Mandiant

WINDOWS ACTOR INSTALLATION

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

- Easy Install
- UI
- API

Easy

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

1. **Prerequisites**
2. **Create a Bulk Registration Token**
3. **Install and register a Windows Actor**

Prerequisites

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

Create a Bulk Registration Token

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

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

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

    b. **Security Zone:** The security zone for the Actors.
    c. **Expiration Date:** The date the token is no longer valid.
    d. **Max Uses:** The number of times the token can be used. This value cannot exceed the number of available Actors allowed by your license.

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

Install and register a Windows Actor

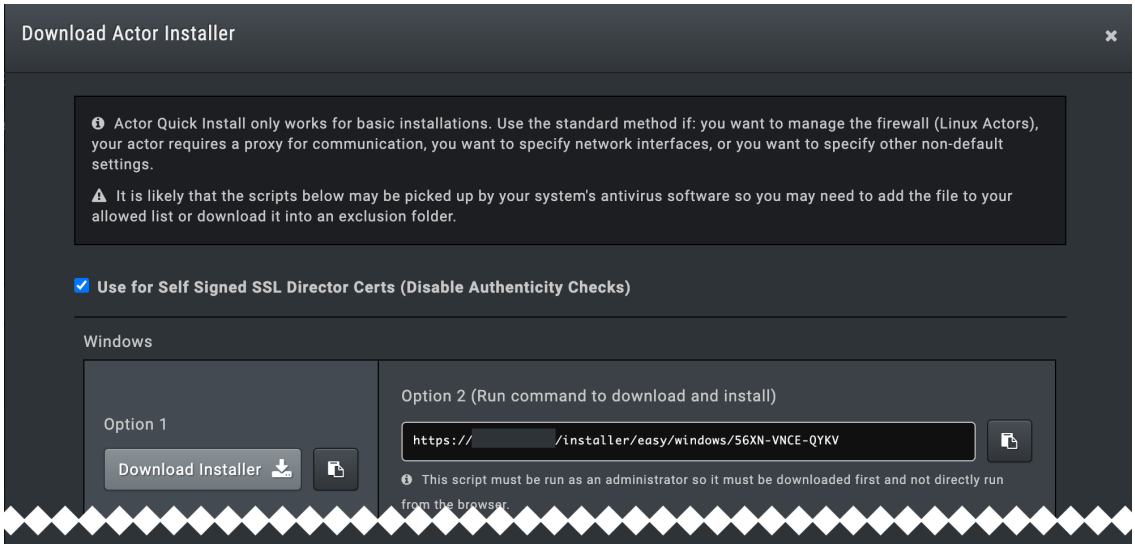
There are several ways to use the bulk registration code to complete installation. The most common use case is included here. After this completes, you have a registered Windows Actor that is configured with Pull Comm mode and Auto Interface enabled. The TAP driver is not installed, so do not use this method if you want to run DNS/ICMP tunneling Actions.

1. Connect to the Windows system using an admin account.
2. Launch the Director & sign in.
3. Select **Environment > Actors**.

4. Locate the token you want to use in the **Bulk Registration Tokens** table and click **Installer** Installer .
5. Select or clear the **Use for Self Signed SSL Director Certs**.

> Clearing this option will mean the install will not verify the certificate during registration and subsequently will not verify the cert when the Actor reaches out to the Director (HTTPS requests).

6. In the **Windows** section, click **Download Installer**. This downloads a zip file that includes the actor_install.bat and the Windows Actor installers.



Installer window for Windows Bulk Registration Token

7. Decompress the zip file.

> If you have Windows 10, you can decompress the zip file from the command line as part of the next step using the `tar` command.

8. Launch the Command Prompt as an Administrator.
9. Navigate to your download location and run actor_install.bat. Examples commands are provided below. The second set of examples is only for Windows 10. The installer automatically chooses the correct version (32- or 64-bit).

```
> cd C:\Users\Username\Downloads\MSVActorInstaller
> actor_install.bat
```

> If your security controls flag the `actor_install.bat` file, contact your security team, and if necessary, add it to the Allow list or Block list.

