Mandiant

INSTALL AND REGISTER A PROTECTED ACTOR

Once you have the host image added to the Protected Theater, you can install the Protected Actor. This process involves three steps:

1. Adding the Protected Actor configuration to the Director.
2. Installing the Protected Actor executable on the target host.
3. Registering the Protected Actor with the Director.

Adding the Protected Actor Configuration to the Director

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click **Add Protected Actor**; the Add Protected Actor form displays.
    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** (https://docs.mandiant.com/home/msv-running-bulk-actions).

    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.

    Endpoint Actors and Protected Theater Actors must use Pull mode.

        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.

    Only Actors that are in Push communication mode can proxy through another Actor. Therefore, Protected Theater Actors cannot proxy through another Actor.

    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. **Protected Theater**: Select the PT that you want to associate the Actor with.
4. Click **Submit**. The Protected Actor displays in the Pending Actors table and a code is generated. This code is used for registration.

The code generated is valid for 15 minutes only; if you don't complete the next step in that 15 minutes you will need to click **New Token** next to the Pending Actor to generate a new code.

Install & Register a Windows Protected Actor

Install the Protected Actor

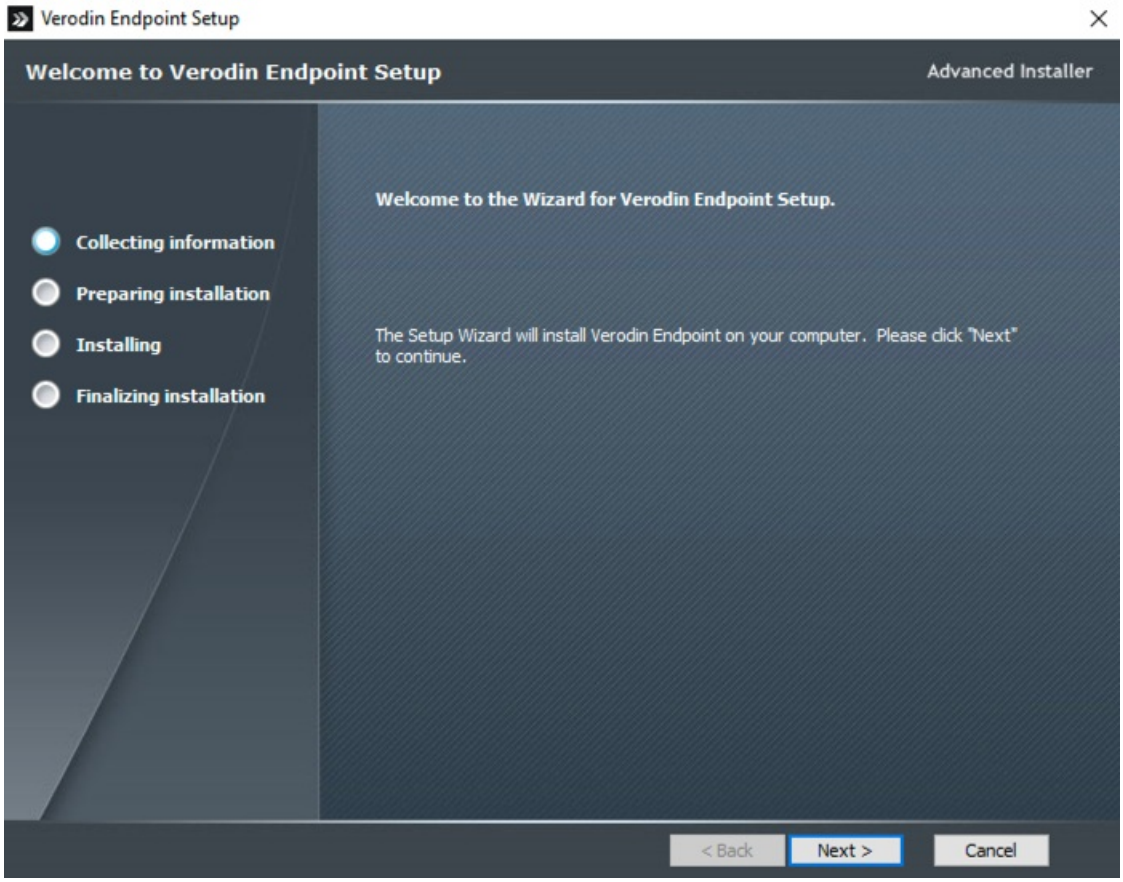
1. Add the Actor executable to the host.
    a. **Option 1**: If you have access to the internet on the host:
        i. Launch the Director.
        ii. Select **Library > Actor Installer Files**.
        iii. Download the Endpoint Actor install file.

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

    b. **Option 2**: Download the **Windows Actor install file (https://docs.mandiant.com/home/msv-actor-installers)** and copy it onto the host.

