 Ùˆ§Ù„Ø¥Øµ Ø¯Ø§Ø±Ø§ Ø§Ù„Ø£Ø¹Ù‰ (Ù„ÙŠØ³ Ø¹Ù„Ù‰ Ù†Ø¸Ø§Ù… Ø§Ù„Øºà Ø´Ù„ Linux))*
  - Ø¹Ø²Ù„ Ø¥ÙŠÙ‚Ø§Ù <token> - Ø¥ÙŠÙ‚Ù Ø¬Ù„Ø³Ø© Ø¹Ø²Ù„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø¨Ø§Ø³Øª Ø§Ù„Ø±Ù… Ø§Ù„Ù…Ø³Ø² Ø§Ù„Ù…Ø³ØªØ®Ø¯Ù… Ù„Ø¨Ø¯Ø¡ Ø¬Ù„Ø³Ø© Ø§Ù„Ø¹Ø²Ù„

- Ø¥Ø¹Ø§Ø¯Ø© - ØªÙŠØ¯ Ø¥Ø¹Ø§Ø¯Ø© Ø§Ù„Ù…Ø§Ø³Ø Ù‡ÙŠ ØªØ´ÙºÙŠÙ„/Ø¥ÙŠÙ‚Ø§Ù Ù‹Ø§Ø©Ø© Ù‹Ø·Ø¬Ù‡ Ø³Ø·Ø± Ø§Ù„Ø£Ù‡Ø§Ø¯Ø©.
  - ÙŠØ¬Ø¨ ØªÙ…ÙŠÙ† Ù‡Ø°Ø§ Ø§Ù„Ø¥Ø¹Ø¯Ø§Ø¯ Ø£ÙŠØ¶Ø§ Ù‡ÙŠ Ù†Ù‡Ø¬ Ø§Ù„Ø¥Øµ Ø§Ù„Ø«Ø§Ù„Ø«.
  - Ø¹Ù„Ù‰ MacØŒ Ù„Ø§ ÙŠØ¤Ø«Ø± Ù‡Ø°Ø§ Ø¹Ù„Ù‰ Ø§Ù„Ø¥Ø¹Ø¯Ø§Ø¯ Ù‡ÙŠ Ù†Ù‡Ø¬ Ø§Ù„Ø«Ø§Ù„Ø«.

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

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

- Ø§Ù„Ù†Ø¬Ø¬ - ÙŠØ¹Ø±Ø¶ Ø§Ù„Ø³ÙŠØ§Ø³Ø© Ø§Ù„ØØ§Ù„ÙŠØ© Ù„Ù„Ø…Ù‡Ø§Ø¬Ù…:

```
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
```

Ø¨Ø§Ù„Ù†Ø³Ø¨Ø© Ù„Ù„Ø¥Øµ Ø§Ù„Ø£Ø§Ø³Ø§Ø³ÙŠØ© 1.16.0 Ù„Ù„Ù…Ù‡Ø§Ø¬Ù… Mac Ù‹Ø§Ù„Ø¥Øµ Ø§Ù„Ø£Ø§Ø³Ø§Ø³ÙŠØ© 1.17.0 Ù„Ù„Ù…Ù‡Ø§Ø¬Ù… Linux Ù‹Ø§Ù„Ø¥Øµ Ø§Ù„Ø£Ø§Ø³Ø§Ø³ÙŠØ© ØªÙ…Ø§Ù†Ù…Ù† Ø§Ù„Ø³ÙŠØ§Ø³Ø© Ø§Ù„Ø®Ø§ØµØ© Ø¨Ø§Ù„Ø¹Ù…Ù„Ø§Ø¡ Ø§Ù„Ø°Ù…Ù† Ø§Ù„Ø®Ø§Ø±Ø¬ÙŠÙ†:

```
Orbital: Enabled
```

Ù‡Ù†Ø§ÙƒÙ Ù‚ÙŠÙ…ØªÙ† Ù„Ø¥Ø¹Ø¯Ø§Ø¯ Ø§Ù„Ø³ÙŠØ§Ø³Ø§Øª Ø§Ù„Ù…ØªÙ‚Ø¯Ù…Ø©:

1. ØªÙ…ÙƒÙŠÙ†: ÙŠØªÙ… ØªÙ…ÙƒÙŠÙ† Ø§Ù„Ù…Ø±Ø§Ù‚Ø¨Ø© Ø§Ù„Ø³Ù„ÙˆÙƒÙŠØ©.
2. Ù…Ø¹Ø·Ù„: ØªÙ… ØªØ¹Ø·ÙŠÙ„ Ø§Ù„Ù…Ø±Ø§Ù‚Ø¨Ø© Ø¹Ù†Ø· Ø·Ø±ÙŠÙ‚ Ø§Ù„Ø³ÙŠØ§Ø³Ø©.

Ø¨Ø§Ù„Ù†Ø³Ø¨Ø© Ù„Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª 1.21.0 Ù…Ù† Ù…Ø§Ùƒ Ù‚Ø§Ø¯Ù…Ø© Ø§Ù„Ø£Ø¬Ù‡Ø²Ø© (Ù‚Ù„ÙŠÙ„ Ø¹Ù„Ù‰ Ù†Ø¸Ø§Ù… Linux)ØŒ ÙŠØªÙ…Ø¨Ø§Ù…Ù† Ø§Ù„Ù†Ø‡Ø¬ ØØ§Ù„Ø© Ø§Ù„Ø³ÙŠØ§Ø³Ø© Ù„Ø¹Ù²Ù„ Ù†Ù‚Ø§Ø· Ø§Ù„Ù†Ù‡Ø§ÙŠØ©:

```
Isolation: Enabled
```

Ù‡Ù†Ø§ÙƒÙ Ù‚ÙŠÙ…ØªÙ† Ù„Ø¥Ø¹Ø¯Ø§Ø¯ Ù†Ù‡Ø¬ Ø§Ù„Ø¹Ù…Ù„:

1. Ù…Ù…Ù†Ù†: ØªÙ… ØªÙ…ÙƒÙŠÙ† Ø¹Ù²Ù„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø¹Ù¨Ø± Ø§Ù„Ù†Ù‡Ø§ÙŠØ©.
2. Ù…Ø¹Ø·Ù„: ØªÙ… ØªØ¹Ø·ÙŠÙ„ Ø¹Ù²Ù„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø¹Ù¨Ø± Ø§Ù„Ù†Ù‡Ø§ÙŠØ©.

- Ù‚Ø¶Ø¹ÙŠØ© - Ø¥Ù‡Ø§Ø± ØØ§Ù„Ø© Ø§Ù„Ù…Ø¶ÙŠÙ„ Ø¨ØªÙ†Ø³ÙŠÙ‚ JSON
  - `Posture Prettyprint` - Ù‚Ø¶Ø¹ Ø§Ù„Ø·Ø¨Ø§Ø¹Ø© Ø¨ØªÙ†Ø³ÙŠÙ‚ JSON Ø¬Ù…ÙŠÙ„ Ø§Ù„Ø·Ø¨Ø§Ø¹Ø©

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

- *Ø¬Ø±(ÙŠØªÙ‚Ù‚Ù‚ Ù‡Ø° Ø§Ù„Ø®Ø§Ø§ Ø§Ù„Ù„Ù„ Ù‚Ù„Ù… Ù„Ù„Ù…Ø³Ø¤Ø®Ø¯Ù… Ø°Ù„Ù†Ø¯Ø§Ø§ Ø§Ù„Ù…Ø¤Ø³Ø³Ø§Øª

Ù…ØªÙˆÙ‚Ù‘Ø© Ù…Ø¤Ù‚ØªØ§ ØØ§Ù„ÙŠØ§.

- ØŸÙ„Ø°Ø§ Ø§Ù„Ù…Ø³ØªØ - Ø¥Ù„Ø§ Ø£ÙŠ Ø¹Ù…Ù„ÙŠØ§Øª Ù…Ø³Ø§ØØ© Ø¥Ø¶Ø§ÙÙŠØ© ØªÙ…Ù†Ø¹ Ø¥Ø¬Ø±Ø§Ø¡ Ø§Ù„ØªØØ¯ÙŠØ«.
- Ù‚Ø§Ø¦Ù…Ø© Ø§Ù„Ù…Ø³ØªØ - Ø³Ø±Ø¹Ø© Ø¹Ù…Ù„ÙŠØ§Øª Ù…Ø³Ø Ù…Ø¬Ø¯ÙˆÙ„Ø© Ù…Ø¹ Ø¥Ø¹Ø§Ø¯Ø© Ø§Ù„Ø¨Ø¯Ø¡ Ø¹Ù„Ù‰ Ø§Ù„Ø®Ø§Ø¯Ù….