Windows 10 commands:

```
> cd C:\Users\Username\Downloads
> tar -xf MSVActorInstaller.zip
> MSVActorInstaller\actor_install.bat
```

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

During the installation, the Service Startup Timeout field is configured to 600 seconds and adds the following new registry key, which has a timeout value in milliseconds: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout`. Until you reboot the Actor, which also reboots the OS, the services start up time remains the Windows default of 30 seconds. If you have a slow Windows environment, we recommend rebooting the Actor before running Actions. For information on how to update this field in the future, see **Editing an Actor (https://docs.mandiant.com/home/msv-editing-an-actor)**.

UI

This is the most detailed installation method, using interactive elements when available. Steps include:

1. **Add the Endpoint Actor Configuration to the Director**
2. **Install the Windows Actor using the Setup Wizard**
3. **Registering the Endpoint Actor**

After installation is complete, we recommend you **Confirm Actor-Director Communication (https://docs.mandiant.com/home/msv-confirming-actor-director-communication)**.

Add the Endpoint Actor Configuration to the Director

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

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

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

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

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

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

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

An Actor can be used as an intermediate proxy in cases of network segmentation policies, where an Actor would not otherwise be reachable by the Director.
For example, given Actor A, which is connected to the Director, and Actor B, which is in a remote network segment, when setting up Actor B, select Actor A in the Proxy Through Actor field.

g. **Location [Local/Cloud]:** The Actor's location; specified as local or within the Cloud (Amazon Web Services or Azure).
h. **Pull Interval:** The time interval (in seconds) between pull attempts between the Actor and the Director.

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

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

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

Create a Bulk Registration Token

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

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

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

   b. **Security Zone:** The security zone for the Actors.
   c. **Expiration Date:** The date the token is no longer valid.
   d. **Max Uses:** The number of times the token can be used. This value cannot exceed the number of available Actors allowed by your license.

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

Install the Windows Actor using the Setup Wizard

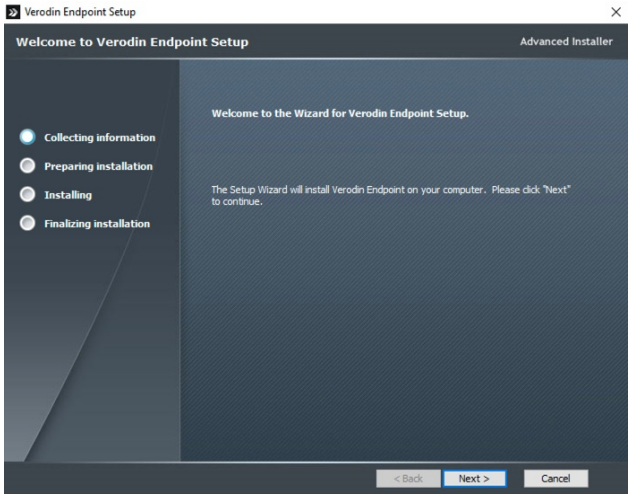
1. Add the Actor executable to the host.
   - **Option 1**: If you have access to the internet on the host:
     1. Launch the Director.

2. Select **Library > Actor Installer Files**.
3. Download the 32-bit (x86) or 64-bit Endpoint Actor install file, as needed.

> **NOTE:** The latest versions of the installer are automatically added to the Actor Installer Files Library if the Director is used for system updates.

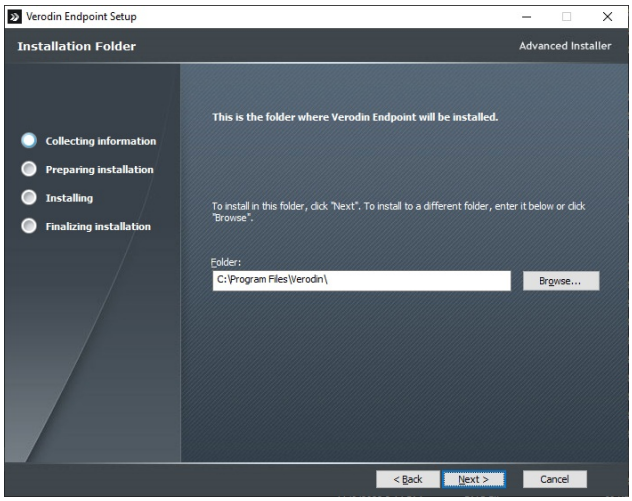
- **Option 2**: Download the Windows Actor install file from the Customer portal and copy it onto the host.