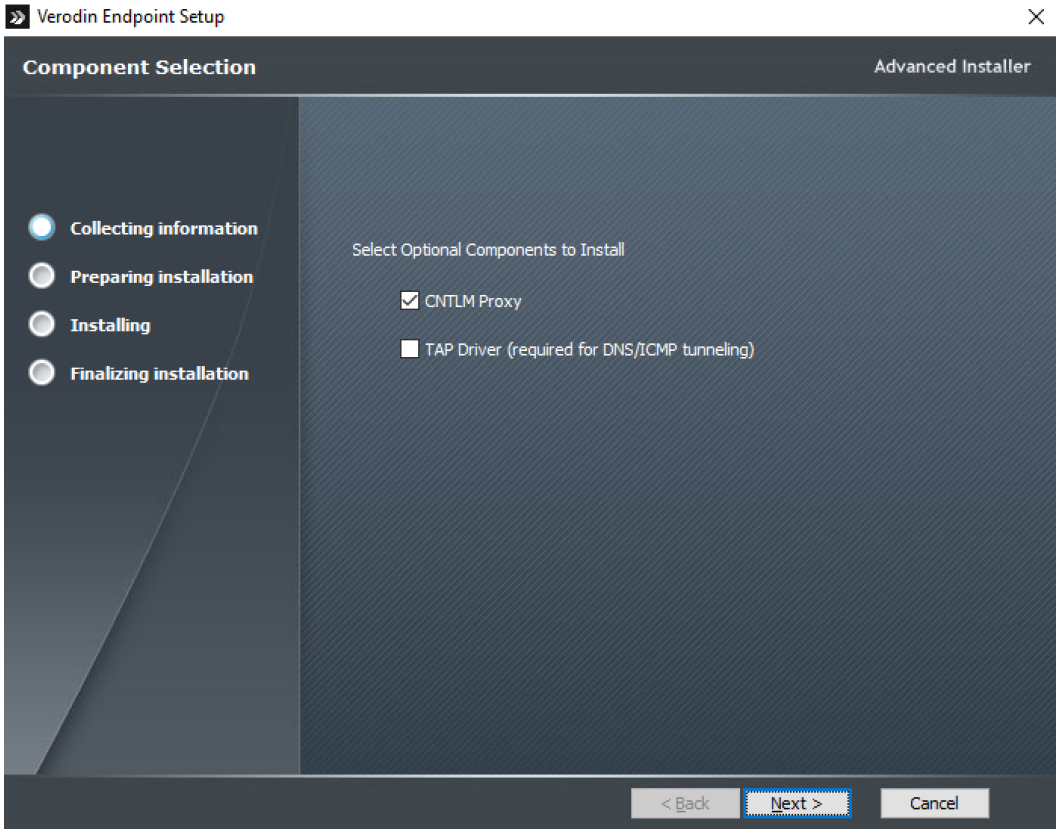
2. Run the Validation Platform Windows Actor executable.
    a. Navigate to the file location.
    b. Right-click on the file (the format will look similar to this, with the 4.9.2.0 replace with the current version: `VerodinEndpointInstaller_4.9.2.0.exe`) and select **Run as Administrator**.
    c. If a User Account Control popup appears, click **Yes**.

3. The Setup Wizard launches; click **Next**.



Start of Install process

4. (Optional) 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.

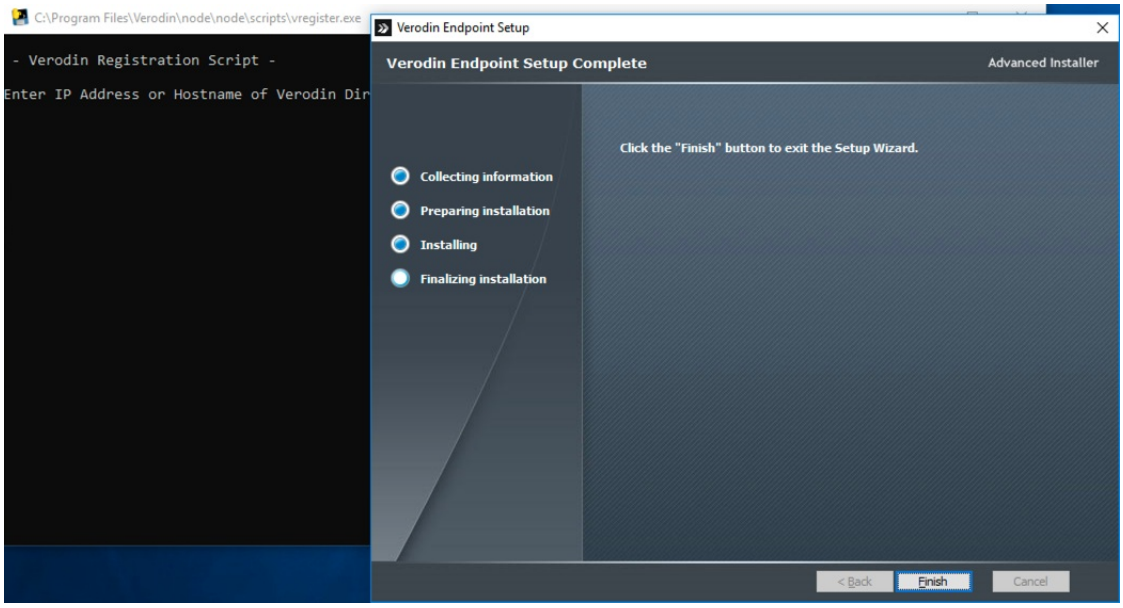


Windows Component selection

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

> A **Validation Platform 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.