- Ø§Ù„Ø®Ø§Ù„Ø© - ØªÙˆÙ‚Ø± Ø§Ù„Ø®Ø§Ù„Ø© Ø§Ù„Ø®Ø§Ù„ÙŠØ© Ù„Ù„Ù…ÙˆØµÙ„ Ø¹Ù„Ù‰ Ø§Ù„Ø†Ø¸Ø§Ù….
  - Ø³Ø¹Ù„Ù‰Ø§Ø§Ø§ Ø§Ù„Ø®Ø§Ù„Ø©- Ø¹Ø±Ø¶ Ø¬Ø¨Ù„Ù„ Ø¨Ø¬Ù…Ù„ Ø§Ù„Ø§Ø§Ø§Ù„ÙŠØ¹ Ø§Ù„Ù„Ù…Ø³ØªØ®Ø¯Ù… Ø§Ù„Ø§Ù…Ø± Ø§Ù„Ø§Ø§Ø§Ù„Ø© Ù…Ø¹ Ø£Ù„ Ø§Ø§Ø§Ù„Ø© Ù…Ø£Ø®Ø§Ø± Ùƒ Ù„Ù„ Ø§Ø§Ù„Ø© Ù…Ø£Ø®Ø§Ø± Ø§Ù„Ø§Ø§Ø§Ù„Ø© Ù…Ø¹ Ø£Ø¹Ø§Ø¯Ø© Ø§Ù„Ø¨Ø¯Ø¡.

```
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
```

Ø¥Ø°Ø§ Ùƒ Ø§Ù†Ø· Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø§ØØªÙˆÙŠ Ø¹Ù„Ù‰ Ø£Ø®Ø·Ø§Ø¡ Ù…Ø«Ù„ Ø§Ù„Ø®Ø¯Ù…Ø§Øª Ø§Ù„Ù…Ø¹Ø·Ù„Ø© Ø£Ùˆ Ø§Ù„Ø®Ø¯Ù…Ø§Øª Ø§Ù„Ù…Ø¹Ø·Ù„Ø© Ø¬Ø²Ø¦ÙŠØ§Ù‹ØŒ Ø§Ù„Ø§Ø§Ø§Ù„Ø© Ù…Ø³Ø¤Ù„Ø© Ø¹Ù† Ø§Ù„Ø®Ø¯Ù…Ø§Øª Ø§Ù„Ù…Ø¹Ø·Ù„Ø© (Critical/Major/Minor). Ø§Ø¹Ø§Ø¯Ø© Ø§Ù„Ø†Ø´Ø§Ø· Ù…Ø† Ø§Ù„Ù„Ø¥ØµØ¯Ø§Ø± 1.12.3 Ù…Ø† Ø§Ù„Ù…Ù„Ø„ØŒ ØªØ¸Ù‡Ø± Ù‚Ø§Ø¦Ù…Ø© Ø³Ø·Ø± Ø§Ù„Ø£Ù‚Ø§Ù…Ø± (CLI)Ù…Ø¹Ù·Ø±Ø§Ø¡ Ø§Ù„Ø£Ø®Ø·Ø§Ø¡ Ø§Ù„Ø£Ù‚Ø§Ù…Ø±ØŒ Ø§Ù„Ø°Ù‰ ÙŠØ¹Ø¬Ø² Ø§Ù„Ø£Ø®Ø·Ø§Ø¡ Ø§Ù„Ø†Ø´Ø·Ø© Ø¹Ù„Ù‰ Ø§Ù„Ø†Ø¸Ø§Ù… Ø£Ùˆ Ø§Ù„Ø®Ø¯Ù…Ø§Øª Ø§Ù„Ù…Ø¹Ø·Ù„Ø© Ø¬Ø²Ø¦ÙŠØ§Ù‹. ÙŠÙ†Ø¬Ø¨ Ù‚Ø§Ø¨Ù„ Ø¹Ù„Ù‰ Ø§Ù„Ø£Ù‚Ø§Ù…Ø± (CLI) Ø¥Ø±Ø´Ø§Ø¯ Ø§Ù„Ø¹Ø¹Ù„Ù„Ø© Ø¨Ø¬Ø¹Ù„ Ø®Ø§Ø¯Ù… Ø§Ù„Ø†Ø¸Ø§Ù… Ø¹Ù„Ù‰ Ø§Ù„Ø†Ø´Ø·Ø©.

