Mandiant

LINUX ACTOR INSTALLATION

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

- Appliances
  - AMI for AWS
  - OVA (Interactive and Automated)
  - VHD for Azure
  - VHD for Hyper-V
- Software
  - Easy Install
  - Standard install
  - Automated install

AMI

This section provides instructions for setting up the network Actor from an AMI. The overall steps involved are listed as follows:

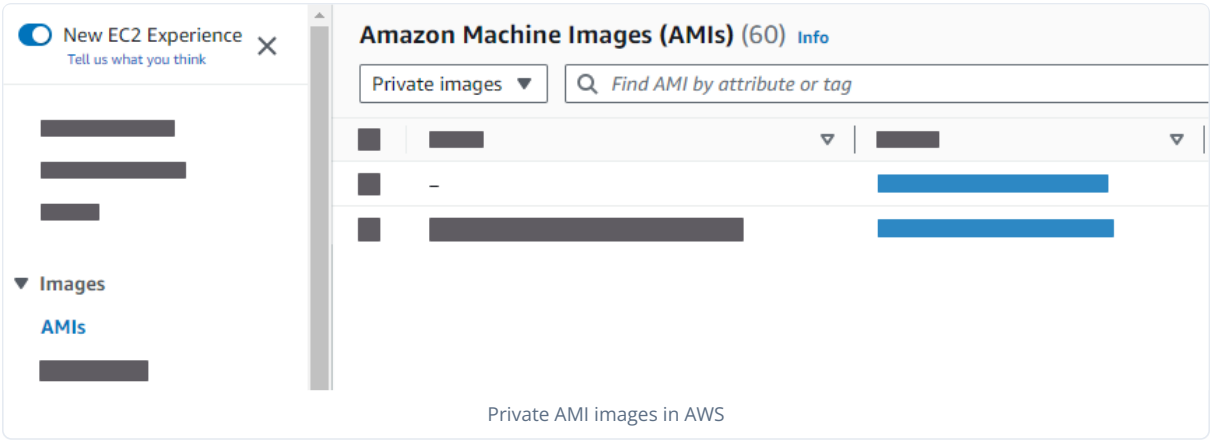
1. **Receive the AMI**
2. **Install the Actor**
3. **Add the Network Actor Configuration to the Director**
4. Optional. **Add a Custom Certificate to the Director**
5. **Configure the Actor's Networking**
6. **Register your Actor using the Director**

Receive the AMI

To make the installation as easy as possible, Security Validation sends you the AMI directly in AWS.

To notify us that you need the AMI:

1. Log into the Customer Portal.
2. Click **Support** **(https://docs.mandiant.com/home/mandiant-support-cases)**.
3. Submit a ticket requesting the AMI, include the following:
   a. AWS Account number
   b. Desired Region
4. When the Security Validation support team receives the ticket, they provide access to the AMI directly in AWS.
5. Once access is granted, the AMI becomes available in your AWS account console in **AMI** > **Private Images**.



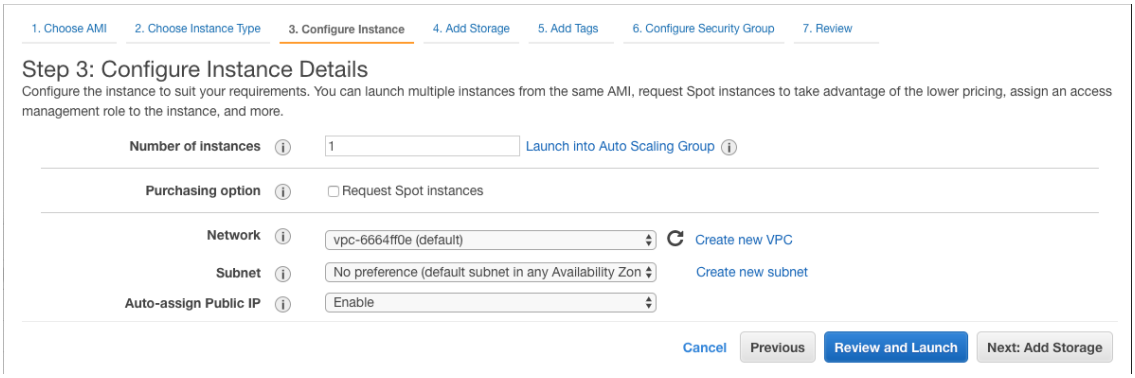
Private AMI images in AWS

Install the Network Actor: AMI

Complete your installation of the Actor on AWS through the Amazon Machine Image (AMI) by using the following procedure.

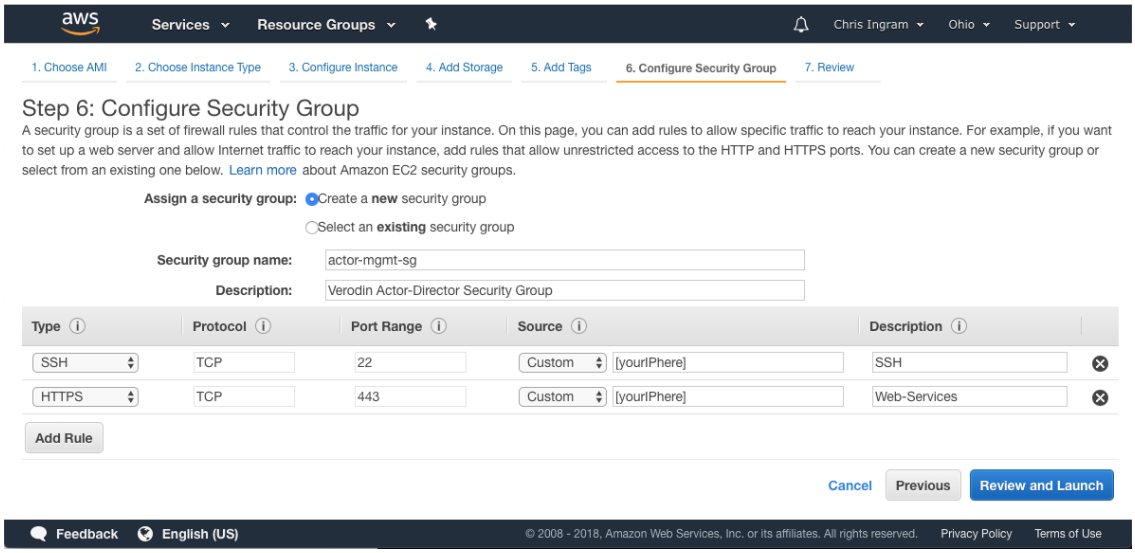
1. In AWS, go to **Images > AMIs > Private Images**.
2. Choose the Security Validation Actor AMI from the list, and click **Next**.
3. Choose an **Instance Type**. See **Network Actor Requirements (https://docs.mandiant.com/home/network-actor-requirements)** for recommendations.
4. Configure instance details, and click **Next: Add Storage**.

> *Do not* set Auto-Assign Public IP to Enable.



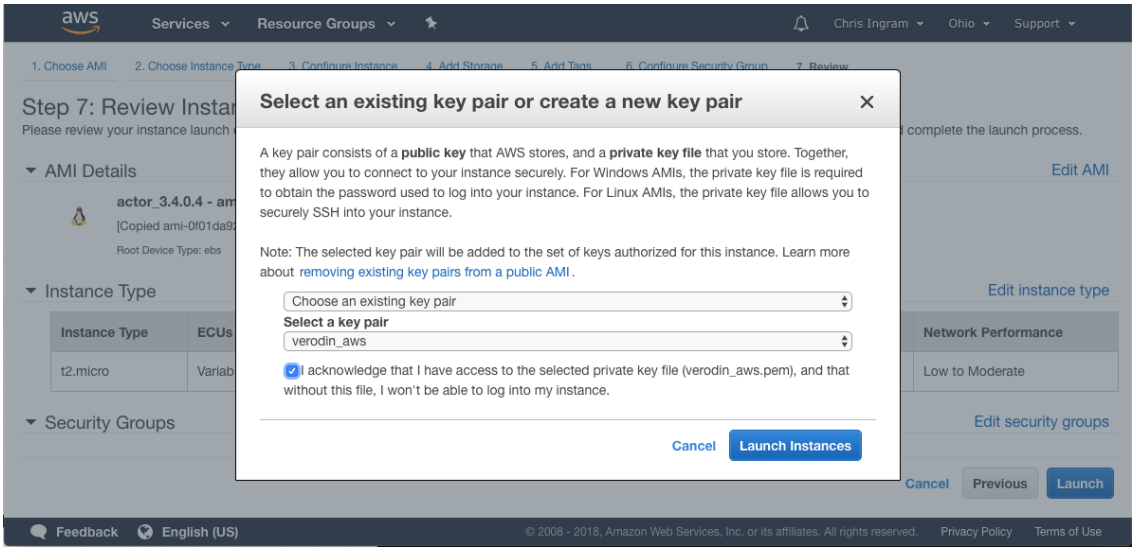
Configure AWS Instance Details

5. Optional: Add storage and click **Next: Add Tags**.
6. Optional: Add tags and click **Next: Configure Security Groups**.
7. Configure a security group that allows Actor and Director communication, as shown in the following image. Click **Review and Launch**.



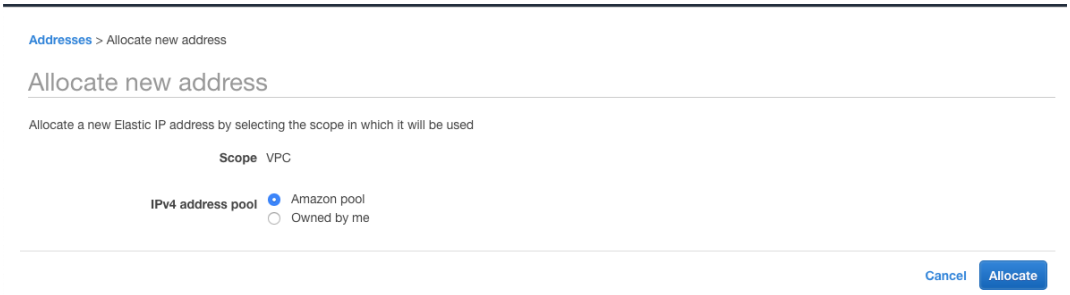
Configure Security Group

8. Review your new instance, and select or create a new key pair.



Select the Key Pair

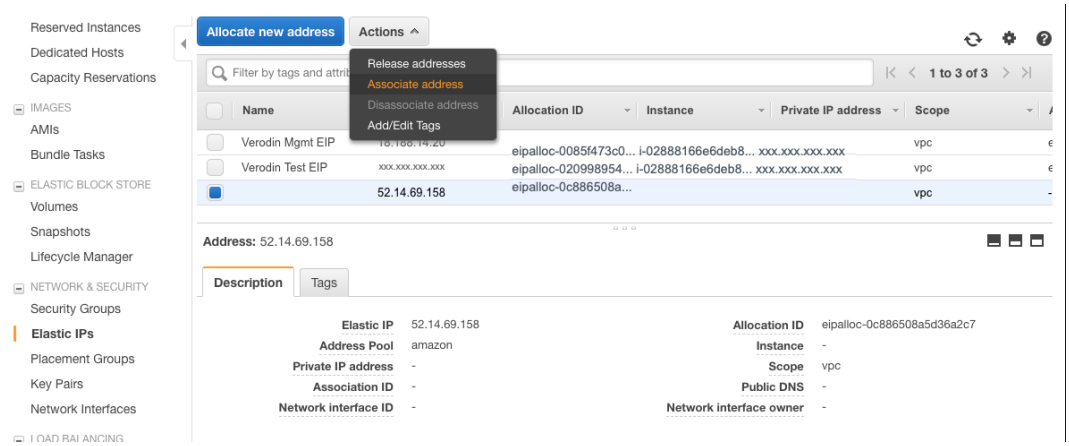
9. Click **Launch Instance**.
10. Allocate a new Elastic IP address to your instance.
    a. Select **Elastic IPs** in the navigation pane.
    b. Click **Allocate new address**.
    c. Select **Amazon pool**.



Allocate Elastic IP Address

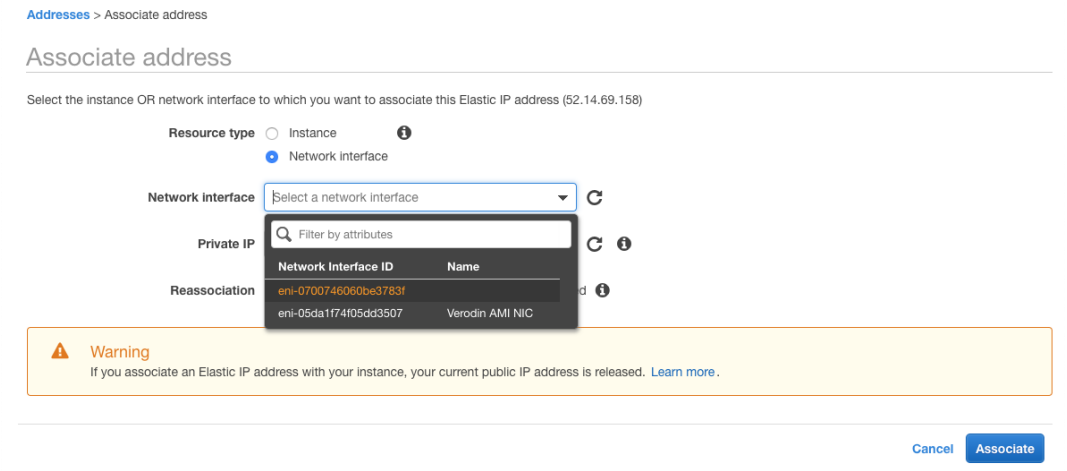
d. Click **Allocate**.
e. Click **Close**.

13. Associate the Elastic IP with the interface.
    a. Select **Actions > Associate address**.



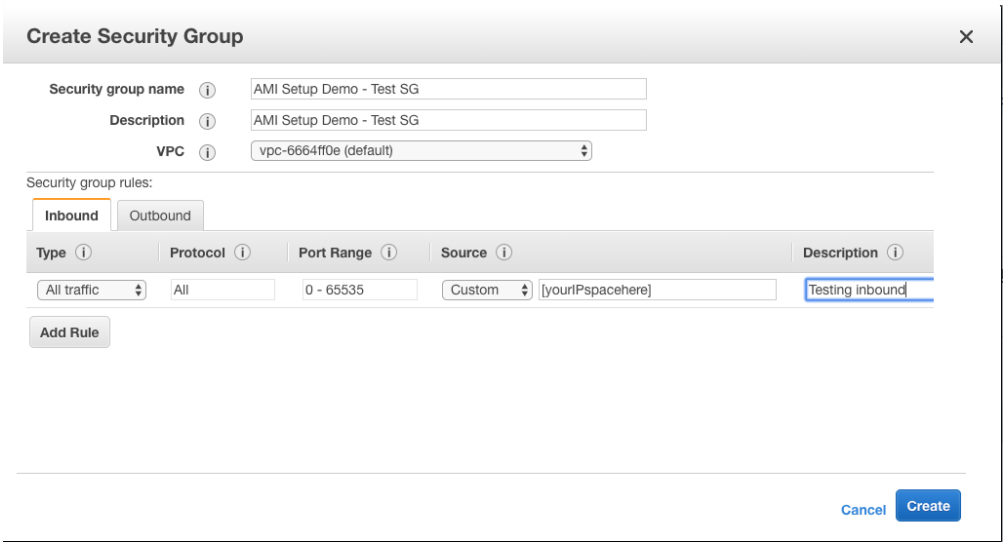
Associate Elastic IP

b. Click **Network interface**, and select the network interface.