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



Install complete

Registering the Protected Actor

The Actor Registration window displays automatically after the Actor installation completes. If you have closed that window, you can navigate to the registration script to run it:

```
C:\Program Files\Verodin\node\node\scripts\vregister
```

1. Enter the requested information:
    a. The *IP address for the Director*
    b. The *code* from the Protected Theater's Pending Actor table
    c. 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.

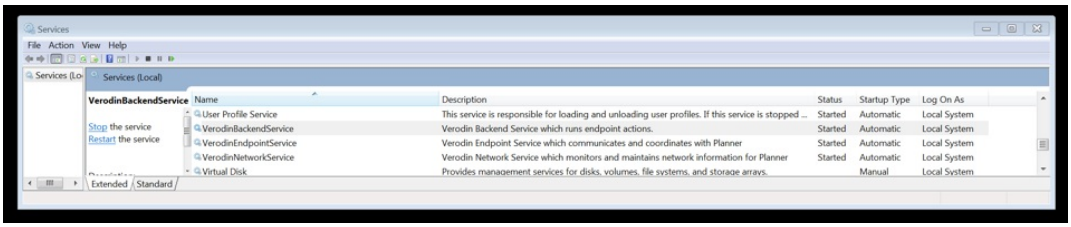
    d. Choose *a proxy option* (if applicable) for the Actor to use to communicate with the Director. The Actor will then complete registration. The command prompt closes when these steps complete.
2. Reboot the Protected Actor. This will finalize the registry changes made during the installation.

- The ServicePipeTimeout, which is tied to the Service Startup Timeout field, is configured to 600 seconds to allow adequate time for services to start when running Actions. By default, Windows has a 30 seconds timeframe, which is generally too short for running Protected Theater Actions. Rebooting the Actor, which reboots the OS, applies the 600 second setting. For information on how to update this, see **Editing Protected Theater or Protected Actor Settings** (https://docs.mandiant.com/home/msv-editing-protected-theater-or-protected-actor-settings).
- If you use Launch Console or Open VNC, communication between the Director and Protected Actor is automatically created, allowing you to register the Actor. If you do not use Launch Console or Open VNC, you need to created a communication rule that allows communication to the Director IP on port 443. See **Protected Theater Configurations** (https://docs.mandiant.com/home/msv-protected-theater-configurations#pt-comm-rule) for instructions.

3. Verify the Actor has registered and is no longer in the Pending Actors table.
   a. Launch the Director.
   b. Click **Environment** > **Protected Theaters**.
   c. Verify the Actor is listed in the Protected Actors table.

4. 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).

5. When you've verified Windows is configured correctly and the Actor is working, **create a snapshot** (https://docs.mandiant.com/home/msv-pt-snapshots) of the Actor.

Install & Register a Linux Protected Actor

A Linux Protected Actor often includes software dependencies. See **Handling Software Dependencies** (https://docs.mandiant.com/home/msv-handling-software-dependencies) for additional details. This is why the first step is setting up a Protected Dynamic Rule to allow communication as needed.

Create & Assign the required Protected Dynamic Rule

> The below is instructions if you are installing a Protected Actor on Ubuntu. You will need to do something similar for RHEL, with the sites based on the configuration of your Linux image.

1. Click **Environment** > **Protected Theaters**.
2. Click **Add Protected Dynamic Rule**.
3. Populate the form
    a. **Name**: Ubuntu archive
    b. **Domain**: us.archive.ubuntu.com
    c. **Protocol**: tcp
    d. **Destination Port**: 80
    e. **Refresh Rate**: 24
4. Click **Create Protected Rule**.
5. Click **Add Protected Rule Assignment**.
6. Populate the form:
    a. **Name**: Ubuntu archive
    b. **Protected Theaters**: Select one or more Protected Theater that needs the communication
    c. **Protected Actor**: Do not select anything
    d. **Protected Rules**: Select Dynamic: ubuntu archive (the rule you created in steps 2-4 above).
7. Click **Create Protected Rule Assignments**. You now have the necessary communication enabled to install the Ubuntu Actor.

Install & Register the Protected Actor

For full installation instructions, see the appropriate installation documentation. The changes to the install that you must remember are:

- The PT Actor should be installed to run as root.
- Any in-platform steps are completed from the **Environment > Protected Theater** page and not the **Environment > Actor** page.
- The Actor must be installed in Pull mode.

Post-Install Verification & Cleanup

Once the Actor is installed, complete the following steps:

- **Verify Linux Actor Configuration after Installation** (https://docs.mandiant.com/home/msv-verify-linux-actor-configuration-after-installation)
- Remove the Protected Dynamic Rules you configured
- Reboot the Protected Theater and **create a snapshot** (https://docs.mandiant.com/home/msv-pt-snapshots) of the Actor.