Mandiant

REGISTER THE WINDOWS ENDPOINT ACTOR

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

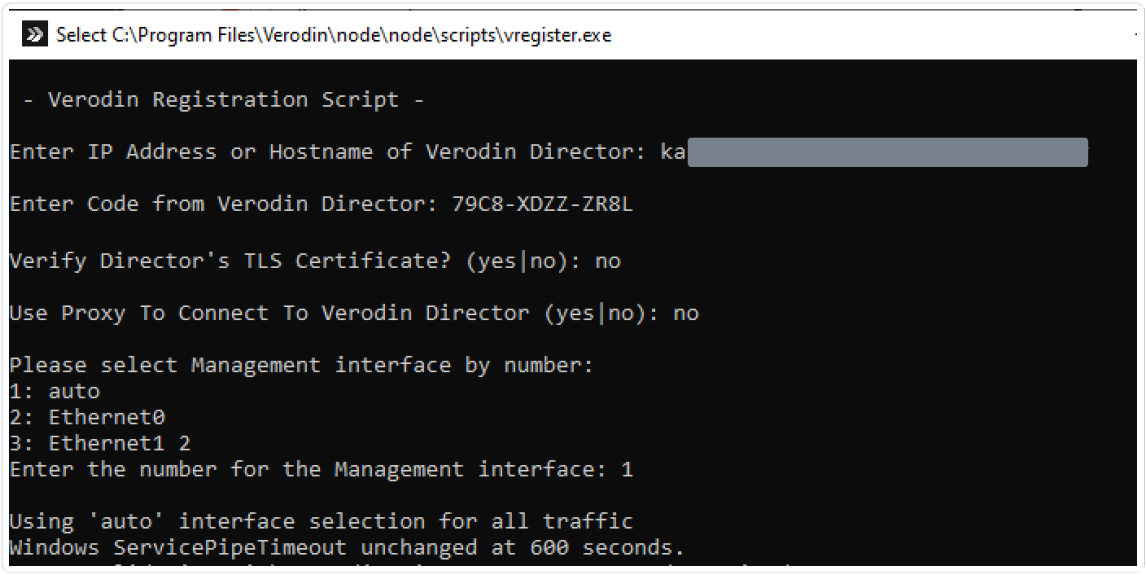
1. When installation completes, the registration command prompt automatically opens. Enter the requested information.

   > 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.

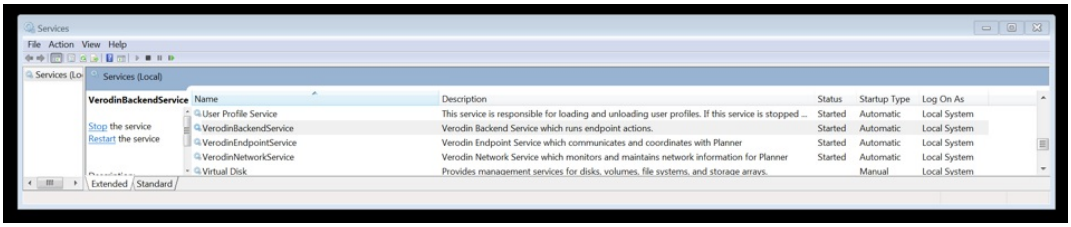
      - If networking for the computer changes frequently, we suggest you use **auto**. When you choose **auto**, the platform selects the interface when you run security content.
      - If you have one available interface and you don't choose auto, the installer automatically assigns the interface to be 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

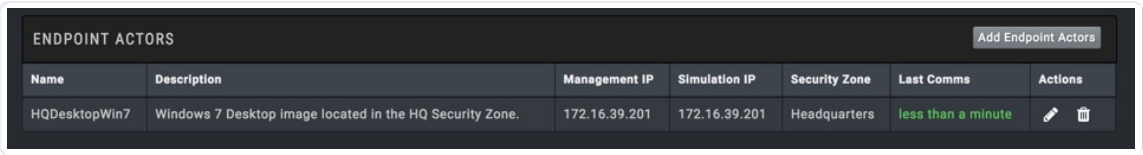
    a. From the run/search bar (you may need to open the Start menu), type **services** and select **Services**.
    b. Locate the services and if they are not Running, click on them one at a time and choose **Start** and **OK**.



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.