Mandiant

MAC ACTOR INSTALLATION

To support our customers' various environments, we provide the following ways to install a Mac Actor:

- Easy Install
- Interactive install
- Automated install

Easy

If you meet the prerequisites, you can use Bulk Registration Tokens to install and register your Actor.

Prerequisites

- You have configured and deployed the operating system
- Your Actor does not need a proxy for communication
- You do not need to select interfaces

Create a Bulk Registration Token

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Click **Add Bulk Registration Token**.
4. Fill out the form and click **Submit**.
    a. **Name:** This value is used in the name of the Actors. The Actor name has the following format:

    <token_name>-#-<Actor IP address>.

    Actor names can be changed. Names must start and end with an alphanumeric character and be no more than 69 characters. Hyphens and periods are allowed but may not be next to each other. Spaces are not allowed.

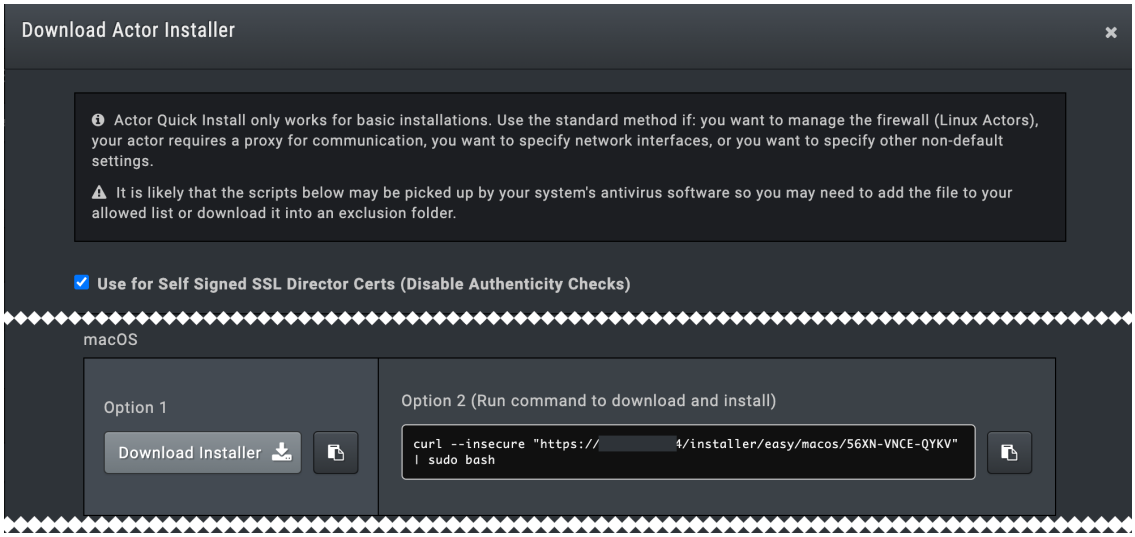
    b. **Security Zone:** The security zone for the Actors.
    c. **Expiration Date:** The date the token is no longer valid.
    d. **Max Uses:** The number of times the token can be used. This value cannot exceed the number of available Actors allowed by your license.
5. The token is created and is listed in the table. The token can be used for the easy install process or for registering Actors after they are installed.

Install and register a Mac Actor

There are several ways to use the bulk registration code to complete installation. The most common use case is included. When this completes, you will have a registered Mac Actor that is configured with Pull Comm mode and Auto Interface enabled.

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Locate the token you want to use in the **Bulk Registration Tokens** table and click **Installer** Installer .
4. Select or clear the **Use for Self Signed SSL Director Certs**.

    Clearing this option means the install does not verify the certificate during registration and subsequently does not verify the cert when the Actor connects to the Director (HTTPS requests).
5. In the **macOS** section, click copy next to the command for Option 2.