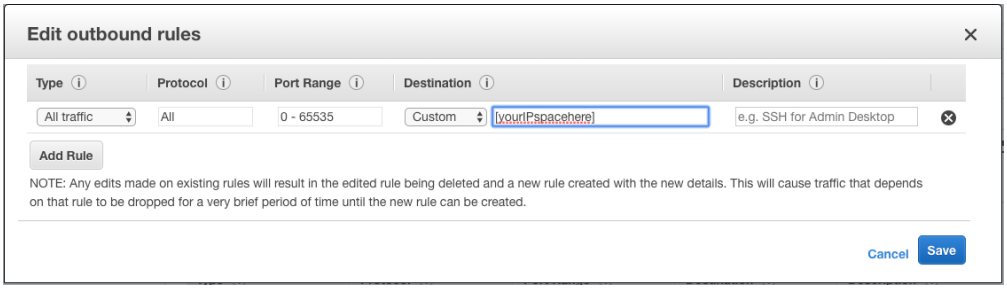
c. Click **Associate**.
d. Enter the private IP address.
e. Click **Associate**.

14. Create a Security Group.
    a. Go to **Network > Security Groups**.
    b. Click **Create Security Group**. Provide the following information.
        - Name
        - Description
        - Select your vpc
        - Configure your Inbound rule as shown.



Configure Inbound Rule - Security Group

        - Configure your Outbound rule as shown.



Configure Outbound Rule - Security Group

Add the Network Actor Configuration to the Director

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

- **Use the Add Network Actors option**
- **Create a bulk registration token**

Adding a Network Actor Configuration using the Director

1. Select **Environment > Actors**.
2. Click **Add Network Actors** and fill out the new Actor form.
   Information about several of the fields is provided below.
   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.

      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.
      i. **Push mode**: Director initiates communication to the Actor
      ii. **Pull mode**: Actor initiates communication with the Director

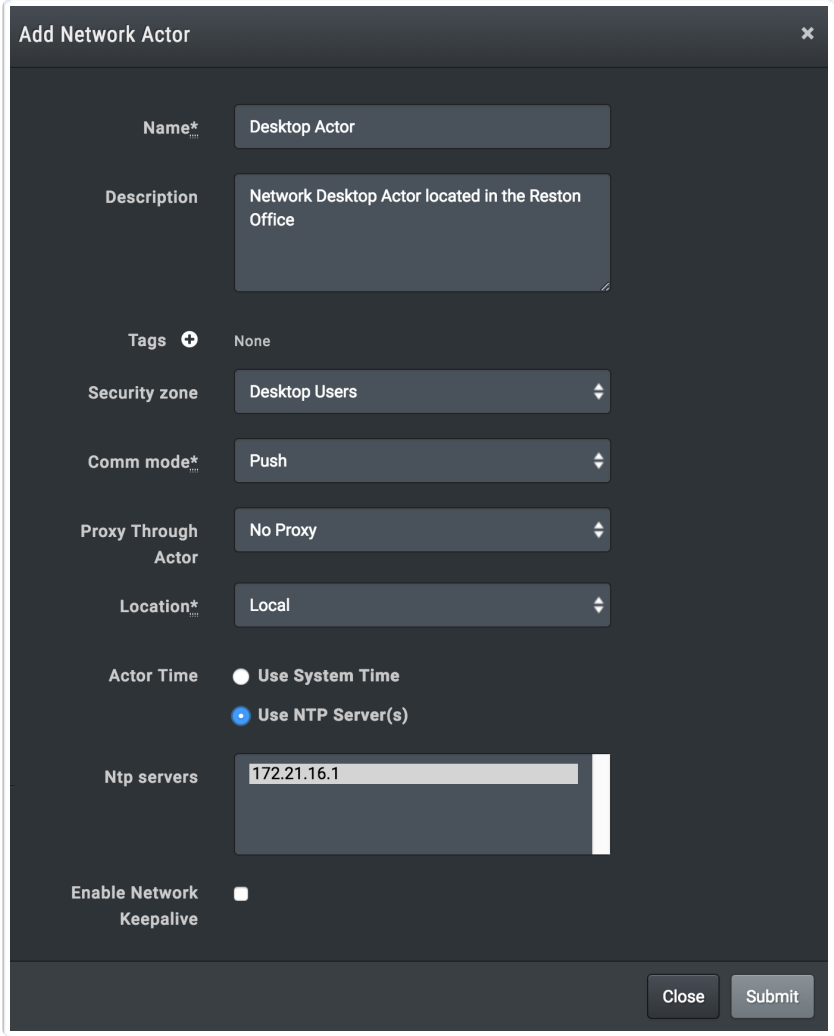
      If the Actor is in Pull mode, you need to run `vregister` to register the Actor to the Director.

   f. **Proxy Through Actor:** Specifies the Actor to use as a proxy to communicate with the Director.

      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. See **Network Actor Requirements (https://docs.mandiant.com/home/msv-network-actor-requirements)** for more information.
   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.
   i. **Actor Time [System/NTP]:** The method used for maintaining the Actor's time. This can be either system time or NTP (see Adding NTP Servers in your Director Install guide if no NTP servers are listed).This must be system time.
   j. **Enable Network Keepalive:** Actors send a periodic (default setting is hourly) ARP request for all Actor interfaces to maintain status in ARP tables.

3. Click **Submit**.
   The Actor is populated in the Pending Actors list and a code is generated. This code must be used for registration within 15 minutes.



Add Network 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.

Add Custom Certificate to the Director

The Security Validation Director and Linux Actors include self-signed certificate. For many organizations, self-signed certificates are not approved. In some instances, a self-signed certificate could cause issues, such as when your Actor is hosted on AWS. The following steps provide instructions on adding the custom certificate to the Director without using the web interface.

1. Create your certificate.
2. Sign into the Director as root.
3. Add your certificate to the following path:

```
/etc/httpd/ssl/apache.dh.crt
```

4. Add your key to the following path:

```
/etc/httpd/ssl/apache.key
```

5. Restart the web server to load the new SSL keys

```
$ sudo systemctl restart httpd
```

Configure Actor Networking

After installing the Actor, you'll need to set up the Actor's networking.

Two network interfaces are required if you want to test Network Controls - one for management interaction with the Director, which should be a static IP, and one for job execution. A third interface for monitoring is supported.

When setting up your interfaces, you can use DHCP. Do not use DHCP to set up multiple interfaces on the same subnet. Doing so may cause communication issues and prevent Actions from running properly. If you have two interfaces on one subnet, each must have its own static IP. See **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) for more information.

Manual changes to network configuration files can be overwritten during updates and in-platform configuration changes.

1. If necessary, log into your Actor.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

```
sudo /opt/apps/verodin/node/node/scripts/vsetnet
```

or

```
sudo vsetnet
```

Remember to use a static IP address.

This command walks you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and are responsible for configuring the networking. For more information about `vsetnet`, see **Configuring an Actor's Network Settings (https://docs.mandiant.com/home/msv-network-actor-requirements#using)**.

Network Actors may be misconfigured if you do not run `vsetnet` before registering the Actor. If the registration process identifies a misconfigured Actor, it will stop and prompt you to run `vsetnet`.

a. When available, we recommend using **`eth0`** for the (management) interface
b. If you're only interested in testing endpoint controls, one interface and not two is required

Network installation prompts

3. After completing configuration, confirm that the IP settings have been changed.

Remember, if you're using an RHEL 8-9 or CentOS 9 system, no network settings are changed based on running `vsetnet`. You must configure the networking on your own.

```
ifconfig
```

Update a Linux Actor's Information in the Director

After updating the Actor's networking, we recommend verifying the changes and then updating the Actor's information in the Director.

1. Log into the Actor from the command line.
2. Confirm that the IP settings have been changed.

```
ifconfig
```

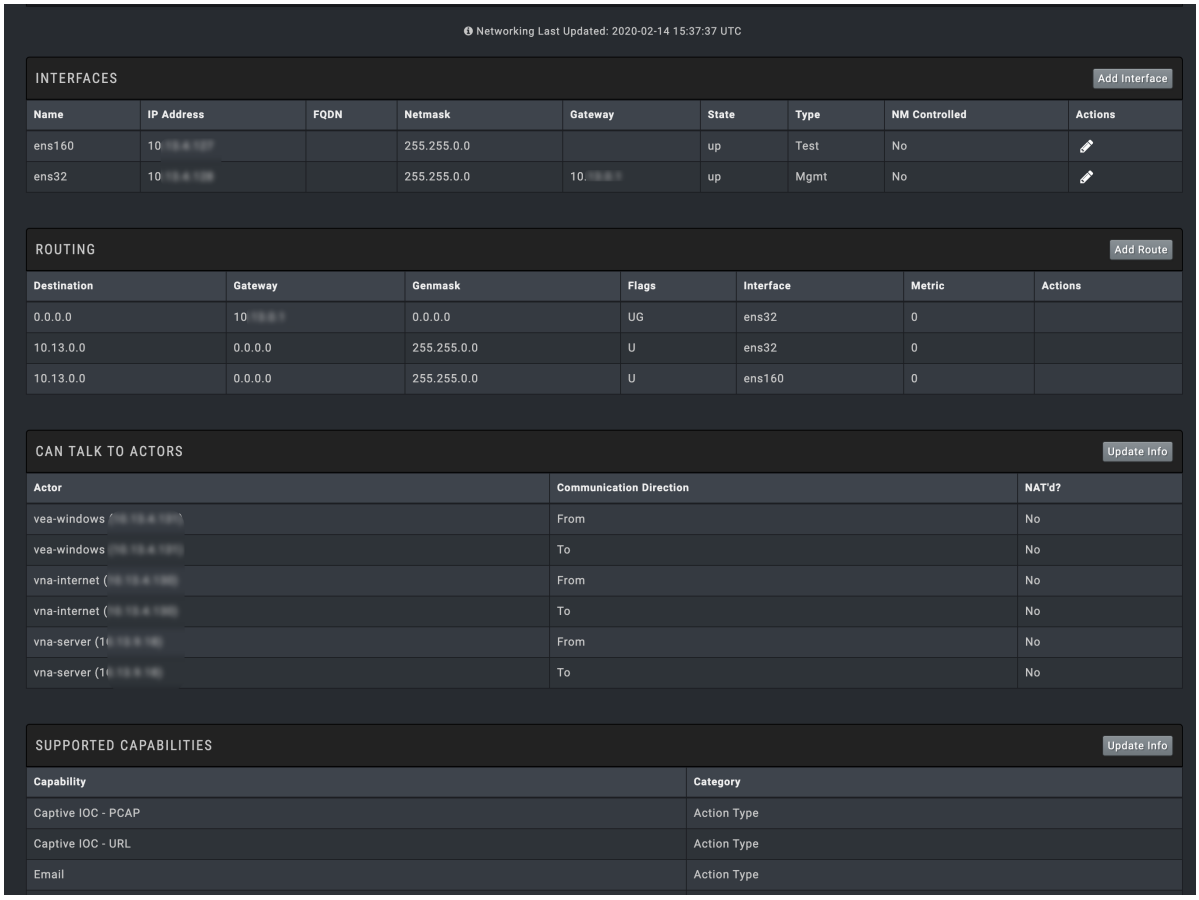
3. Launch the Director.
4. Select **Environment > Actors**.
5. Locate the Actor you updated, open its Action menu, and click **Edit**.
6. Click **Refresh Actor Info**.

Within the Director, you can review and refresh the Actor's network settings. Depending on the Actor, you may also be able to directly update information. This information includes

- Interfaces
- Routing
- Communication with Actors
- Supported Capabilities

> The configuration changes you can make to the Actor's Networking in the Director depend on the form-factor used to install the Actor and if the Validation Platform is managing the Network information.

If you change an Actor's network information using the Director, we recommend updating its **Can Talk to Actors** and **Supported Capabilities** settings.



Actor Networking configuration and capabilities

If your network changes after installing your Actor or you want to change how the Actor's networking is managed, you can update the Actor's networking using the vsetnet command. For full details on how to run the vsetnet command, see the Actor installation documentation for your platform.

Update a Linux Actor's Network Settings

If your network changes after installing your Actor, you can update the Actor's networking using the `vsetnet` command. If you're managing multiple interfaces on the same subnet for a Network Actor, see **Using Multiple Interfaces on the same Subnet (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info)** before running `vsetnet`.

When you run vsetnet on an Actor installed using the OVA appliance, the first decision you make is whether you will manually manage the Actor's network configuration files or have the Validation Platform manage it. Items to consider when making this decision include:

- Allowing the Validation Platform to manage the network configuration improves network reliability and stability.
- Actors that meet the requirements but were installed before version 4.0.1.0 came out will have this setting disabled.
- This setting can be modified by rerunning `vsetnet` for the Actor.
- Enabling this setting overwrites any changes that you've made to the Actor's network configuration files.

For release 4.14.0.2 onward, if you specify Verodin Control during `vsetnet`, `vsetnet` configures the system as follows:

- If DHCP is selected for all interfaces configured, `cloud-init` remains in a running state.
- If Static IPs are used for one interface or more, `cloud-init` is disabled.

If Verodin Control is declined during `vsetnet`, you are responsible for configuring or disabling `cloud-init`.

If another configuration is required, you can make changes as needed after you run `vsetnet`. However, re-running vsetnet can reset settings. To enable or disable `cloud-init`, the `vsetnet` code adds or removes the file: `/etc/cloud/cloud-init.disabled`. If the automatic configuration doesn't suit your needs, you can manually add or remove the file, as needed.

Actors on RHEL/CentOS 7.x systems cannot be completely managed by the Validation Platform. However, you can use the platform to update the network configuration files for those Actors. The Validation Platform cannot manage or update the network configuration files for any endpoint Actor or Actors on RHEL 8 - 9, CentOS 9, and Ubuntu systems.

1. Log into the Actor from the command line.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

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

   or

   ```
   sudo vsetnet
   ```

   This will walk you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you'll need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and you're responsible for configuring the networking.

> **IMPORTANT:** If you're managing multiple interfaces on the same subnet, see **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) before running `vsetnet`. If you're rerunning `vsetnet` and are prompted "Will Verodin control the network configuration files?", saying **yes** means that the platform will start managing the networking and will overwrite any changes you previously made to the network configuration files.

3. After completing configuration, confirm that the IP settings have been changed.

```
ifconfig
```

4. Launch the Director.
5. Select **Environment > Actors**.
6. Locate the Actor that you want to configure, open its Action menu, and click **Edit**.
7. Click **Refresh Actor Info**.

