Mandiant

COMMAND LINE INSTALLATION AND REGISTRATION - MAC ACTORS

Installing and configuring the Actor can be completed from the command line.

Install the Actor

1. Obtain the installer and add it to the system. The installer can be download from **Library > Actor Installer Files.**
2. Log in to the system as an administrative.
3. For MacBooks with an M1 processor, enable Rosetta.

   If you are running a new MacBook with an M1 processor, installation will fail if Rosetta is not enabled before installing the Actor. To enable Rosetta, run the following command: `softwareupdate --install-rosetta` .

4. (Optional) The default install location is `/Users/Shared/Verodin` . To install in a different location:
   a. In the same directory as the installer package, create a config file named `endpoint.conf` .
   b. Edit the file so it contains the following two lines, where *DESTINATION* is a valid directory that exists on the machine:

   ```
   PATH=DESTINATION
   TYPE=Pull
   ```

   If the directory does not exist when you run the installer, the installer returns an error.

5. Run the following command to install the Actor, where *PATH* is the location of the installer.

   ```
   sudo installer -pkg PATH/VerodinEndpoint-4.8.3.0.pkg -target /Applications
   ```

Configure the Networking and Register the Actor

This process is valid for Mac and Linux Actors.

1. Complete the network configuration using `vsetnet` . This command walks you through configuring the networking.

   If you choose to set it up manually:
   - If you are not using RHEL 8 or CentOS 8, for each interface you use you need its IP address, netmask, gateway, and DNS information.
   - If you're using RHEL 8 or CentOS 8, you only select the interface and are responsible for configuring the networking.

   a. From a terminal window, run the following command:

   ```
   $ sudo /Users/Shared/Verodin/node/node/scripts/vsetnet
   ```

   If you specified a different install location in step 1, modify the path to scripts accordingly.

   b. Specify which interface, from the list, to use for management and press `Return` . For example, `en0` .

   - If networking for the computer changes frequently, we suggest you use **auto**. When you choose **auto**, the platform will select the interface when you run security content.
   - Interfaces that do not include MACs should be available, letting you use VPN interfaces.

c. (Optional) If available and necessary, specify a second interface for test Data.
After the networking is set up, the Actor restarts the platform services.

2. Register your Actor from the command line.

> When an unexpected response is received, a message will be displayed and a `response.txt` file is created.

a. Run `vregister`. For a full list of available arguments, see **vregister arguments explained (https://docs.mandiant.com/home/msv-installing-configuring-the-mac-actor-command-line#arg)**.
   - Linux: If the scripts directory is in the PATH, run the following command:

     ```
     sudo vregister
     ```

   - Linux: If the scripts directory is not in the PATH, run the following command, modifying the patch if you installed to a different directory:

     ```
     $ sudo /opt/apps/verodin/node/node/scripts/vregister
     ```

   - Mac:

     ```
     $ sudo /Users/Shared/Verodin/node/node/scripts/vregister
     ```

     If you specified a different install location, modify the path to scripts accordingly.

b. Enter the IP Address or Hostname of your Director.
c. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actors table
   - *bulk registration token code* in the Bulk Registration Tokens table

d. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
When set to Yes, the certificate is verified during registration and then every time the Actor connects to the Director (HTTPS requests).This prompt only appears for Pull Actors.

> Actors can verify that TLS certs signed by public CAs, but not private CAs.

e. Specify if you want to connect to the Director using a proxy [yes|no].
f. If you said yes to using a proxy, provide the proxy details.

> If you have a Firewall enabled on the Mac, you may be prompted to allow or deny communication to the Actor. This prompt could happen after registration completes or when you try to run your first Action for the Actor. Allow this communication or all Actions run on the Actor errors.

vregister Arguments Explained

- minimum `vregister` command:

  ```
  vregister [planner_ip] [register_code] [{yes,no,None}] [{yes,no,None}] --mgmt-interface [{auto, interface}] --test-interface
  ```

- `vregister` with simple proxy configuration:

  ```
  vregister [planner_ip] [register_code] [{yes}] [{yes,no,None}] --proxy-authtype [{http,ntlm,kerberos}] --proxy-host [PROXY_HOST]
  ```

Positional arguments details:

- `planner_ip`
- `register_code` : This is either the code you received from adding the Actor configuration to the Director or the code for the bulk registration token
- `{yes,no,None}` : Use Proxy Settings? If this is no, any optional proxy arguments included will be ignored
- `{yes,no,None}` : Skip configuration check?
- `--mgmt-interface` : Values include `auto` and *`the interface`*
- `--test-interface` : Values include `auto` and *`the interface`*

Optional arguments (if there's nothing after the argument, the argument describes what should be entered as the value):

- `-h, --help` : show this help message and exit
- `--no-tls-verify` : When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).

  

  NOTE: Actors can verify TLS certs signed by public CAs, but not private CAs.
- `--include-tap-adapters` : When included, you will see and be able to select existing TAP adapters for the management and test interfaces.
- `--proxy-authtype` : Values include `http, ntlm, kerberos`
- `--proxy-user`
- `--proxy-password`
- `--proxy-host`
- `--proxy-port`
- `--proxy-ntlm-configfile`
- `--proxy-kerberos-domain-controller`
- `--proxy-kerberos-realm`
- `--proxy-kerberos-fqdn`