2. Run the Validation Platform Windows Actor executable.
   a. Navigate to the file location.
   b. Right-click on the file (`VerodinEndpoint_[version].exe`) and select **Run as Administrator**.
   c. If a User Account Control popup appears, click **Yes**.
3. The Setup Wizard launches; click **Next**.



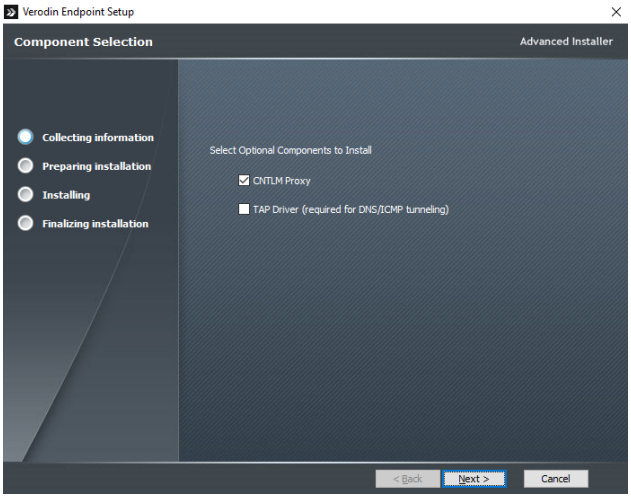
Start of Install process

4. (Optional) Change the default location if you prefer to install the Windows Actor in a different folder or drive.



Location of installation

5. (Optional) Select or clear the checkboxes for the optional components and click **Next**.
    - **CNTLM Proxy** installs an executable that is used when/if you configure communications from the Actor using NTLM proxy with a config file. This is selected by default.
    - **TAP Driver** is a driver that is required if you want to run DNS tunneling Actions. This is not selected by default. It is NOT required for Validation on Demand.

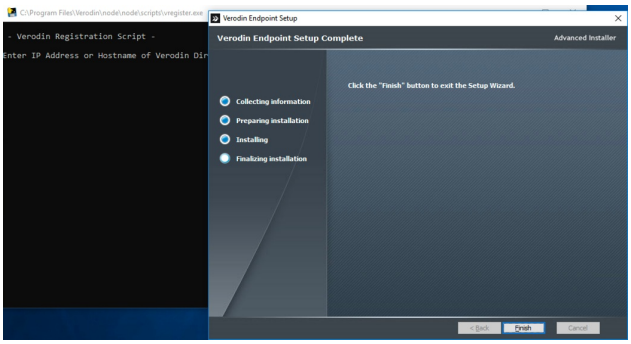


Windows Component selection

6. On the **Ready to Install** screen, click **Install**. The Setup Wizard installs the Validation Platform Endpoint Agent.

> **NOTE:** A **Security Validation Credential Provider** is installed but is only used in Protected Theater. This allows the Actor to use Microsoft Windows user accounts when running Actions and save screenshots of what occurs when the Action is run.

7. Click **Finish** on the Setup Complete screen. This will close the Setup Wizard and you'll see the Actor registration command prompt.



Install complete

Register the Endpoint Actor

When you use the install wizard, the registration starts automatically after the installation completes.