Register the Network Actor to the Director

There are two ways to register your Network Actors to the Director:

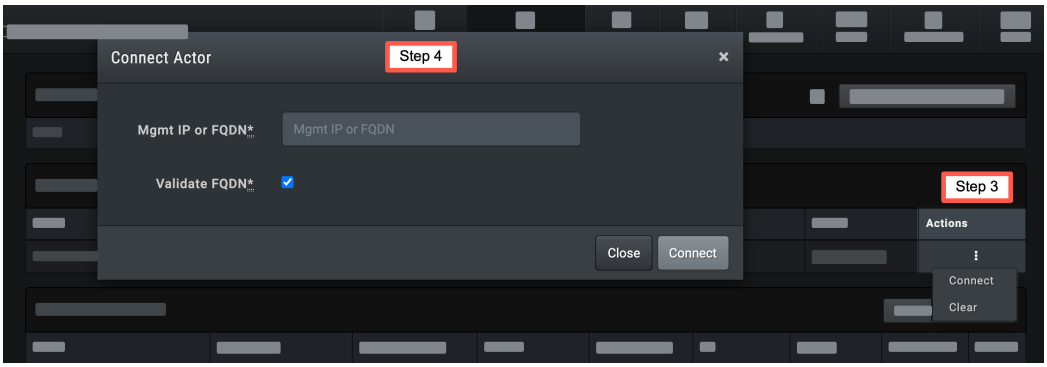
- **Register a Push Mode Actor**
- **Register a Pull Mode Actor**

Register a Push Mode Actor to the Director

Follow one of the sets of steps, depending on how you're registering your Actor:

Pending Actor

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu and Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.
   - The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   - Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.
   - **Description:** Short description of the Actor
   - **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
   - **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
   - Optional. Select **Enable Network Keepalive.**
5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.

Register a Pull Mode Actor by using the command line

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

   If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.
3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table
5. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
   When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).This prompt only appears for Pull Actors.

   Actors can verify TLS certs signed by public CAs, but not private CAs.
6. If desired, add a proxy.
   a. Enter **yes**.
   b. Enter the *Proxy IP* and *Proxy Port*.
   c. If there is an account associated with the proxy, enter *the account info*.
   The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

OVA (Interactive)

The installation of the Network OVA Actor can be completed using the Director and wizards and scripts that walk you through the install:

1. **Add the Network Actor Configuration to the Director**
2. **Install the Actor**
3. **Configure the Actor's Networking**
4. **Register your Actor using the Director**

Add the Network Actor Configuration to the Director

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

   If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.
3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table
5. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
   When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).This prompt only appears for Pull Actors.

   Actors can verify TLS certs signed by public CAs, but not private CAs.
6. If desired, add a proxy.

a. Enter **yes**.
b. Enter the *Proxy IP* and *Proxy Port*.
c. If there is an account associated with the proxy, enter *the account info*.
The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

Install the Actor

1. Download the appropriate Actor file.
2. Import the virtual machine into the existing virtual infrastructure and boot it. This launches the Network Actor install wizard.
3. After the wizard completes, a login prompt is displayed. Enter the default operating system username and password noted in **Validation Platform Credentials** **(https://docs.mandiant.com/home/validation-platform-credentials)**.

Configure the Actor's Networking

After installing the Actor, you'll need to set up the Actor's networking.

Two network interfaces are required if you want to test Network Controls - one for management interaction with the Director, which should be a static IP, and one for job execution. A third interface for monitoring is supported.

When setting up your interfaces, you can use DHCP. Do not use DHCP to set up multiple interfaces on the same subnet. Doing so may cause communication issues and prevent Actions from running properly. If you have two interfaces on one subnet, each must have its own static IP. See **Using Multiple Interfaces on the same Subnet** **(https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info)** for more information.

> Manual changes to network configuration files can be overwritten during updates and in-platform configuration changes.

1. If necessary, log into your Actor.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

   ```
   sudo /opt/apps/verodin/node/node/scripts/vsetnet
   ```

   or

   ```
   sudo vsetnet
   ```

   > Remember to use a static IP address.

   This command walks you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and are responsible for configuring the networking. For more information about `vsetnet`, see **Configuring an Actor's Network Settings (https://docs.mandiant.com/home/msv-network-actor-requirements#using)**.

   > Network Actors may be misconfigured if you do not run `vsetnet` before registering the Actor. If the registration process identifies a misconfigured Actor, it will stop and prompt you to run `vsetnet`.

   a. When available, we recommend using **`eth0`** for the (management) interface
   b. If you're only interested in testing endpoint controls, one interface and not two is required

Network installation prompts

3. After completing configuration, confirm that the IP settings have been changed.

> Remember, if you're using an RHEL 8-9 or CentOS 9 system, no network settings are changed based on running `vsetnet`. You must configure the networking on your own.

```
ifconfig
```

Update a Linux Actor's Information in the Director

After updating the Actor's networking, we recommend verifying the changes and then updating the Actor's information in the Director.

1. Log into the Actor from the command line.
2. Confirm that the IP settings have been changed.

   ```
   ifconfig
   ```

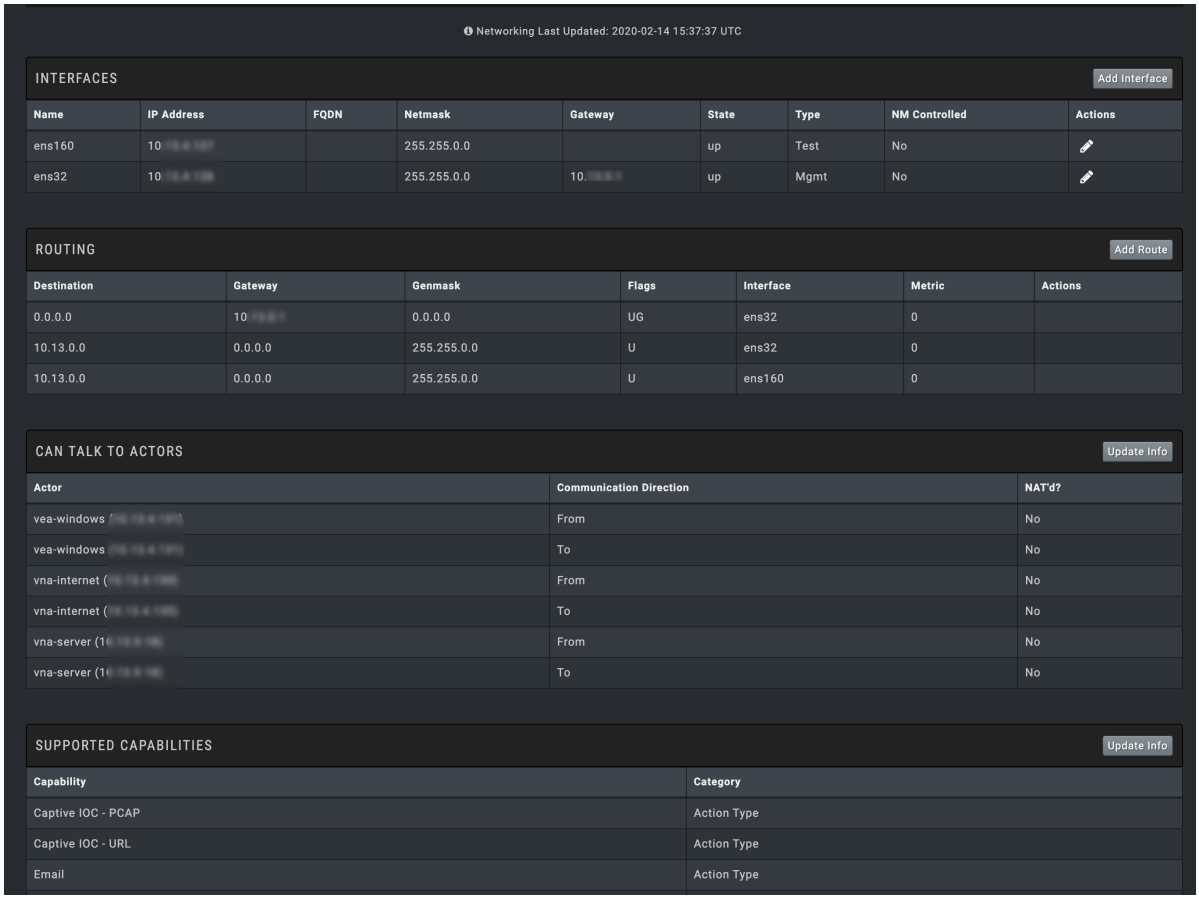
3. Launch the Director.
4. Select **Environment > Actors**.
5. Locate the Actor you updated, open its Action menu, and click **Edit**.
6. Click **Refresh Actor Info**.

Within the Director, you can review and refresh the Actor's network settings. Depending on the Actor, you may also be able to directly update information. This information includes

- Interfaces
- Routing
- Communication with Actors
- Supported Capabilities

> The configuration changes you can make to the Actor's Networking in the Director depend on the form-factor used to install the Actor and if the Validation Platform is managing the Network information.

If you change an Actor's network information using the Director, we recommend updating its **Can Talk to Actors** and **Supported Capabilities** settings.



Actor Networking configuration and capabilities

If your network changes after installing your Actor or you want to change how the Actor's networking is managed, you can update the Actor's networking using the vsetnet command. For full details on how to run the vsetnet command, see the Actor installation documentation for your platform.

Update a Linux Actor's Network Settings

If your network changes after installing your Actor, you can update the Actor's networking using the `vsetnet` command. If you're managing multiple interfaces on the same subnet for a Network Actor, see **Using Multiple Interfaces on the same Subnet (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info)** before running `vsetnet`.

When you run vsetnet on an Actor installed using the OVA appliance, the first decision you make is whether you will manually manage the Actor's network configuration files or have the Validation Platform manage it. Items to consider when making this decision include:

- Allowing the Validation Platform to manage the network configuration improves network reliability and stability.
- Actors that meet the requirements but were installed before version 4.0.1.0 came out will have this setting disabled.
- This setting can be modified by rerunning `vsetnet` for the Actor.
- Enabling this setting overwrites any changes that you've made to the Actor's network configuration files.

For release 4.14.0.2 onward, if you specify Verodin Control during `vsetnet`, `vsetnet` configures the system as follows:

- If DHCP is selected for all interfaces configured, `cloud-init` remains in a running state.
- If Static IPs are used for one interface or more, `cloud-init` is disabled.

If Verodin Control is declined during `vsetnet`, you are responsible for configuring or disabling `cloud-init`.

If another configuration is required, you can make changes as needed after you run `vsetnet`. However, re-running vsetnet can reset settings. To enable or disable `cloud-init`, the `vsetnet` code adds or removes the file: `/etc/cloud/cloud-init.disabled`. If the automatic configuration doesn't suit your needs, you can manually add or remove the file, as needed.

Actors on RHEL/CentOS 7.x systems cannot be completely managed by the Validation Platform. However, you can use the platform to update the network configuration files for those Actors. The Validation Platform cannot manage or update the network configuration files for any endpoint Actor or Actors on RHEL 8 - 9, CentOS 9, and Ubuntu systems.

1. Log into the Actor from the command line.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

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

   or

   ```
   sudo vsetnet
   ```

   This will walk you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you'll need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and you're responsible for configuring the networking.

   IMPORTANT: If you're managing multiple interfaces on the same subnet, see **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) before running `vsetnet`. If you're rerunning `vsetnet` and are prompted "Will Verodin control the network configuration files?", saying **yes** means that the platform will start managing the networking and will overwrite any changes you previously made to the network configuration files.
3. After completing configuration, confirm that the IP settings have been changed.

   ```
   ifconfig
   ```
4. Launch the Director.
5. Select **Environment > Actors**.
6. Locate the Actor that you want to configure, open its Action menu, and click **Edit**.
7. Click **Refresh Actor Info**.

Register your Actor using the Director

There are two ways to register your Network Actors to the Director:

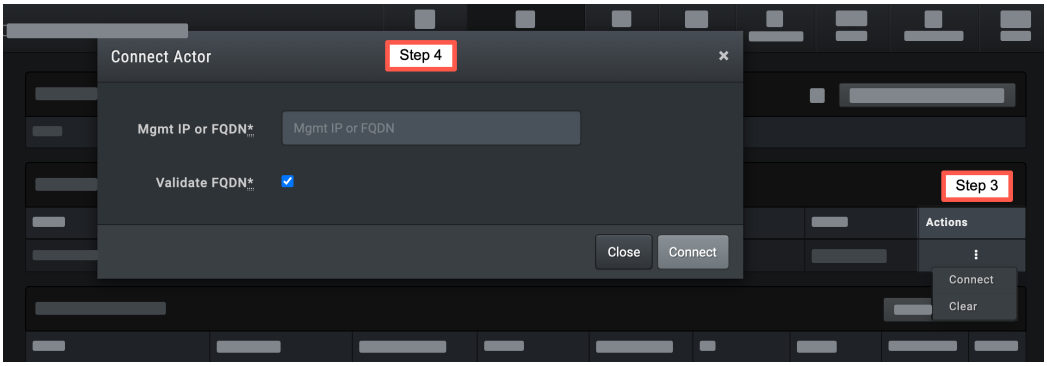
- **Register a Push Mode Actor**
- **Register a Pull Mode Actor**

Register a Push Mode Actor to the Director

Follow one of the sets of steps, depending on how you're registering your Actor:

Pending Actor

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu and Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.
   - The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   - Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.
   - **Description:** Short description of the Actor
   - **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
   - **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
   - Optional. Select **Enable Network Keepalive.**
5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.

Register a Pull Mode Actor by using the command line

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.

3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table
5. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
   When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).This prompt only appears for Pull Actors.

   Actors can verify TLS certs signed by public CAs, but not private CAs.
6. If desired, add a proxy.
   a. Enter **yes**.
   b. Enter the *Proxy IP* and *Proxy Port*.
   c. If there is an account associated with the proxy, enter *the account info*.
   The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

OVA (Automated)

Installing the Network OVA Actor can be partially automated. Follow these steps:

1. **Add the Actor Configuration - API**
2. **Install the Actor**

3. **Configure Networking using a JSON File**
4. **Register your Network OVA Actor - Automated**

Add the Actor Configuration - API

You can either add the **Actor Configuration** or **Create a Bulk Registration token**. If you aren't comfortable using the platform API, you can **Adding the Network Actor Configuration to Director (https://docs.mandiant.com/home/msv-adding-the-network-actor-configuration-to-director)** **Registering your Network Actor using the Director (https://docs.mandiant.com/home/msv-registering-your-actor-using-the-director)** or **Adding the Endpoint Actor Configuration to the Director (https://docs.mandiant.com/home/msv-adding-the-endpoint-actor-configuration-to-the-director)** instead.

> **NOTE:** If you use the bulk registration token, your Actor will use Pull communication. You can edit Network Actors after the Actor is registered if you want it in Push.

To Use the Platform API to add the Actor Configuration

Create the Actor Configuration in the Director by posting to the Director API.

1. Create a JSON file, **nodes.json** (a sample JSON is shown below).

```
network_request = { "node" : { "name": "test-network",
"desc": "test network",
"security_zone_id": 1,
"location": "Local",
"node_type": "network"
"comm_mode": "Pull",
"pull_interval": "30"},
"proxy_node_id": "4"
}
```

   - `node_type` options are `network` and `endpoint`.
   - When `node_type` is `endpoint`, `comm_mod` e must be `Pull`.
   - `comm_mode` options are `Pull` and `Push`.

2. Post **nodes.json** to the Director.

```
$ https://director_ip/nodes.json
```

   Once it is posted, it will respond with the registration code, which expires in 15 minutes.

To Create Bulk Registration Tokens using the API

Create the Bulk Registration Token by posting to the Director API.

1. Create a JSON file, **save_bulk_token.json** (a sample JSON is shown below).

```
{
"bulk_token": {
"name": "test",
"security_zone_id": 3,
"expiration_date": "2020-12-30",
"max_uses": "2"
}
}
```

2. Post **save_bulk_token.json** to the Director.

```
$ https://director_ip/save_bulk_token.json
```

Once it is posted, it will respond with the bulk registration token code, which is valid through the expiration date.