Ù…Ø«Ø§Ù„:

```
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 failed, retrying	Endpoint identity registration failed. Connector will retry.	Cannot reach AMP services. Missing SSL certificates.
Connecting...	Registering with disposition service.	--
Connection failed, retrying	Registration with disposition service failed. Connector will retry.	Cannot reach AMP services. Missing SSL certificates.
** 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, retrying	Lost connection to the disposition service after an initial connection was established. Connector will attempt to reconnect.	Network connection to the disposition service has been interrupted.
Offline (the network is down)	The local network has been disconnected.	Cable disconnected. The network interface is disabled.

** indicates the current status of the Connector

Ø¨Ø§Ù„Ù†Ø³Ø¨Ø© Ù„Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª Ø§Ù„Ø³Ø§Ø¨Ù‚Ø© 1.16.0 Ù„Ù„Ù…Ùˆ Mac Ù‚Ø§Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª Ø§Ù„Ø£Ø¯Ù« Ù‚Ø§Ù„Ø¥ØµØ¯Ø§Ø± 1.17.0 Ù„Ù„Ù…Ùˆ Linux Ù‚Ø§Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª Ø§Ù„Ø£Ø¯Ù«ØŒÙŠØªØ¹Ù† Ø§Ù„Ù‚Ø¹ Ø§Ù„Ø§Ø³Ù… Ù„Ù„Ù…Ø¯Ø®Ù„ Ø¹Ù„Ù‰ Ø§Ù„Ø¥Ø¯Ø®Ø§Ù„:

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

Ù‡Ù†Ø§Ùƒ Ø«Ù„Ø§Ø« Ù‚ÙŠÙ… Ù„Ù„Ù‚Ø¹ Ø§Ù„Ø§Ø³Ù…:

1. ØªÙ…Ùƒ Ù† (Ø§Ù„Øªø´ÙŠÙ„): ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ø§Ø³Ø© Ø§Ù„Ø§Ø³Ù© Ù„Ø¯ Ù…Ø¯Ø®Ù„ Orbital Ù‚ Orbital service Ù‚ÙŠØ¯ Ø§Ù„Ø¬Ø´ØºÙŠÙ„ Ø§Ù„Ø§Ø³Ø§ Ø¹Ù„Ù‰ Ø§Ù„Ø…Ø¨ÙˆÙŠÙ‚Øª.
2. ØªÙ…Ùƒ Ù† (Ø¹Ø¯Ø´ÙŠÙ„): ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ø§Ø³Ø© Ø§Ù„Ø§Ø³Ù© Ù„Ø¯ Ù…Ø¯Ø®Ù„ Orbital Ù‚Ù„Ùƒ Ø®Ø¯Ù…Ø© Orbital Ù„Ø§ Øªø¹Ù…Ù„ Ø§Ù„Ø§Ø³Ø§ Ø¹Ù„Ù‰ Ø§Ù„Ø…Ø¨ÙˆÙŠÙ‚Øª.
3. Ù…Ø¹Ø·Ù„: ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ø§Ø³Ø© Ø§Ù„Ø§Ø³Ù© Ù„Ù… Øªø¹Ù…Ù„ Ø¨Ø´ÙƒÙ„ Ø¬ÙŠØ¯ Orbital.

Ø¨Ø§Ù„Ù†Ø³Ø¨Ø© Ù„Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª Ù…Ø§ Ù‚Ø¨Ù„ Mac 1.21.0 Ù‚Ø§Ù„Ø¥ØµØ¯Ø§Ø±Ø§Øª Ø§Ù„Ø£Ø¯Ù« (Ù‚Ù„ÙŠÙ³ Ø¹Ù„Ù‰ Ù†Ø¸Ø§Ù… Ø§Ù„Øªø´ÙŠÙ„ Linux)ØŒØªØ¹Ø¯Ù„ Ù†

Ø§Ù„ØØ§Ù„Ø© Ø§Ù„ØØ§Ù„ÙŠØ© Ù„Ø¹Ø²Ù„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø¹Ù„Ù‰ Ø§Ù„ÙƒÙ…Ø¨ÙŠÙˆÙ„Ø±:

```
Isolation: Isolated
```

Ù‡Ù†Ø§Ùƒ Ø«Ù„Ø§Ø« Ù‚ÙŠÙ… Ù„Ù„Ù‚Ø¹ Ø§Ù„Ù…Ø¯Ø§Ø±Ø©:

1. Ù…Ø¹Ø²Ù„: ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ù„Ø³Ø© Ø§Ù„ØØ§Ù„ÙŠØ© Ù‚Ø¯ Ø¹Ø²Ù„Øª Ø§Ù„Ù…Ø¯Ø§Ø±Ø© Ù…Ø¹Ø²Ù„Ø© Ø§Ù„Ø¢Ù† Ø§Ù„Ø¥Ø¯Ø®Ø§Ù„.
2. Ø°ÙŠÙ„ Ù…Ø¹Ø²Ù„: ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ù„Ø³Ø© Ø§Ù„ØØ§Ù„ÙŠØ© Ù‚Ø¯ Ø¹Ø²Ù„Øª Ø§Ù„Ø¢Ù† Ø§Ù„Ø¥Ø¯Ø®Ø§Ù„ Ù„ÙŠØ³ Ù…Ø¹Ø²Ù„Ø§Ù‹.
3. Ù…Ø¹Ø·Ù„ Ù€ÙŠ Ø§Ù„Ù†Ø¬Ø¬: ÙŠØ´ÙŠØ± Ø¥Ù„Ù‰ Ø£Ù† Ø§Ù„Ø³Ù„Ø³Ø© Ø§Ù„ØØ§Ù„ÙŠØ© Ù„Ù… Ø¨Ø¹Ø¯ Ø¹Ø²Ù„ Ø¹Ù†Ø¯ Ø¹Ø¨ÙˆØ± Ø¹Ù¢Ù„ Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ©.

- ø³ø²ø§ù…ù† - Ù…Ø²Ø§Ù…Ù†Ø© Ø§Ù„Ù…Ø¹Ø¯Ø§Øª Ø¹Ù„Ù‰ Ø§Ù„ØØ§Ù„ÙŠØ© Ù„Ø¶Ù…Ø§Ù† Ø£ØØ¯Ø« Ù†Ø³Ø®Ø© Ù„Ø¯Ù‰ Ø£Ø¬Ù†Ø¬Ø© Ù†Ø´Ø·Ø©.

- ø²ù†ø¬ø± - ØªØ´ÙŠØ±/Ø¥ÙŠÙ‚Ø§Ù Ø³Ø´Ø¹ØªÙŠÙ† Ø³Ø¬Ù„ Ø§Ù„Ù…Ø±Ø§Ù‚Ø¨Ø© Ø³Ø·Ø± Ø£Ø¬Ù‡Ø²Ø©.

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

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

Ù…Ø¹Ù„Ù‚Ù…Ø§Øª Ø¥Ø¶Ø§ÙÙŠØ©

Ø§Ù„Ø¯Ø¹Ù… Ø§Ù„ÙÙ†Ù‰ Ù‚Ø§Ù„Ù…Ø³Ø§Ø¹Ø¯Ø© - Cisco Systems

Ù†Ù‚Ø·Ø© Ø§Ù„Ù†Ù‡Ø§ÙŠØ© Ø§Ù„Ø¢Ù…Ù†Ø© Ù„Ø¥Ù…Ø¯Ø§Ø¯ Ù† Cisco - Ø¯Ù„ÙŠÙ„ Ø§Ù„Ù…Ø³Ø³Ø®Ø¯Ù…

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).