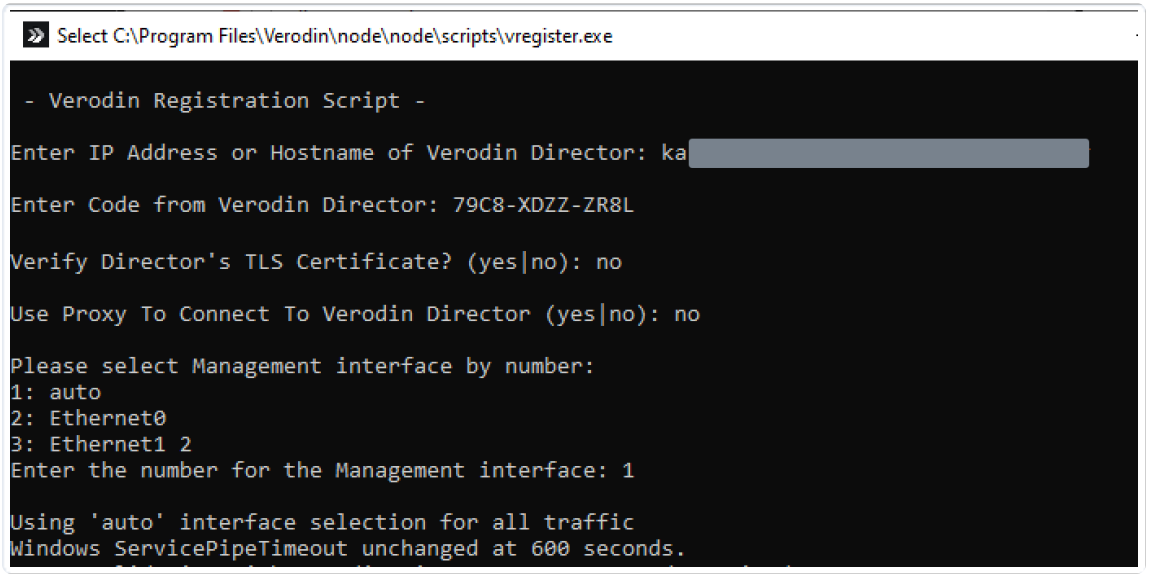
1. When installation completes, the registration command prompt automatically opens. Enter the requested information.

> The final screen of the install wizard and the command prompt might both be open at the same time.

a. The Director's *FQDN or IP address*
b. 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
c. Verify the Director's TLS Certificate. When set to Yes, the certificate is verified during registration and then every time the Actor reaches out to the Director (HTTPS requests).
d. Optional: Add a proxy.
   i. Enter **Yes.**
   ii. Enter the *Proxy IP* and *Proxy Port*.
   iii. If there is an account associated with the proxy, enter *the account info*.
e. Configure your interfaces. You can directly assign the interface or you can choose to have it auto select the interface when running security content.

   > VPN and PPP interfaces are available for selection.

   - If networking for the computer changes frequently, we suggest you use **auto**. When you choose **auto**, the platform selects the interface when you run security content.
   - If you have one available interface and you don't choose auto, the installer automatically assigns the interface to be used for both Management and Testing.
   - If you have multiple available interfaces and do not choose auto, you must select the interface to be used, first for the Management interface and then for the Test interface.
f. After selecting the interfaces, the installer validates the information and finalizes the registration.

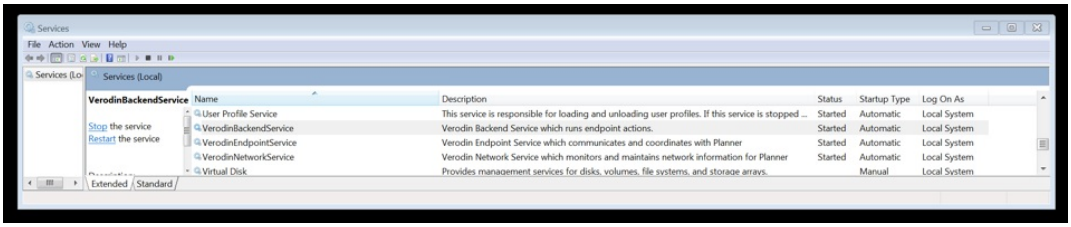


Registration script sample

2. For a Windows Actor or a Windows Protected Actor to work, its services must be running. Validate the following Security Validation services are running on the host:

- VerodinEndpointService
- VerodinBackendService
- VerodinNetworkService

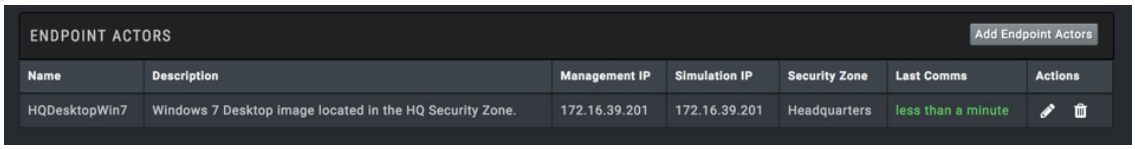
a. From the run/search bar (you may need to open the Start menu), type **services** and select **Services**.
b. Locate the services and if they are not Running, click on them one at a time and choose **Start** and **OK**.