Install the Actor

1. Download the appropriate Actor file.
2. Import the virtual machine into the existing virtual infrastructure and boot it. This launches the Network Actor install wizard.
3. After the wizard completes, a login prompt is displayed. Enter the default operating system username and password noted in **Validation Platform Credentials** (https://docs.mandiant.com/home/validation-platform-credentials).

Configure Networking using a JSON File

After installing the Actor, you need to setup the Actor's Networking.

Two network interfaces are required if you want to test Network Controls - one for management interaction with the Director, which should be a static IP, and one for job execution. A third interface for monitoring is supported.

- When setting up your interfaces, you have the option to use DHCP. Do not use DHCP to setup multiple interfaces on the same subnet. Doing so may cause communication issues and prevent Actions from running properly. If you have two interfaces on one subnet, each must have its own static IP. See **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) for more information.
- Manual changes to network configuration files can be overwritten during updates and in-platform configuration changes.
- This process is only valid for Actors using RHEL 7.x or CentOS 7.x (both OVA and installable software formats). In addition to the OS requirements, it should only be used if you are managing the networking. For RHEL 7.x or CentOS 7.x, if you want the Validation Platform to manage the networking, you must **run the vsetnet command** (https://docs.mandiant.com/home/msv-linux-actor-installation#standard).
- This process should only be used if you are managing the networking. If you want Validation Platform to manage the networking, you must **run the vsetnet command** (https://docs.mandiant.com/home/msv-linux-actor-installation#standard).

1. Create a JSON file, **actor-config.json**, that contains the configurations for your interfaces (management, test, and if using, monitor).

```
{
"management" :
{ "name" : "eth0", "dhcp" : "false", "ip_address" : "172.27.73.6", "netmask" : "255.255.252.0", "gateway" :
"172.27.72.1", "dns" : "172.27.72.1", "rewrite" : "true" }
,
"test" :
{ "name" : "eth1", "dhcp" : "true", "rewrite" : "true" }
}
```

   - The configuration can be setup with static information, as shown in the Management configuration.
   - The configuration can be setup to use DHCP, as shown in the Test configuration.

- You can turn the rewrite option on or off.

2. Use the json file to automatically set the configuration.

```
$ sudo vsetnet -c actor-config.json
```

> **NOTE:** `vsetnet` can be run at anytime; if you run it after the Actor has been registered, remember to go into the Director and refresh the Actor's network info

3. After completing configuration, confirm the IP settings have been changed.

```
ifconfig
```

Register your Network OVA Actor - Automated

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

> If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.

3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table
5. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
   When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).This prompt only appears for Pull Actors.

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

6. If desired, add a proxy.
   a. Enter **yes**.
   b. Enter the *Proxy IP* and *Proxy Port*.
   c. If there is an account associated with the proxy, enter *the account info*.
   The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

VHD for Azure

This section contains information for the installation of an Actor from a VHD file on Azure. The overall steps involved are listed as follows:

1. **Install on Azure**
2. **Set up Networking**
3. **Add the Network Actor Configuration to the Director**
4. **Register your Actor using the Director**

Install the Actor: Azure

Installing the Actor VHD on Azure is a multi-step process:

1. Convert the VHD from a Dynamic to Static Disk
2. Upload and Deploy the VHD to your Azure instance
3. Configure the Actor

Prerequisites

- Your Director must be using a Public IP.
- You must create a Public IP to use with your the Actor or configure a private address in Azure that is routable to the Director.
- If deploying an Actor from a Linux image that was not a Mandiant MSV generated VHD:
  - Ensure the `LinuxDiagnostic` is disabled.
  - The `waagent` must also be disabled, and treat the deployment as any other Marketplace image that doesn't require `waagent`.
- Conversion of VHDs requires a Windows 10 desktop and an account with administrator permissions to install and run:
  - Hyper-V Management Tools
  - Hyper-V Powershell Modules
  - Hyper-V Services
  - Rights to access to the Azure Subscription Web UI or install AZ.Compute Powershell module

Convert the VHD from Dynamic to a Static disk

The Security Validation team provides VHD files for the installation of the Director and the Actor. To upload this to Azure, you must first convert it to Dynamic to Static disks.

Convert your VHD from Dynamic to Static Disks

1. Download the VHD image from the Mandiant Documentation Portal.
2. Extract the archive. It should extract a VHD file.
3. Run one of the following commands, depending on if you are installing a Director or Actor (*VERSION* corresponds to the version of the file that you downloaded):

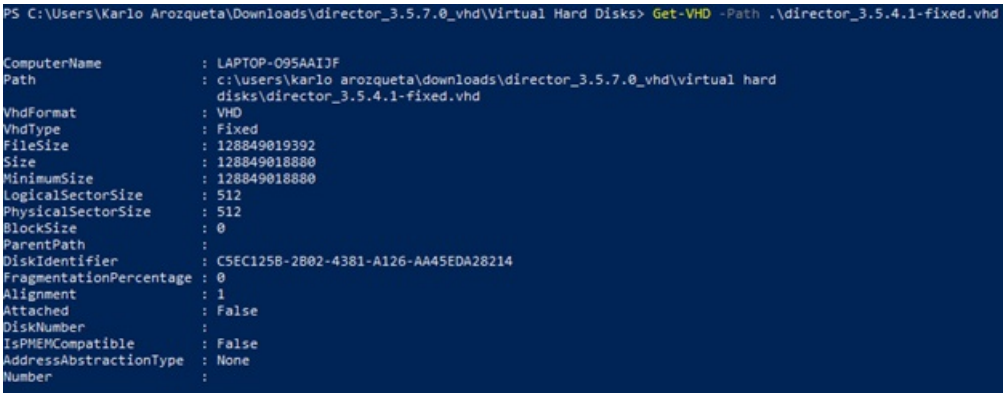
```
Convert-VHD -Path .\director_VERSION.vhd -DestinationPath .\director_VERSION-fixed.vhd -VHDType Fixed
```

```
Convert-VHD -Path .\actor_VERSION.vhd -DestinationPath .\actor_VERSION-fixed.vhd -VHDType Fixed
```

4. You can verify the conversion was successful by running one of the following commands:

```
Get-VHD -Path .\director_VERSION-fixed.vhd
```

```
Get-VHD -Path .\actor_VERSION-fixed.vhd
```



Verify successful conversion

If the conversion was successful, you can upload the VHD to Azure.

Troubleshooting Conversion issues

Some errors you might see when you try the conversion include:

```
Convert-VHD : You do not have the required permission to complete this task. Contact the administrator of the authorization policy
for the computer
```

- This error means you are running PowerShell under the User context. Re-launch as an administrator.

```
Convert-VHD : The term 'Convert-VHD' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
```

- This error indicates that certain Windows features must be enabled for the command to process correctly. Proceed to the next steps to install the required services.

If you receive either of these errors, you need specific Hyper-V PowerShell tools to manage the Hyper-V. These can be installed by using PowerShell or through the GUI.

Add the Hyper-V PowerShell using PowerShell

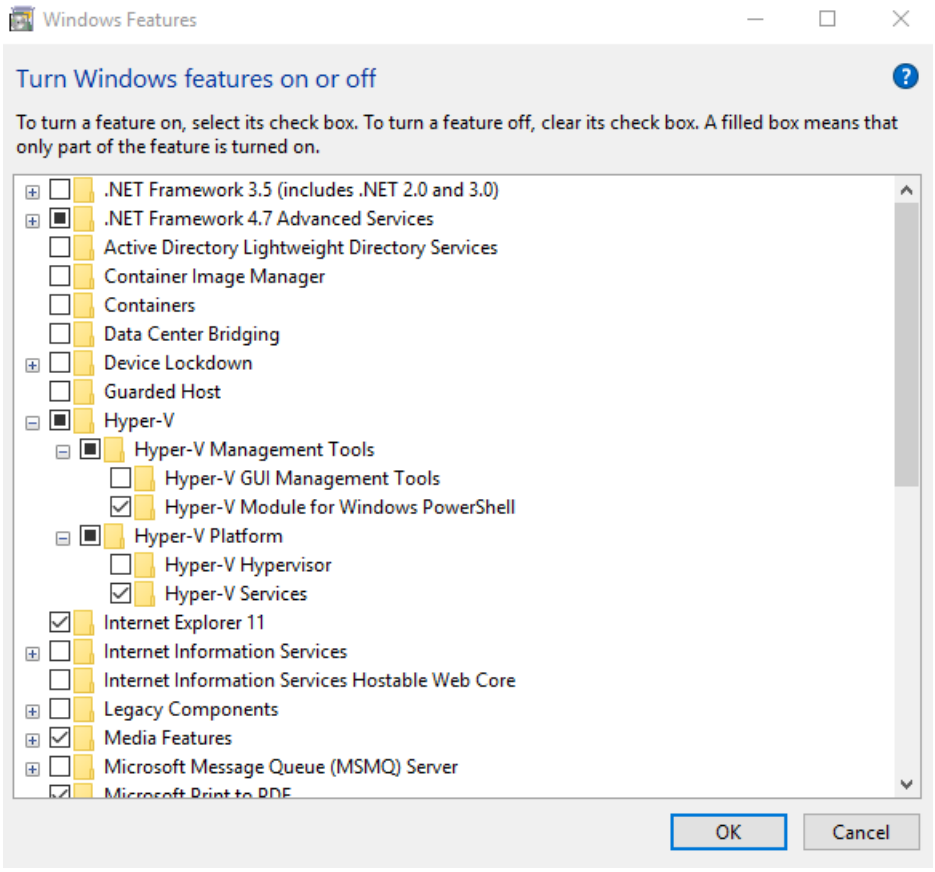
> This procedure requires an internet connection.

While running PowerShell as an administrator, run the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
```

Add the Hyper-V PowerShell using the web interface

1. Open the Windows Control Panel.
   Select **Programs** (or **Programs and features**, based on your version of Windows).
   Select **Turn windows features on or off**.
2. Scroll down to Hyper-V and expand the options. Select the following Options:
   - Under **Hyper-V Management tools**, check the box for **Hyper-V Module for Windows PowerShell**.
   - Under **To add the Hyper-V PowerShell using PowerShell** , check the box for **Hyper-V Services**.



Hyper-V Windows Features

Sources

- https://superuser.com/questions/1307441/powershell-resize-vhd-is-not-recognized-as-the-name-of-a-cmdlet
- https://social.technet.microsoft.com/Forums/windowsserver/en-US/cdd725d6-7f7b-4022-a19e-

f7d242ba514b/convert-dynamic-to-fixed-size-vhd?forum=winserverhyperv
- https://www.altaro.com/hyper-v/gathering-vhd-info-get-vhd-powershell/

Upload and Deploy the VHD to Azure

After you convert the Director or Actor VHD from Dynamic to Static disks, you can upload it to Azure. This process can be done using the GUI or from the command line. This process requires the following steps:

- Install the PowerShell cmd-let module
- Upload the VHD
- Convert the page blob to a managed disk

Install the PowerShell cmd-let module

1. Launch Windows PowerShell as an administrator.

   If you can only launch as a user, you can append `-Scope CurrentUser` to the commands in step 2 to install as a user.

2. Use the following command to install the PowerShell cmd-let module:

```
Install-Module -Name Az.Compute -Force
```

Upload the VHD from the GUI

Reference the following article: **https://aidanfinn.com/?p=20441**.

If you prefer a user interface, install Azure Storage Explorer. This interface allows you to drag-and-drop uploads and downloads to Azure storage containers.

Upload the VHD using the Command line

1. Run the following command to log in in to your Azure account:

```
Login-AzAccount
```

   This step launches a web browser and prompts you to log in to Azure.

2. In Azure, verify you have the following prerequisites set up:
   - A resource group created
   - A storage blob
   - A container in that blob to upload to

3. Upload the VHD by running the following command:

```
Add-AzVhd -ResourceGroupName 'myResourceGroup' -Destination 'https://[myStorageAccount].blob.core.windows.net/[container]/[name.vhd]' -LocalFilePath '[path.vhd]'
```

   Ensure the `--Blob-Type` is `PageBlob`.

   This step scans the static VHD and determines the free space (zeros) on the disk (expanded blank space). This step then uploads the VHD as a page storage blob. The upload size should be equivalent to the pre-converted disk size (dynamic to static), which as of March 2020, is approximately 11GB. Once uploaded, you must convert the page storage blob to a managed disk (next steps), which requires the full 160GB of the expanded disk.

4. If necessary, log back into the Azure instance using the following command:

```
Login-AzAccount
```

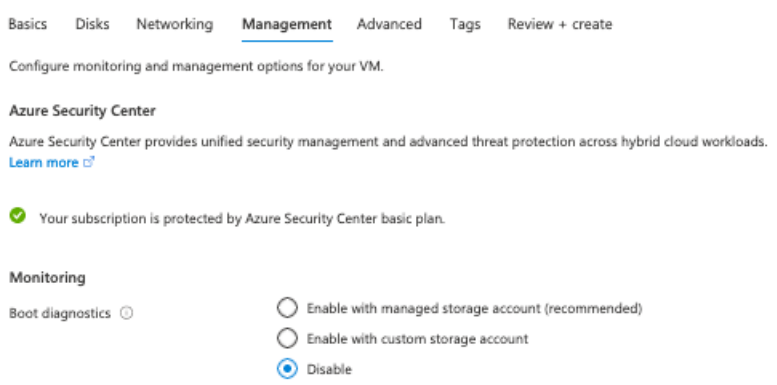
Convert the page storage blob to a managed disk

A sample of the script is provided as follows. You can also access the script from **https://docs.microsoft.com/en-us/azure/virtual-machines/scripts/virtual-machines-windows-powershell-sample-create-managed-disk-from-vhd**.