Installer window for MacOS Bulk Registration Token

6. Using an account that has root access, SSH to the Mac system.
7. For MacBooks with an M1 processor, enable Rosetta.

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

8. Paste the command to start the install. An example is provided:

   ```
   $ curl --insecure "https://10.10.10.144/installer/easy/macos/36LL-8APQ-1D3B" | sudo bash
   ```

   The Actor installs and registers. When it completes, the Actor is listed in the **Endpoint Actors** table.

Interactive

There are several ways you can add the Actor configuration to the Director:

- Use the Add Endpoint Actors option in the Director UI
- **Create a bulk registration token** for use during registration
- Use the API, discussed in **Adding the Actor Configuration - API** **(https://docs.mandiant.com/home/msv-adding-the-actor-configuration-api)**

Add a Windows, Mac, or Unix Actor as an Endpoint Actor Configuration in the Director

1. Launch the Director.
2. Select **Environment > Actors**.
3. Click **Add Endpoint Actors** and fill out the new Actor form.
   a. **Name:** Label for the Actor.
      Best practice is to include the security zone as part of the name, which makes it easier when assigning Actors to Jobs.
   b. **Description:** Free text description for the Actor
   c. **User Tags:** Select existing user-created tags or add new ones to label this Actor.

      NOTE: User tags are used for running bulk Actions. See **Running Bulk Actions** **(https://docs.mandiant.com/home/msv-running-bulk-actions)** for more information.

d. **Security Zone:** The area of your network where the Actor will live.
   Security zones are added to the Director after the Director is installed (see Adding Security Zones in your Director Install guide if there are no security zones listed).
e. **Comm Mode:** The communications mode by which the Director and Actor communicate. This must be **Pull mode**, which means the Actor initiates communication with the Director.
f. **Proxy Through Actor:** Specifies the Actor to use as a proxy to communicate with the Director.

> **IMPORTANT:** Only Actors that are in Push communication mode can proxy through another Actor. Therefore, Actors installed as endpoint Actors or Protected Theater Actors cannot proxy through another Actor.

   An Actor can be used as an intermediate proxy in cases of network segmentation policies, where an Actor would not otherwise be reachable by the Director.
   For example, given Actor A, which is connected to the Director, and Actor B, which is in a remote network segment, when setting up Actor B, select Actor A in the Proxy Through Actor field.
g. **Location [Local/Cloud]:** The Actor's location; specified as local or within the Cloud (Amazon Web Services or Azure).
h. **Pull Interval:** The time interval (in seconds) between pull attempts between the Actor and the Director.

4. Click **Submit**.
   The Actor is added to the Pending Actors list and a code is generated. This code must be used for registration and is only valid for 15 minutes.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cf4253b2606144059e09e/n/add-actor-config-win.png)

Add Endpoint Actor Form

After the Actor is registered, you can review and update the Actor details and capabilities. For more details, see **Editing an Actor (https://docs.mandiant.com/home/msv-editing-an-actor)**.

Create a Bulk Registration Token

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Click **Add Bulk Registration Token**.
4. Fill out the form and click **Submit**.
   a. **Name:** This value is used in the name of the Actors. The Actor name has the following format:

   `<token_name>-#-<Actor IP address>`.

   > Actor names can be changed. Names must start and end with an alphanumeric character and be no more than 69 characters. Hyphens and periods are allowed but may not be next to each other. Spaces are not allowed.

   b. **Security Zone:** The security zone for the Actors.
   c. **Expiration Date:** The date the token is no longer valid.

d. **Max Uses:** The number of times the token can be used. This value cannot exceed the number of available Actors allowed by your license.

5. The token is created and is listed in the table. The token can be used for the easy install process or for registering Actors after they are installed.

Install the Mac Actor

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

   If you're 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 shows an error.

5. Process the installer by double-clicking on the installer package.

   If you encounter an error in opening the installer, **Command+Click** the installer package and click **Open**.

6. Click **Continue** to begin the installation process.
7. If prompted, select the drive you want to install to and then click **Continue**.
8. Click **Install**. Enter your password to verify that you want to continue with the installation.
   The installer runs. This process could take several minutes, depending upon your system.
9. Click **Close** to exit the installer.

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.

Automated

Mandiant

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`