Security Validation Windows Services running

If the services did not or will not start, you may need to add them to your Allow list. After updating your Allow list, try to start the services again. If you need help with this process, or if the services still aren't running after you've completed the steps, **contact support (https://docs.mandiant.com/home/customer-support)**.

3. Verify the Actor is registered and is no longer in the Pending Actors table.
   a. Launch the Director.
   b. Select **Environment > Actors**.
   c. Verify the Actor is now appearing in the Endpoint Actors table.



Actor Registration in the Director

During the installation, the Service Startup Timeout field is configured to 600 seconds and adds the following new registry key, which has a timeout value in milliseconds: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout`. Until you reboot the Actor, which also reboots the OS, the services start up time will remain the Windows default of 30 seconds. If you have a slow Windows environment, we recommend rebooting the Actor before running Actions. For information on how to update this field in the future, see **Editing an Actor (https://docs.mandiant.com/home/msv-editing-an-actor)**.

Troubleshooting registration

Some Windows environments have various interface configurations that might not be supported with the Actors registration script. In these cases, manual configuration of the `node_settings.conf` file might be required:

1. Edit the following file: `/opt/apps/verodin/node/settings/node_settings.conf`

```
primary_nic = Ethernet [X]
primary_ip = <IPV4_Address>
primary_auto = false
```

Where:

- *X* is the value of the ethernet interface.
- *IPV4_Address* is the static IP address of the Actor that you're trying to register.

2. Save the file and then rerun `vregister`. Select the primary NIC value (`Ethernet [X]`) for the Management interface.

API

Installing the Windows Actor can be automated to some degree. Steps include:

1. **Add the Actor Configuration - API**
2. **Install and register the Windows Actor from the Command Line**

Add 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.

Install and register the Windows Actor from the Command Line

The Windows Actor can be installed completely from the command line. You must have admin permissions to run the install this way.

1. Transfer the install.exe file to the Windows System.
2. Install the Actor, or Install and Register the Actor. You can run the install and registration separately or combined. Several examples are provided.
   For a full list of available arguments, see **vregister arguments explained**.

   > The default installation path is C:\Program Files\Verodin, but you can override this using the alternate path installation example below.

   - **Standard install**:

     "C:*path*\VerodinEndpoint-*[version#]*.exe" /qn

     If you want to run DNS/ICMP tunneling Actions, include `TAPDRIVER="True"`, which will install the required driver.
     For example:

     "C:\Users\%USERNAME%\Desktop\VerodinEndpoint-4.10.0.0.exe" TAPDRIVER="True" /qn

   - **Installation to an alternate path and/or drive**

     C:*path*\VerodinEndpoint-*[version#]*.exe TAPDRIVER="True" /qn VREGISTER_ARGS="*Director_IP register_code* no --mgmt-interface *interface name* --no-tls-verify" APPDIR=*Drive:\Path*

     You can use the `APPDIR` property to override the default install path (C:\Program Files\Verodin), which can be useful when installing silently via `/qn`. You can also change the default drive if you want to install the Windows Actor somewhere aside from C:\.
     For example:

     C:\Users\%USERNAME%\Desktop\VerodinEndpoint-4.10.0.0.exe TAPDRIVER="True" /qn VREGISTER_ARGS="10.10.10.10 MZZ8-8JJH-CJ48 no --mgmt-interface Ethernet0 --no-tls-verify" APPDIR=D:\MyPath

   - **Installation and registration with auto interface selection and no proxy**:

"C:*path*\VerodinEndpoint-*version#*.exe" TAPDRIVER="True" /qn VREGISTER_ARGS="*Director IP register_code* no --mgmt-interface *interface name*"

For example:

"C:\Users\%USERNAME%\Desktop\VerodinEndpoint-4.10.0.0.exe" /qn VREGISTER_ARGS="10.10.10.10 MZZ8-8JJH-CJ48 no --mgmt-interface auto"

- **Installation and registration not using auto interface selection and no proxy** :

"C:\Users\%USERNAME%\Desktop\VerodinEndpoint-*[version#]*.exe" TAPDRIVER="True" /qn VREGISTER_ARGS="*Director IP register_code* no --mgmt-interface *interface* --test-interface *interface name*"

For example:

"C:\Users\%USERNAME%\Desktop\VerodinEndpoint-4.10.0.0.exe" TAPDRIVER="True" /qn VREGISTER_ARGS="10.10.10.10 MZZ8-8JJH-CJ48 no --mgmt-interface Ethernet0"

- **Installation and registration not using auto interface selection and using a proxy** (all proxy arguments included to show expected order):

"C:\Users\%USERNAME%\Desktop\VerodinEndpoint-*version#*.exe" TAPDRIVER="True" /qn VREGISTER_ARGS="*Director IP register_code* no --mgmt-interface *interface name* --test-interface *interface name* --proxy-authtype *authtype* --proxy-user *user* --proxy-password *password* --proxy-host *host* --proxy-port *port* --proxy-ntlm-configfile *file* --proxy-kerberos-domain-controller *controller* --proxy-kerberos-realm *realm* --proxy-kerberos-fqdn *fqdn*"

For example:

"C:\Users\%USERNAME%\Desktop\VerodinEndpoint-4.10.0.0.exe" TAPDRIVER="True" /qn VREGISTER_ARGS="10.10.10.10 MZZ8-8JJH-CJ48 yes --proxy-authtype http --proxy-host 10.10.1.1"

3. If you did not register the Actor during installation, complete the registration. The command varies based on your network setup.
   - **Using auto interface selection and no proxy**:
     "C:\Program Files\Verodin\node\node\scripts\vregister.exe" *Director IP register_code* no --mgmt-interface auto
     For example:
     "C:\Program Files\Verodin\node\node\scripts\vregister.exe" 10.10.10.10 MZZ8-8JJH-CJ48 no --mgmt-interface auto

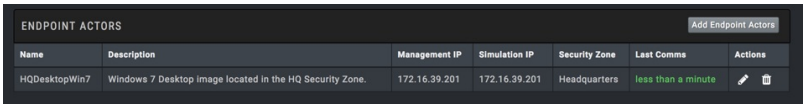
4. Validate that the required Validation Platform services are running.

```
sc query VerodinEndpointService
```

```
sc query VerodinBackendService
```

```
sc query VerodinNetworkService
```

5. Verify the Actor has registered and is no longer in the Pending Actors table.
   a. Launch the Director.
   b. Select **Environment > Actors**.
   c. Verify the Actor is now appearing in the Endpoint Actors table.



During the installation, the Service Startup Timeout field is configured to 600 seconds and adds the following new registry key, which has a timeout value in milliseconds: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout`. Until you reboot the Actor, which also reboots the OS, the services start up time will remain the Windows default of 30 seconds. If you have a slow Windows environment, we recommend rebooting the Actor before running Actions. For information on how to update this field in the future, see **Editing an Actor (https://docs.mandiant.com/home/msv-editing-an-actor)**.

vregister Arguments explained

- minimum `vregister` command:

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

- `vregister` with simple proxy configuration:

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

Positional arguments details:

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

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

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

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

- `--include-tap-adapters` : When included, you will see and be able to select existing TAP adapters for the management and test interfaces.
- `--proxy-authtype` : Values include `http, ntlm, kerberos`
- `--proxy-user`
- `--proxy-password`
- `--proxy-host`
- `--proxy-port`
- `--proxy-ntlm-configfile`
- `--proxy-kerberos-domain-controller`
- `--proxy-kerberos-realm`
- `--proxy-kerberos-fqdn`