```
#Provide the subscription Id where Managed Disks will be created
$subscriptionId = 'yourSubscriptionId'

#Provide the name of your resource group where Managed Disks will be created.
$resourceGroupName ='yourResourceGroupName'

#Provide the name of the Managed Disk you are creating
$diskName = 'yourDiskName'

#Provide the size of the disks in GB. It should be greater than the VHD file size. (160GB)
$diskSize = '160'

#Provide the storage type for Managed Disk. Premium_LRS or Standard_LRS.
$storageType = 'Premium_LRS'

#Provide the Azure region (e.g. westus) where Managed Disk will be located.
#This location should be same as the storage account where VHD file is stored
#Get all the Azure location using command below:
#Get-AzLocation
$location = 'westus'

#Provide the URI of the VHD file (page blob) in a storage account. Please not that this is NOT the SAS URI of the stora
ge container where VHD file is stored.
#e.g. https://contosostorageaccount1.blob.core.windows.net/vhds/contosovhd123.vhd
#Note: VHD file can be deleted as soon as Managed Disk is created.
$sourceVHDURI = 'https://contosostorageaccount1.blob.core.windows.net/vhds/contosovhd123.vhd'

#Provide the resource Id of the storage account where VHD file is stored.
#e.g. /subscriptions/6472s1g8-h217-446b-b509-314e17e1efb0/resourceGroups/MDDemo/providers/Microsoft.Storage/
storageAccounts/contosostorageaccount
#This is an optional parameter if you are creating managed disk in the same subscription
$storageAccountId = '/subscriptions/yourSubscriptionId/resourceGroups/yourResourceGroupName/providers/Microsoft
.Storage/storageAccounts/yourStorageAccountName'

#Set the context to the subscription Id where Managed Disk will be created
Select-AzSubscription -SubscriptionId $SubscriptionId

$diskConfig = New-AzDiskConfig -AccountType $storageType -Location $location -CreateOption Import -StorageAccou
ntId $storageAccountId -SourceUri $sourceVHDURI -OsType Linux

New-AzDisk -Disk $diskConfig -ResourceGroupName $resourceGroupName -DiskName $diskName
```

Deploy the VHD

1. Deploy the VHD by building a new Virtual Machine with the newly staged **Managed Disk**.
   Ensure Boot monitoring is set to **Disable** on the virtual machine. Not setting this properly may result in Azure warning of an incomplete boot and a triggered automatic reboot of the VM.



2. For an Actor that will have multiple interfaces, you must to shutdown the VM after deployment and add the optional TEST and MONITOR network interfaces.
    - These interfaces can be on the same subnet as the original MGMT interface.
    - As stated in the Actor operational documentation, the TEST and MONITOR interfaces should be a static IP and routable with a default gateway. A static public IP address is optional ONLY if testing is contained within customer private address space or a common outbound routed gateway is used to reach the internet.
    - After attaching the interfaces, reboot the VM and become familiar with which interfaces is the original MGMT interface and new TEST and MONITOR interfaces before proceeding to run `vsetnet`.
3. For Mandiant-provided VHD images, accessing the newly built VM is performed through an SSH connection that uses the default initial login on the IP address that was provided by the Azure installation.
    - Ensure the default account is changed soon after installation and is set to an appropriately complex combination.
    - Apply firewall rules in your Azure subscription that limit inbound connections to the MGMT interface of the newly deployed Actor. See documentation on required ports for Actor operations.

Set up Networking

1. Boot the installed image and open a console to the image through the virtual infrastructure.
2. After the boot, a login prompt is displayed; Enter the default operating system username and password (Validation Platform Credentials) and update if necessary.
3. Set up the Network Configuration.

    Remember to use a static IP address.

    ```
    sudo vsetnet
    ```

    a. We recommend using `eth0` for the (management) interface.
    b. Only one IP address is necessary for Actors.

4. Confirm the IP settings have been changed.

    ```
    ifconfig
    ```

Add the Network Actor Configuration to the Director

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

- **Use the Add Network Actors option**

- **Create a bulk registration token**

Adding a Network Actor Configuration using the Director

1. Select **Environment > Actors**.
2. Click **Add Network Actors** and fill out the new Actor form.
   Information about several of the fields is provided below.
   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.

      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.
      i. **Push mode**: Director initiates communication to the Actor
      ii. **Pull mode**: Actor initiates communication with the Director

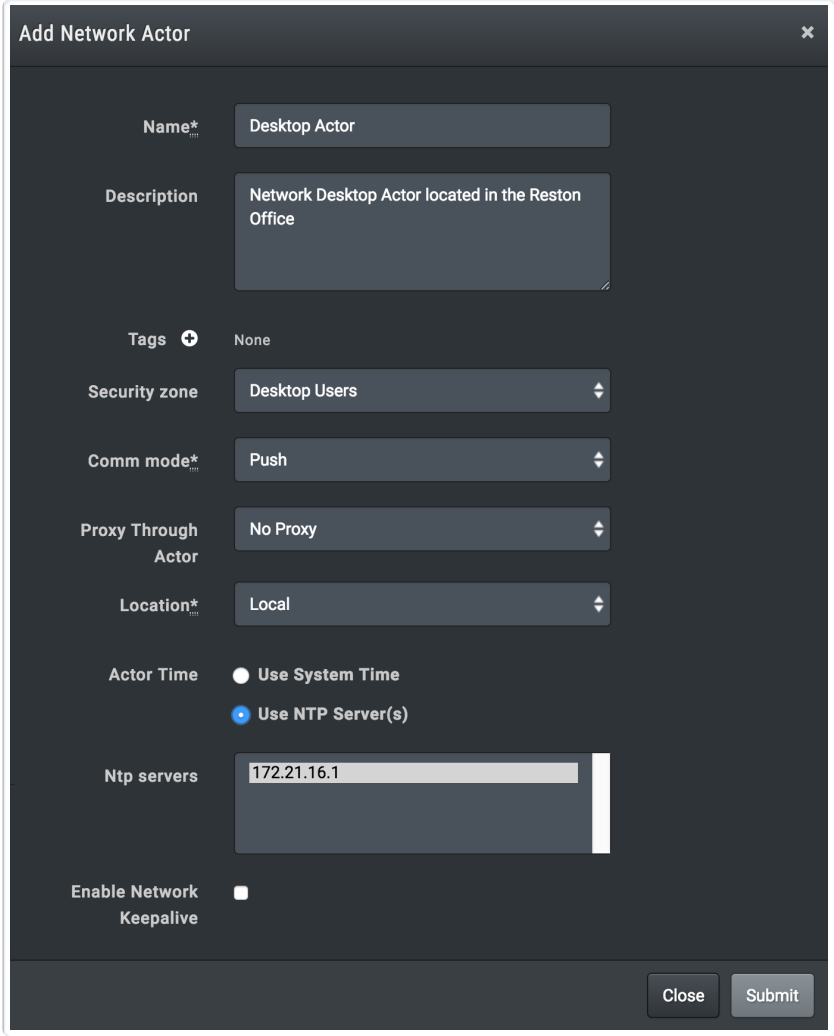
      If the Actor is in Pull mode, you need to run `vregister` to register the Actor to the Director.

   f. **Proxy Through Actor:** Specifies the Actor to use as a proxy to communicate with the Director.

      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. See **Network Actor Requirements (https://docs.mandiant.com/home/msv-network-actor-requirements)** for more information.
   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.
   i. **Actor Time [System/NTP]:** The method used for maintaining the Actor's time. This can be either system time or NTP (see Adding NTP Servers in your Director Install guide if no NTP servers are listed).This must be system time.
   j. **Enable Network Keepalive:** Actors send a periodic (default setting is hourly) ARP request for all Actor interfaces to maintain status in ARP tables.
3. Click **Submit**.
   The Actor is populated in the Pending Actors list and a code is generated. This code must be used for registration

within 15 minutes.



Add Network 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.

Register your Actor using the Director

There are two ways to register your Network Actors to the Director:

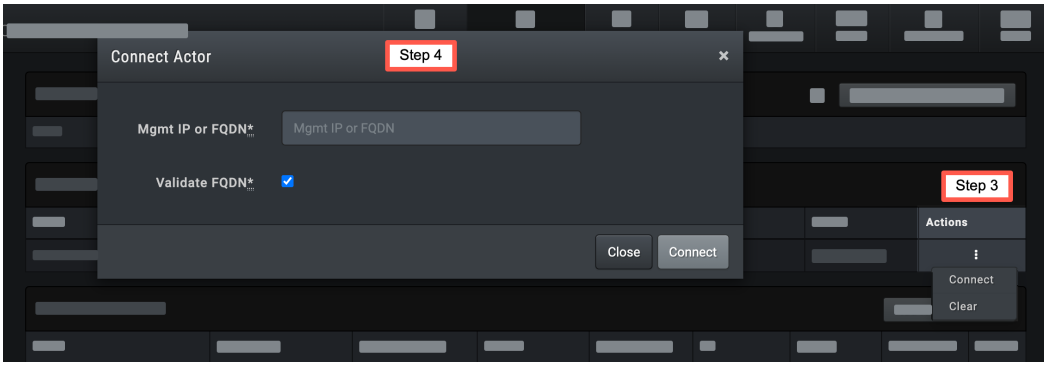
- **Register a Push Mode Actor**
- **Register a Pull Mode Actor**

Register a Push Mode Actor to the Director

Follow one of the sets of steps, depending on how you're registering your Actor:

Pending Actor

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu and Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.
   - The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   - Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.

- **Description:** Short description of the Actor
- **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
- **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
- Optional. Select **Enable Network Keepalive.**

5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.

Register a Pull Mode Actor by using the command line

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

> If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.

3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table

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

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

6. If desired, add a proxy.
   a. Enter **yes**.
   b. Enter the *Proxy IP* and *Proxy Port*.
   c. If there is an account associated with the proxy, enter *the account info*.
   The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

VHD for Hyper-V

This section contains information for the installation of an Actor from a VHD file on Hyper-V. The overall steps involved are listed as follows:

1. **Install on Hyper-V**
2. **Set up Networking**
3. **Add the Network Actor Configuration to the Director**
4. **Register your Actor using the Director**

Install the Actor: Hyper-V

Prerequisites

If you're deploying a VHD or installer-based Actor and want to set the IP address to a static value, controlled by the Actor, the host adapter must be configured to support a static MAC address.

To achieve this, you must disable dynamic MAC addresses:

1. Open Hyper-V Manager and then VM settings.
2. Here, expand the **Network Adapter** and go to **Advanced Features**.
3. To set the VM with a static MAC address, enable the **Static** option and enter a unique address for the adapter.

> A dynamically assigned address may be sufficient for a static assignment, but if unsure, enter a unique address manually.

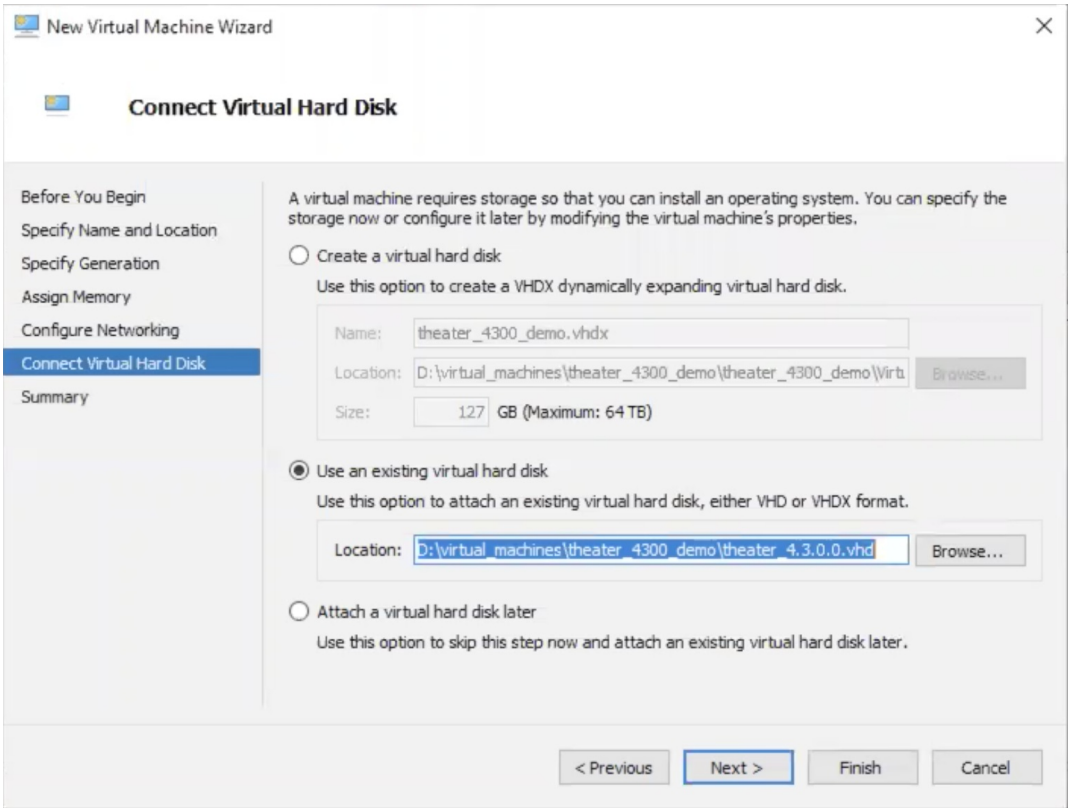
Install the Actor on Hyper-V

1. Download the VHD image from **Actor and Protected Theater Downloads (https://docs.mandiant.com/home/msv-actor-installers)**.
2. Extract the VHD and then copy it to your desired location. If you have a standard virtual machines folder, we suggest you use that.
3. Create the Virtual Machine in Hyper-V.
    a. Click **New** > **Virtual Machine**.
    b. Click **Next**.
    c. Enter a **Name** for your Actor virtual machine and (optional) select the **Location** where the virtual machine should be stored. Then click **Next**.

d. Specify **Generation**. Generation 1 is recommended. Then click **Next**.
e. Assign Memory. **4096 mb** is recommended. For additional details, see **Network Actor Requirements (https://docs.mandiant.com/home/network-actor-requirements)**. Then click **Next**.

> IMPORTANT: Do NOT select Use Dynamic Memory for this virtual machine.

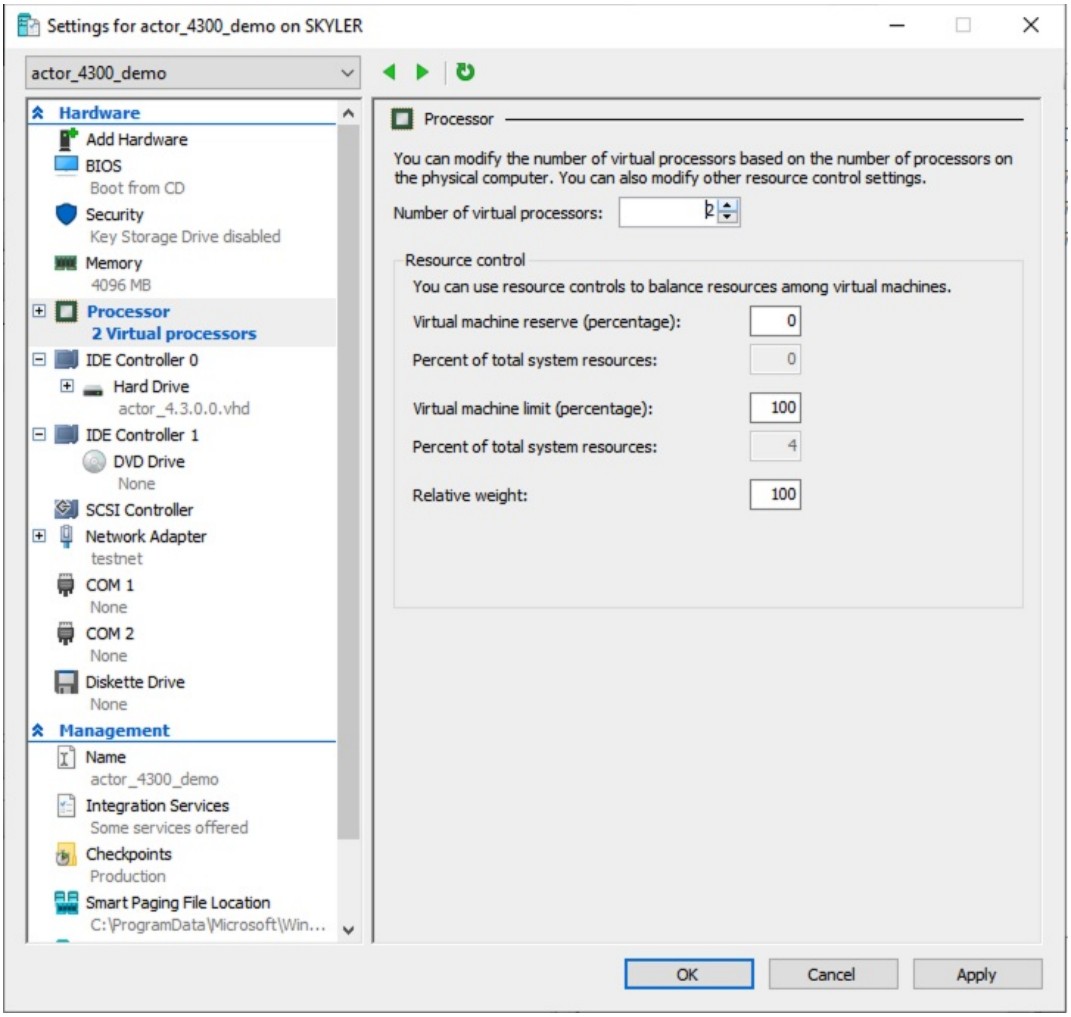
f. Select your network **Connection**. Then click **Next**.
g. Choose **Use an existing virtual hard disk** , navigate to the disk's location, and then click **Next**.



Hyper-V example: Connecting a Virtual Hard Disk to a new Virtual Machine

h. Verify everything is configured as expected and then click **Finish**. The virtual machine will display and be selected in the Virtual Machines list.

4. Update the Virtual Machine's Processor info.
   a. Select your Actor Virtual Machine and click **Settings**.
   b. Click **Processor**, adjust Number of virtual processors to **2**, click **Apply**, and click **OK**.



Hyper-V: Adding processors to a virtual machine

5. Expose the Virtualization Extensions for your VM.
    a. Open a Windows PowerShell Admin window
    b. Run the following command:

```
Set-VMProcessor <VMName> -ExposeVirtualizationExtensions $true
```

6. Start the Virtual Machine by selecting the VM in Hyper-V Manager and clicking **Connect**.

Set up Networking

1. Boot the installed image and open a console to the image through the virtual infrastructure.
2. After the boot, a login prompt is displayed; Enter the default operating system username and password (Validation Platform Credentials) and update if necessary.
3. Set up the Network Configuration.

> Remember to use a static IP address.

```
sudo vsetnet
```

    a. We recommend using `eth0` for the (management) interface.

b. Only one IP address is necessary for Actors.

4. Confirm the IP settings have been changed.

```
ifconfig
```

Add the Network Actor Configuration to the Director

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

- **Use the Add Network Actors option**
- **Create a bulk registration token**

Adding a Network Actor Configuration using the Director

1. Select **Environment > Actors**.
2. Click **Add Network Actors** and fill out the new Actor form.
   Information about several of the fields is provided below.
   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.

> 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.
      i. **Push mode**: Director initiates communication to the Actor
      ii. **Pull mode**: Actor initiates communication with the Director

> If the Actor is in Pull mode, you need to run `vregister` to register the Actor to the Director.

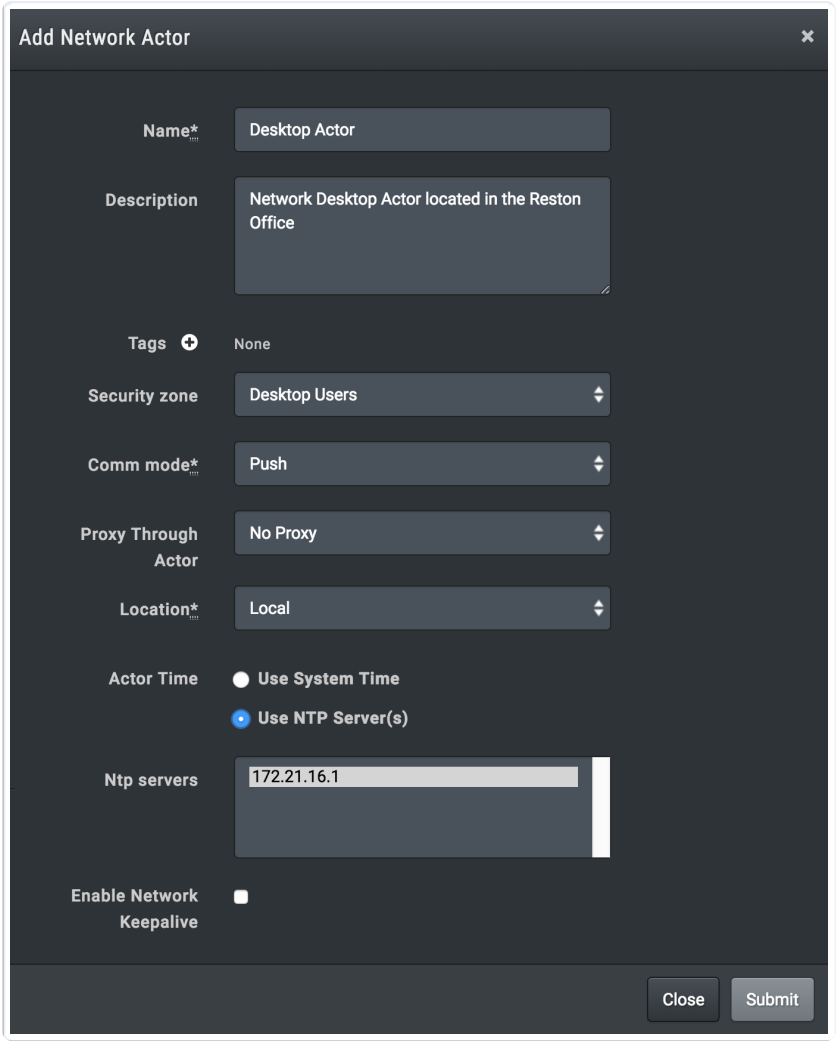
   f. **Proxy Through Actor:** Specifies the Actor to use as a proxy to communicate with the Director.

> 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. See **Network Actor Requirements (https://docs.mandiant.com/home/msv-network-actor-requirements)** for more information.
   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.
i. **Actor Time [System/NTP]:** The method used for maintaining the Actor's time. This can be either system time or NTP (see Adding NTP Servers in your Director Install guide if no NTP servers are listed).This must be system time.
j. **Enable Network Keepalive:** Actors send a periodic (default setting is hourly) ARP request for all Actor interfaces to maintain status in ARP tables.

3. Click **Submit**.
   The Actor is populated in the Pending Actors list and a code is generated. This code must be used for registration within 15 minutes.



Add Network 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.

Register your Actor using the Director

There are two ways to register your Network Actors to the Director:

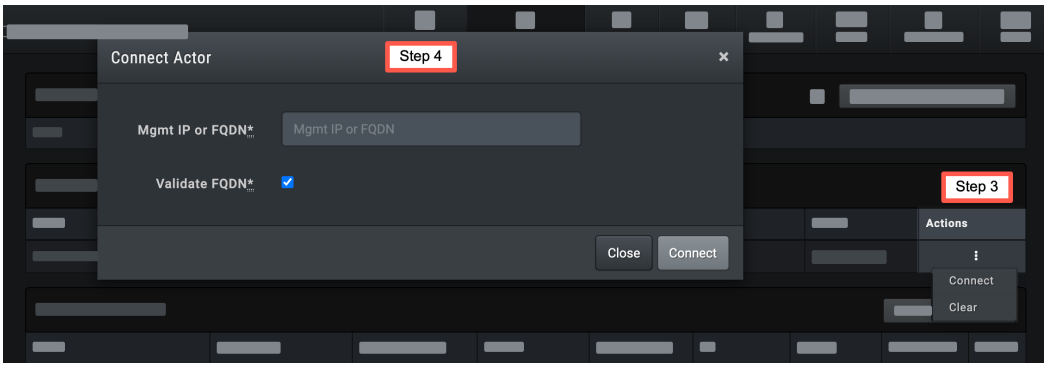
- **Register a Push Mode Actor**
- **Register a Pull Mode Actor**

Register a Push Mode Actor to the Director

Follow one of the sets of steps, depending on how you're registering your Actor:

Pending Actor

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu and Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.

- The message "Actor '*actor name*' is being registered and will update automatically below" displays.
- Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.
   - **Description:** Short description of the Actor
   - **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
   - **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
   - Optional. Select **Enable Network Keepalive.**
5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.

Register a Pull Mode Actor by using the command line

1. Connect to the Actor by using SSH.
2. Using an elevated command prompt, navigate to the scripts directory and run `vregister`.

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

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

   If you need to see Tap Adapters when selecting the interfaces, add the argument `--include-tap-adapters` when running vregister.
3. Enter the Director's *FQDN or IP address*.
4. Enter the appropriate code from the Director:
   - *registration code* in the Pending Actor's table
   - *bulk registration token code* in the Bulk Registration Tokens table
5. If prompted, specify if you want to verify the Director TLS Certificate [yes|no].
   When set to Yes, it'll verify the certificate during registration and then every time the Actor reaches out to the Director (HTTPS requests).This prompt only appears for Pull Actors.

   Actors can verify TLS certs signed by public CAs, but not private CAs.
6. If desired, add a proxy.
   a. Enter **yes**.
   b. Enter the *Proxy IP* and *Proxy Port*.
   c. If there is an account associated with the proxy, enter *the account info*.
   The command line states "Successfully validated with Verodin Director" and the Director's Actor listing moves the Actor from the Pending Actors list to the Actors list.

Example of registration steps using `vregister`

```
[nodeone@actor ~]$ sudo vregister

 - Verodin Registration Script -

Enter IP Address or Hostname of Verodin Director: 172.16.39.193

Enter Code from Verodin Director: XXXX-XXXX-XXXX

Use Proxy To Connect To Verodin Director (yes|no): yes

Enter Proxy IP Address: 172.16.71.234

Enter Proxy Port: 443

Enter Proxy Username (blank for none): verodinuser

Enter Proxy Password:
```

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
- The Security Validation platform can manage the firewall configuration (Linux Actors)

There are also some OS specific requirements:

- Red Hat Enterprise Linux (RHEL), CentOS, and Rocky Linux
  - The account you use to connect to the OS and install is in the `sudoers` file.
  - The `/tmp` directory must allow executable files or you must have defined a different `/tmp` directory (where the installer downloads to).

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.

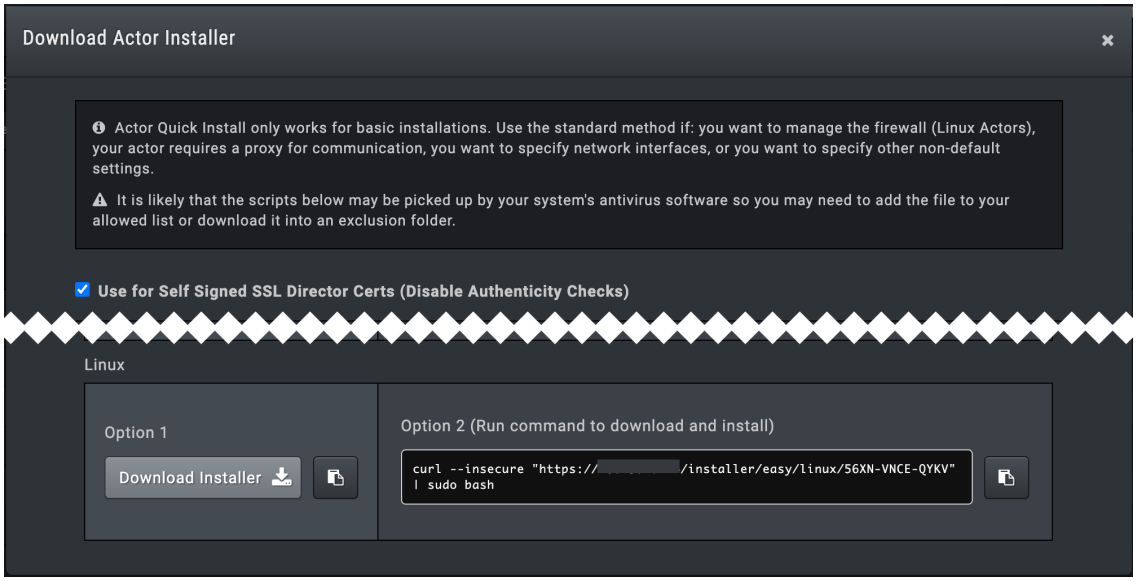
Install and register a Linux Actor

There are several ways to use the bulk registration code to complete installation. The most common use case is included here. After this process completes, you have a registered Linux Actor that is configured with Pull Comm mode. The Actor also has management and test interfaces configured to use the network interface associated with the default route.

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Locate the token that you want to use in the **Bulk Registration Tokens** table on the Actors page 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. Subsequently, the install does not verify the cert when the Actor connects to the Director (HTTPS requests).

5. In the **Linux** section, click **copy** next to the command for Option 2.



Installer window for Linux Bulk Registration Token

6. Using an account that has root access, SSH to the Linux system.
7. Paste the command to start the install. An example is provided:

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

   The Actor installs and registers. When it completes, the Actor is listed in one of the following tables: the Endpoint Actors table for Ubuntu or the Network Actors table for RHEL/CentOS/Rocky Linux.

Standard

The installation of the Actor can be completed using the Director and an install wizard. This guide will walk you through the following:

Add the Network Actor Configuration to Director

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

- Use the Add Network Actors option
- Create a bulk registration token

Adding a Network Actor Configuration using the Director

1. Select **Environment > Actors**.
2. Click **Add Network Actors** and fill out the new Actor form.
   Information about several of the fields is provided below.
   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.

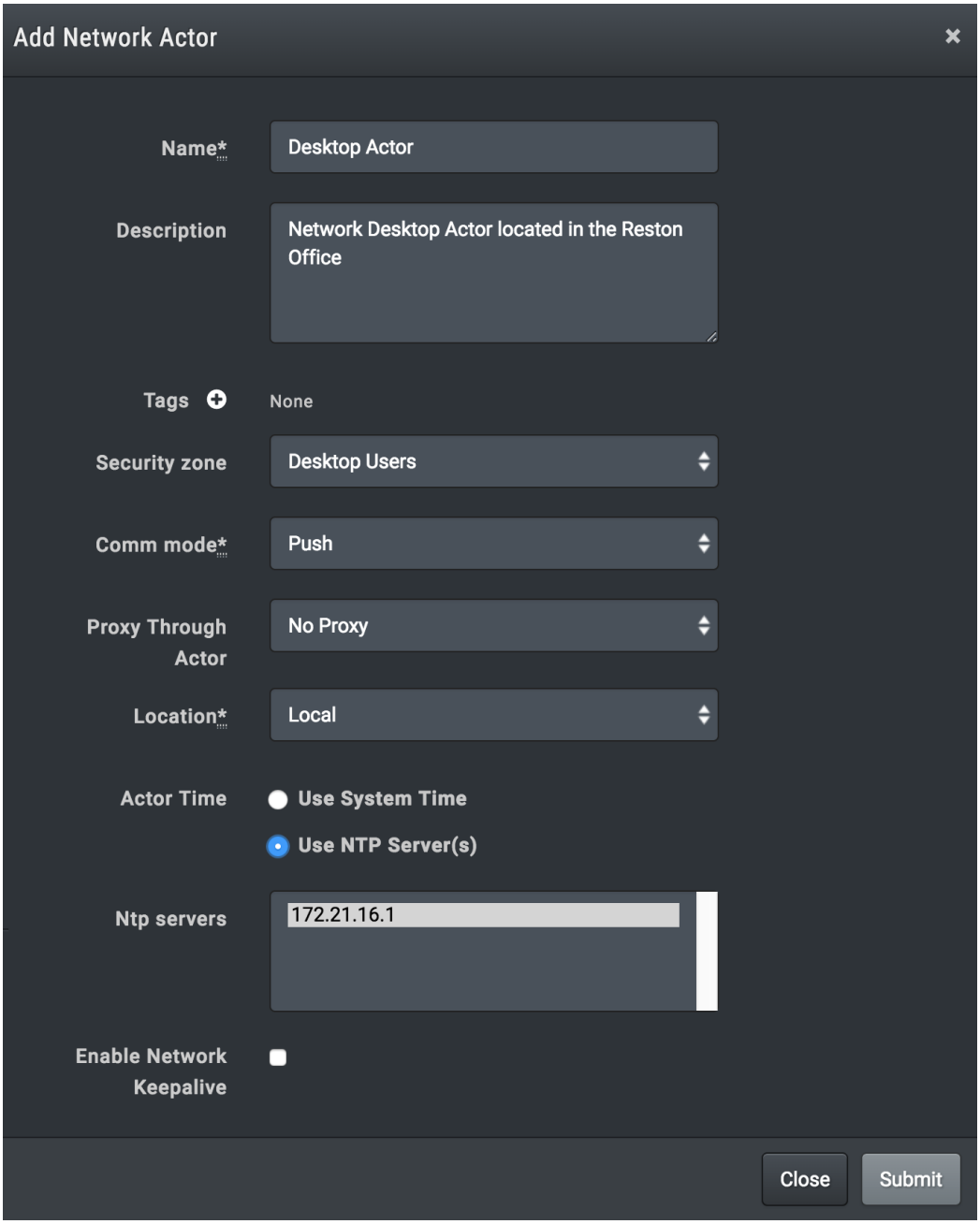
   d. **Security Zone:** The area of your network where the Actor will live.
      Security zones are added to the Director after the Director is installed (see Adding Security Zones in your Director Install guide if there are no security zones listed).
   e. **Comm Mode:** The communications mode by which the Director and Actor communicate.
      i. **Push mode:** Director initiates communication to the Actor
      ii. **Pull mode:** 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.
   i. **Actor Time [System/NTP]:** The method used for maintaining the Actor's time. This can be either system time or NTP (see Adding NTP Servers in your Director Install guide if no NTP servers are listed).This must be system time.
   j. **Enable Network Keepalive:** Actors will send a periodic (default setting is hourly) ARP request for all Actor interfaces to maintain status in ARP tables.

3. Click **Submit**.
   The Actor will be populated in the Pending Actors list and a code will be generated. This code must be used for registration within 15 minutes.



Add Network 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/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 Linux Network Actor

The Actor installer is provided as a gzipped tar archive file: actor_*[version]*.tar.gz.

Regardless of which installation method you use, this installer installs all required dependencies.

> The Security Validation team recommends using an online repository to install the dependencies. If this is not possible, use a CentOS machine. There is a copy of the CentOS dependencies as part of the installable software. For more information, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.

If there are issues during installation, specific messages are provided so you can quickly resolve the issue and continue.

The Actor tar file consists of the following items:

- `verodin-actor-install` : the executable installer
- `files` : a folder containing files used by the installer
- `example-ubuntu.ini` : a sample ini file that can be used to automate the installation on Ubuntu
- `example-centos.ini` : a sample ini file that can be used to automate the installation on CentOS or RHEL
- `README` : a short text file with an overview of the install process

Complete the installation

> Use the account you created in **Configure the Environment (https://docs.mandiant.com/home/msv-actor-configure-the-environment)**.

This section provides the steps, and when applicable, sample commands, used to install the Actor.

1. **Download the installer (https://docs.mandiant.com/home/msv-actor-installers)** and then copy it to the system where you want to install it.

```
$ scp <file name> user@<ip address>:
```

2. Use ssh to open a command line on the system where you want to install the Actor. Director.
3. Untar the Actor tar.gz file.

```
$ tar -xvf actor_version.tar.gz
```

4. Change to the newly uncompressed Actor directory and then run the installer.

> If there is a space in the path, the install will fail.

```
$ cd actor_version
```

```
$ sudo ./verodin-actor-install
```

Keep in mind the following settings during installation:

a. **User**: This is the user account you created that includes root access.
b. **Group**: This is the system group to run the Validation Platform programs and services.
c. **Test Network and Monitor Interfaces**: If you do not have a separate interface, you can press Enter. Unless a value is specified, the test interface will use the management interface.
d. **Repository**: The preferred method is to get the files online using yum because it will be more in tune with your security policy. For more information, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.
e. Sudoers enabled

> Enabling sudoers is preferred. If you do not enable it, or if it is inadvertently modified, a copy is backed up in /opt/apps/verodin/node/settings/verodin_sudoers.

5. The installer will then check your input and verify preliminary conditions are satisfied. Possible outcomes of this check include:

- **Issue Found:** Did not run as root

> Additional Issues could be identified and presented to you. The messages presented will be as detailed as the issues you have seen here.

- **Issue Found:** Did not have a valid user entered
- **Major Issue Found:** detailed information will be provided
- **No Issue Found:** The installation will continue, verifying requirements and packages are installed. A sample of what is displayed is shown below.

> - The installation can be a long-running process. Allow at least 10 minutes for installation to complete.
> - The Validation Platform creates or overwrites any existing nginx.service file during installation. The path to this nginx.service file is /usr/lib/systemd/system/nginx.service.

```
checking is_root_user... ok
```

```
checking user_exists... ok
```

```
checking interface_exists... ok
```

```
checking interface_is_up... ok
checking cpu_count_actor... ok
checking memory_size_actor... ok
installing optional local repository...ok
installing dependencies from yum repository...ok
installing verodin actor to opt/apps...ok
Generating a 4096 bit RSA private key
.....++
writing new private key to 'server.key'
-----
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
..+.....+.....++*++*
The installation information gathered is saved in the file actor.ini
Log information is contained in actor-install.log.
```

6. Optional: Add the scripts directory to the `PATH`

```
To utilize verodin scripts please add this to the appropriate bash profile
export PATH=/opt/apps/verodin/node/node/scripts:$PATH
And add this path to the appropriate secure path
/opt/apps/verodin/node/node/scripts
```

Adjust the directory if you modified where you installed the Actor.

Configure the Linux Network Actor

After installing the Actor, you'll need to set up the Actor's networking.

Two network interfaces are required if you want to test Network Controls - one for management interaction with the Director, which should be a static IP, and one for job execution. A third interface for monitoring is supported.

When setting up your interfaces, you can use DHCP. Do not use DHCP to set up multiple interfaces on the same subnet. Doing so may cause communication issues and prevent Actions from running

properly. If you have two interfaces on one subnet, each must have its own static IP. See **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) for more information.

Manual changes to network configuration files can be overwritten during updates and in-platform configuration changes.

1. If necessary, log into your Actor.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

```
sudo /opt/apps/verodin/node/node/scripts/vsetnet
```

or

```
sudo vsetnet
```

Remember to use a static IP address.

This command walks you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and are responsible for configuring the networking. For more information about `vsetnet`, see **Configuring an Actor's Network Settings** (https://docs.mandiant.com/home/msv-network-actor-requirements#using).

Network Actors may be misconfigured if you do not run `vsetnet` before registering the Actor. If the registration process identifies a misconfigured Actor, it will stop and prompt you to run `vsetnet`.

   a. When available, we recommend using **`eth0`** for the (management) interface
   b. If you're only interested in testing endpoint controls, one interface and not two is required

Network installation prompts

3. After completing configuration, confirm that the IP settings have been changed.

> Remember, if you're using an RHEL 8-9 or CentOS 9 system, no network settings are changed based on running `vsetnet`. You must configure the networking on your own.

```
ifconfig
```

Update a Linux Actor's Information in the Director

After updating the Actor's networking, we recommend verifying the changes and then updating the Actor's information in the Director.

1. Log into the Actor from the command line.
2. Confirm that the IP settings have been changed.

```
ifconfig
```

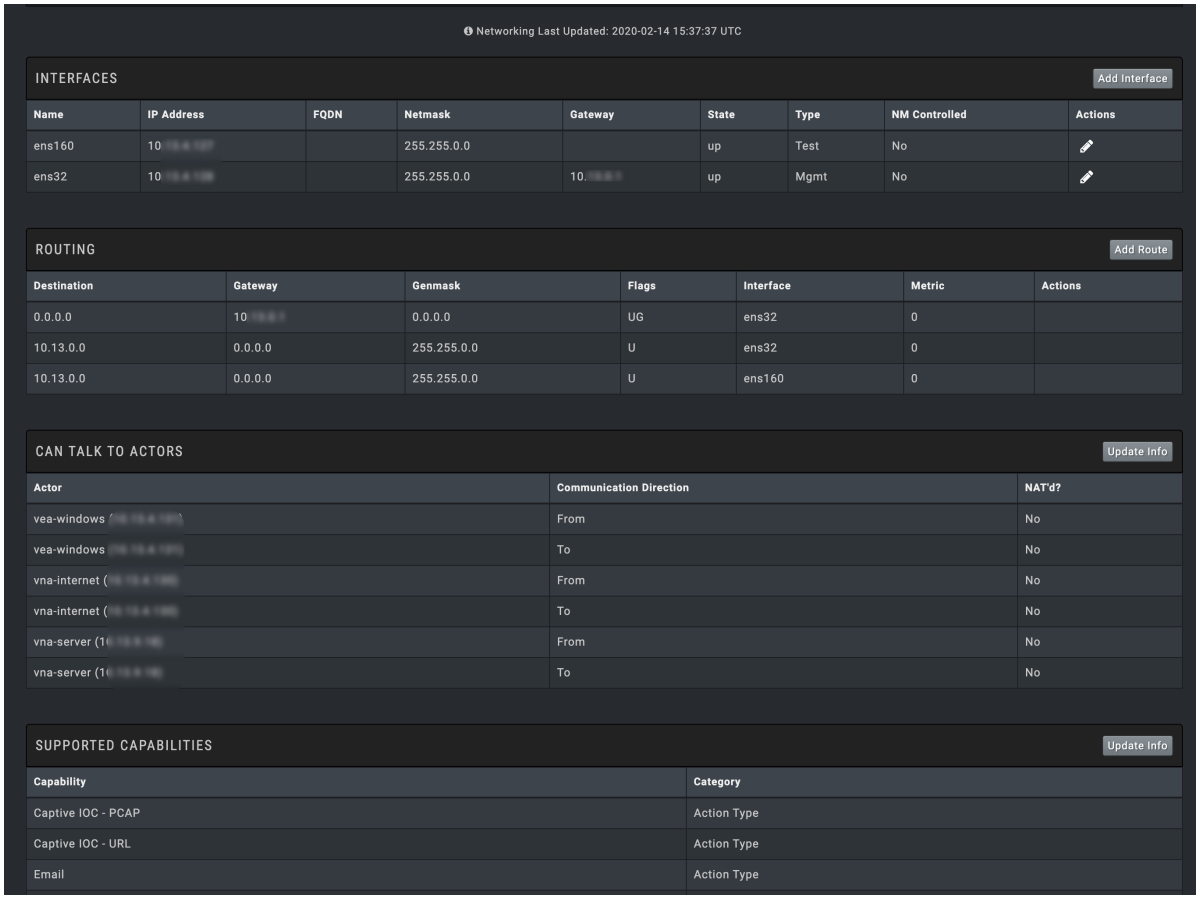
3. Launch the Director.
4. Select **Environment > Actors**.
5. Locate the Actor you updated, open its Action menu, and click **Edit**.
6. Click **Refresh Actor Info**.

Within the Director, you can review and refresh the Actor's network settings. Depending on the Actor, you may also be able to directly update information. This information includes

- Interfaces
- Routing
- Communication with Actors
- Supported Capabilities

> The configuration changes you can make to the Actor's Networking in the Director depend on the form-factor used to install the Actor and if the Validation Platform is managing the Network information.

If you change an Actor's network information using the Director, we recommend updating its **Can Talk to Actors** and **Supported Capabilities** settings.



Actor Networking configuration and capabilities

If your network changes after installing your Actor or you want to change how the Actor's networking is managed, you can update the Actor's networking using the vsetnet command. For full details on how to run the vsetnet command, see the Actor installation documentation for your platform.

Update a Linux Actor's Network Settings

If your network changes after installing your Actor, you can update the Actor's networking using the `vsetnet` command. If you're managing multiple interfaces on the same subnet for a Network Actor, see **Using Multiple Interfaces on the same Subnet (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info)** before running `vsetnet`.

When you run vsetnet on an Actor installed using the OVA appliance, the first decision you make is whether you will manually manage the Actor's network configuration files or have the Validation Platform manage it. Items to consider when making this decision include:

- Allowing the Validation Platform to manage the network configuration improves network reliability and stability.
- Actors that meet the requirements but were installed before version 4.0.1.0 came out will have this setting disabled.
- This setting can be modified by rerunning `vsetnet` for the Actor.
- Enabling this setting overwrites any changes that you've made to the Actor's network configuration files.

For release 4.14.0.2 onward, if you specify Verodin Control during `vsetnet`, `vsetnet` configures the system as follows:

- If DHCP is selected for all interfaces configured, `cloud-init` remains in a running state.
- If Static IPs are used for one interface or more, `cloud-init` is disabled.

If Verodin Control is declined during `vsetnet`, you are responsible for configuring or disabling `cloud-init`.

If another configuration is required, you can make changes as needed after you run `vsetnet`. However, re-running vsetnet can reset settings. To enable or disable `cloud-init`, the `vsetnet` code adds or removes the file: `/etc/cloud/cloud-init.disabled`. If the automatic configuration doesn't suit your needs, you can manually add or remove the file, as needed.

Actors on RHEL/CentOS 7.x systems cannot be completely managed by the Validation Platform. However, you can use the platform to update the network configuration files for those Actors. The Validation Platform cannot manage or update the network configuration files for any endpoint Actor or Actors on RHEL 8 - 9, CentOS 9, and Ubuntu systems.

1. Log into the Actor from the command line.
2. Run the following command to select the interfaces (all) and update the network configuration (RHEL 7.x, CentOS 7.x). If you did not update the PATH, use the first command, updating the path if necessary.

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

   or

   ```
   sudo vsetnet
   ```

   This will walk you through configuring the networking. If you choose to set it up manually and you are not using RHEL 8 - 9 or CentOS 9, for each interface you use you'll need its IP address, netmask, gateway, and DNS information. If you're using RHEL 8 - 9 or CentOS 9, you only select the interface and you're responsible for configuring the networking.

   IMPORTANT: If you're managing multiple interfaces on the same subnet, see **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) before running `vsetnet`. If you're rerunning `vsetnet` and are prompted "Will Verodin control the network configuration files?", saying **yes** means that the platform will start managing the networking and will overwrite any changes you previously made to the network configuration files.
3. After completing configuration, confirm that the IP settings have been changed.

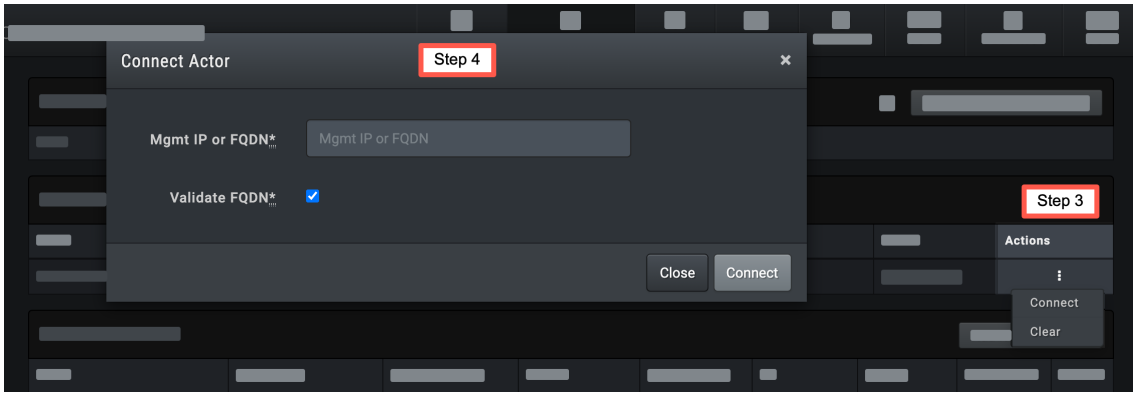
   ```
   ifconfig
   ```
4. Launch the Director.
5. Select **Environment > Actors**.
6. Locate the Actor that you want to configure, open its Action menu, and click **Edit**.
7. Click **Refresh Actor Info**.

Register your Network Actor using the Director

There are two ways to register your Network Actors in the Director: **Register a Pending Actor** or **Register an Actor that uses Push communication using a bulk registration token**.

Register a Pending Actor from the Director

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu & Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.
   - The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   - Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Register an Actor using Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.
   - **Description:** Short description of the Actor
   - **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
   - **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
   - (Optional) **Enable Network Keepalive**
5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.

Automated

The installation of the Actor can be completely automated. This guide walks you through the following:

1. **Adding the Actor Configuration - API**
2. **Installing the Actor - Automated Method**
3. **Configuring Networking Using a JSON File**

4. **Registering Your Actor - Automated Method**

Adding the Actor Configuration - API

You can do one of the following:

- **Add the Actor Configuration** or
- **Create a Bulk Registration token**.

If you aren't comfortable using the platform API, you can **Add the Network Actor Configuration to Director (https://docs.mandiant.com/home/msv-adding-the-network-actor-configuration-to-director)**, **Register your Network Actor using the Director (https://docs.mandiant.com/home/msv-registering-your-actor-using-the-director)**, or **Add the Endpoint Actor Configuration to the Director (https://docs.mandiant.com/home/msv-adding-the-endpoint-actor-configuration-to-the-director)** instead.

> If you use the bulk registration token, your Actor uses Pull communication. You can edit Network Actors after the Actor is registered if you want it in Push.

Use the Platform API to add the Actor Configuration

Create the Actor Configuration in the Director by posting to the Director API.

1. Create a JSON file, `nodes.json`. The following is a sample JSON.

```
network_request = { "node" : { "name": "test-network",
"desc": "test network",
"security_zone_id": 1,
"location": "Local",
"node_type": "network"
"comm_mode": "Pull",
"pull_interval": "30"},
"proxy_node_id": "4"
}
```

   - `node_type` options are `network` and `endpoint`.
   - When `node_type` is `endpoint`, `comm_mode` must be `Pull`.
   - `comm_mode` options are `Pull` and `Push`.

2. Post `nodes.json` to the Director.

```
$ https://director_ip/nodes.json
```

   Once the file is posted, the registration code is returned, which expires in 15 minutes.

Create Bulk Registration Tokens using the API

Create the Bulk Registration Token by posting to the Director API.

1. Create a JSON file, `save_bulk_token.json`. The following is a sample JSON.

```
{
"bulk_token": {
"name": "test",
"security_zone_id": 3,
"expiration_date": "2020-12-30",
"max_uses": "2"
}
}
```

2. Post `save_bulk_token.json` to the Director.

```
$ https://director_ip/save_bulk_token.json
```

Once the file is posted, the bulk registration token code is returned, which is valid through the expiration date.

Installing the Actor - Automated Method

The Actor installer is provided as a gzipped tar archive file: actor_*[version]*.tar.gz.

Regardless of which installation method you use, this installer will install all required dependencies.

> The Security Validation team recommends using an online repository to install the dependencies. If this is not possible, use a CentOS machine. There is a copy of the CentOS dependencies as part of the installable software. For more information, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.

If there are issues during installation, specific messages are provided so you can quickly resolve the issue and continue.

The Actor tar file consists of the following items:

- `verodin-actor-install` : the executable installer
- `files` : a folder containing files used by the installer
- `example-ubuntu.ini` : a sample ini file that can be used to automate the installation on Ubuntu
- `example-centos.ini` : a sample ini file that can be used to automate the installation on CentOS or RHEL
- `README` : a short text file with an overview of the install process

Start the Installation

1. Download the installer from the Customer Portal (**https://msv.mandiant.com (https://msv.mandiant.com/)**) and then copy it to the system where you want to install it.

```
$ scp <file name> user@<ip address>:
```

2. Use ssh to open a command line on the system where you want to install the Actor.

> Use the account you created in **Configure the Environment (https://docs.mandiant.com/home/msv-configure-the-environment)**.

3. Untar the Actor tar.gz file.

```
$ tar -xvf actor_version.tar.gz
```

4. Choose one of the following installation methods:
   - **(Option 1) - Direct Install with flags**
   - **(Option 2) - Automated installation with an ini file**

Option 1: Direct Install with Flags

1. Launch the installer using flags to identify the variable responses.
   - **Method 1**: Including the required flags only (sample values are provided)

2. ```
   $ cd actor_version
   ```

   ```
   $ sudo ./verodin-actor-install --user nodeone --group nodeone --management eth0 --repository yum
   ```

   ```
   $ sudo ./verodin-actor-install --management eth0
   ```

   - **Method 2**: Including required flags and optional flags (sample values are provided)
     Add optional flags if you want to enabled/disable items (modify the default behavior that is assigned when the flag is not included)

3. ```
   $ cd actor_version
   ```

   ```
   $ sudo ./verodin-actor-install --user nodeone --group nodeone --management eth0 --repository yum --test eth1 --monitor eth2 --prefix /opt/apps/ --kerberos --disable-fw-control --disable-sudoers --disable-cmd-alias
   ```

   ```
   $ sudo ./verodin-actor-install --management eth0 --test eth1 --monitor eth2 --prefix /opt/apps/ --kerberos --disable-fw-control --disable-sudoers --disable-cmd-alias
   ```

   - The specified username must be an active user on the system.
   - To test network security controls, you must use two interfaces. If you do not have a separate interface to use for your monitor interface, you can remove it. Unless a value is specified, the test interface is automatically used.

   Repository options are yum (getting the dependencies online / a customer provided repository) or verodin (using the files that are included with the installer). The verodin repository is only valid for CentOS systems.
   The preferred method is to get the files online using yum, because it will be more in tune with your security policy. For more information, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.

   To see a full list of the flags, you can type the following command:

   ```
   sudo ./verodin-actor-install --help
   ```

   Arguments:

   - **-c or --config-file**: a Validation Platform installation configuration file
   - **-p or --prefix**: the prefix of the location where the verodin folder will reside
   - **-u or --user**: the username for file and process ownership
   - **-g or --group**: the group for file and process ownership
   - **-k or --kerberos**: the Actor will use a kerberos proxy
   - **--disable-fw-control**: the Actor will not control firewall/iptables
   - **--disable-sudoers**: Do not create /etc/sudoers.d/verodin for Actor privilege escalation

     Enabling sudoers is preferred. If you do not enable it, or if it is inadvertently modified, a copy is backed up in /opt/apps/verodin/node/settings/verodin_sudoers.

   - **--disable-cmd-alias**: Do not write cmd_alias commands to /etc/sudoers.d/verodin for Actor privilege escalation

- **-m or --management**: the network interface to use for communications
- **-t or --test**: the network interface to use for Actions
- **-b or --monitor**: network interface to use for Monitor Actions
- **--nginx16**: Use RHEL7 nginx16 package instead of CentOS nginx package
- **-r or --repository**: the source for packages: yum or verodin

2. The installer will check your input and verify preliminary conditions are satisfied (installing as root, username exists, system requirements are met, etc.). If no issues are found, installation will complete. If issues are found, the installer provides messages clearly identifying the issue.
3. (Optional) Add the scripts directory to the `PATH`

```
To utilize verodin scripts please add this to the appropriate bash profile
```

```
export PATH=/opt/apps/verodin/node/node/scripts:$PATH
```

```
And add this path to the appropriate secure path
```

```
/opt/apps/verodin/node/node/scripts
```

Adjust the directory if you modified where you installed the Actor.

Option 2: Automated installation with an ini file

1. Create the configuration file, **my-actor.ini** and open it.

```
$ cd actor_version
```

```
$ cp example-centos.ini my-actor.ini
```

```
$ cp example-ubuntu.ini my-actor.ini
```

```
$ vi my-actor.ini #
```

2. Update the **my-actor.ini** configuration file you just created, editing the options as instructed by the comments in that file. A sample file that does not include descriptions is shown below.

- To test network security controls, you must use two interfaces. If you do not have a separate interface to use for your monitor interface, you can remove it. Unless a value is specified, the test interface is automatically used.
- Enabling sudoers is preferred. If you do not enable it, or if it is inadvertently modified, a copy is backed up in /opt/apps/verodin/node/settings/verodin_sudoers.

Repository options are yum (getting the dependencies online / a customer provided repository) or verodin (using the files that are included with the installer). The verodin repository is only valid for CentOS systems.
The preferred method is to get the files online using yum, because it will be more in tune with your security policy. For more information, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.

```
[options]
```

```
user = nodeone
```

```
group = nodeone
```

```
management = interface
repository = yum
## Optional
test = eth1
monitor = eth2
prefix = /opt/apps
kerberos = False
firewall_control = True
sudoers = True
cmd_alias = True
```

3. Launch the installer with the configuration file:

```
$ sudo ./verodin-actor-install --config-file my-actor.ini
```

   The installer will then check the user input and verify preliminary conditions are satisfied (installing as root, user name exists, system requirements are met, etc). If there are no issues installation will occur. If issues are identified, you will see messages that clearly identify the issue.

4. (Optional) Add the scripts directory to the `PATH`

```
To utilize verodin scripts please add this to the appropriate bash profile
export PATH=/opt/apps/verodin/node/node/scripts:$PATH
And add this path to the appropriate secure path
/opt/apps/verodin/node/node/scripts
```

   Adjust the directory if you modified where you installed the Actor.

Configuring Networking Using a JSON File

After installing the Actor, you need to setup the Actor's Networking.

Two network interfaces are required if you want to test Network Controls: one for management interaction with the Director, which should be a static IP, and one for job execution. A third interface for monitoring is supported.

- When setting up your interfaces, you can use DHCP. Do not use DHCP to set up multiple interfaces on the same subnet. Doing so may cause communication issues and prevent Actions from running properly. If you have two interfaces on one subnet, each must have its own static IP. See **Using Multiple Interfaces on the same Subnet** (https://docs.mandiant.com/home/msv-network-actor-requirements#vsetnet-info) for more information.
- Manual changes to network configuration files can be overwritten during updates and in-platform configuration changes.
- This process is only valid for Actors using RHEL 7.x or CentOS 7.x and earlier (both OVA and installable software formats). In addition to the OS requirements, it should only be used if you are managing the networking. For RHEL 7.x or CentOS 7.x, if you want the Validation Platform to manage the networking, you must run the vsetnet command.
- This process should only be used if you are managing the networking. If you want Validation Platform to manage the networking, you must run the vsetnet command.

1. Create a JSON file, **actor-config.json**, that contains the configurations for your interfaces (management, test, and if using, monitor).

```
{
"management" :
{ "name" : "eth0", "dhcp" : "false", "ip_address" : "172.27.73.6", "netmask" : "255.255.252.0", "gateway" :
"172.27.72.1", "dns" : "172.27.72.1", "rewrite" : "true" }
,
"test" :
{ "name" : "eth1", "dhcp" : "true", "rewrite" : "true" }
}
```

   - The configuration can be set up with static information, as shown in the Management configuration.
   - The configuration can be set up to use DHCP, as shown in the Test configuration.
   - You can turn the rewrite option on or off.

2. Use the JSON file to automatically set the configuration.

```
$ sudo vsetnet -c actor-config.json
```

   NOTE: `vsetnet` can be run at anytime; if you run it after the Actor has been registered, remember to go into the Director and refresh the Actor's network info

3. After completing configuration, confirm the IP settings have been changed.

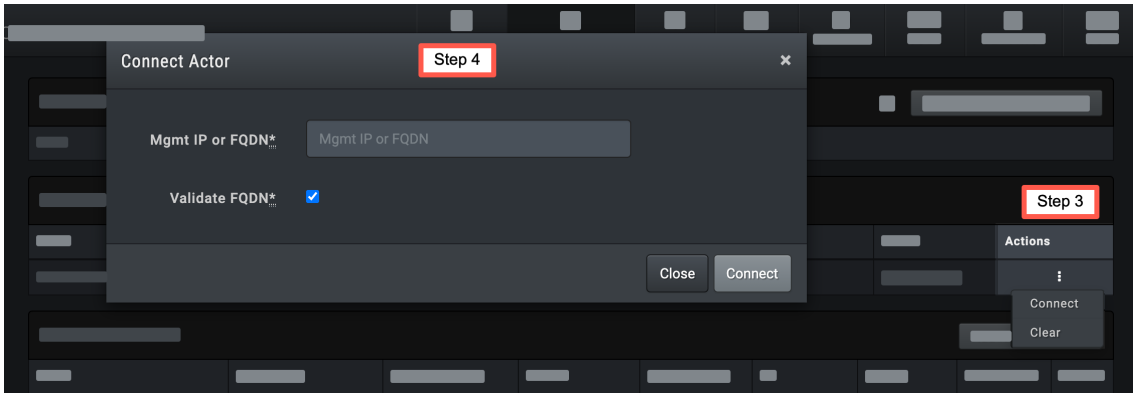
```
ifconfig
```

Registering Your Actor - Automated Method

There are two ways to register your Network Actors in the Director: **Register a Pending Actor** or **Register an Actor that uses Push communication using a bulk registration token**.

Register a Pending Actor from the Director

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Actor in the Pending Actors table, expand the **Actions** menu and click **Connect to initiate a Director-to-Actor registration**.



Actor Action menu & Connect Actor form

4. Enter the Actor's *FQDN or IP address*.
5. (Optional) Clear the **Validate FQDN** checkbox.
   Clearing this checkbox allows you to register push Actors when DNS resolution is not possible due to your network setup.
6. Click **Connect**.
   - The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   - Once registration is complete, the Actor moves from the Pending Actors table to the Network Actors list.

Register an Actor using Bulk Registration Tokens

1. Launch the Director and sign in.
2. Select **Environment > Actors**.
3. Identify the Bulk Registration Token you want to use to register the Actor, expand the **Actions** menu and click **Register Push**.
4. Populate the Register Push Actor form and then click **Submit**.
   - **Name:** The default name of the Actor is the name of the token with a numeral appended.
   - **Description:** Short description of the Actor
   - **Mgmt IP or FQDN:** The IP address or fully qualified domain name of the Actor.
   - **Actor Time:** Select **Use System Time** or **Use NTP Server(s)**.
   - (Optional) **Enable Network Keepalive**
5. The message "Actor '*actor name*' is being registered and will update automatically below" displays.
   Once registration is complete, the Actor moves from the Pending section under the bulk token to the Network Actors list.