Mandiant

EASY ACTOR INSTALLATION

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

Prerequisites for Security Validation

- You have configured / deployed the operating system
- Your Actor does not need a proxy for communication
- You do not need to select Interfaces
- The Validation Platform can manage the firewall configuration (Linux Actors)

There are also some OS specific requirements:

- Redhat & CentOS
  - 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 (this is 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   c. **Expiration Date:** The date the token is no longer valid.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.

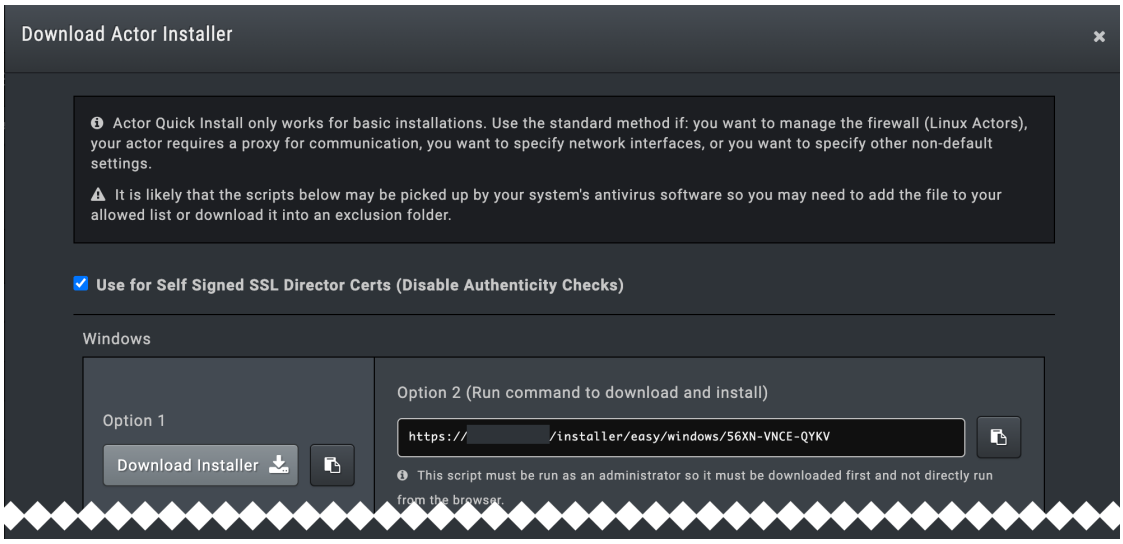
Install and register a Windows Actor

There are several ways to use the bulk registration code to complete installation. The most common use case is included here. When 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**.
5. Select or clear the **Use for Self Signed SSL Director Certs**.

> Clearing this option means the install does not verify the certificate during registration and subsequently does not verify the cert when the Actor 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. The following are examples commands and 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.

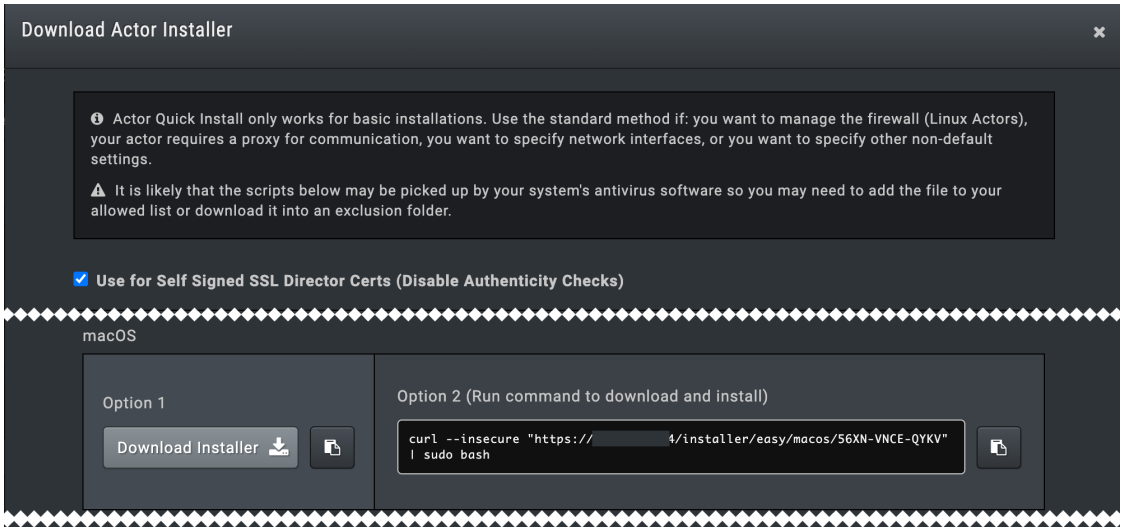
During the installation, the Service Startup Timeout field is configured to 600 seconds and adds the following new registry key, which has a timeout value in milliseconds: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServicesPipeTimeout`. Until you reboot the Actor, which also reboots the OS, 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)**.

Install and register a Mac Actor

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

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

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



Installer window for MacOS Bulk Registration Token

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

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

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

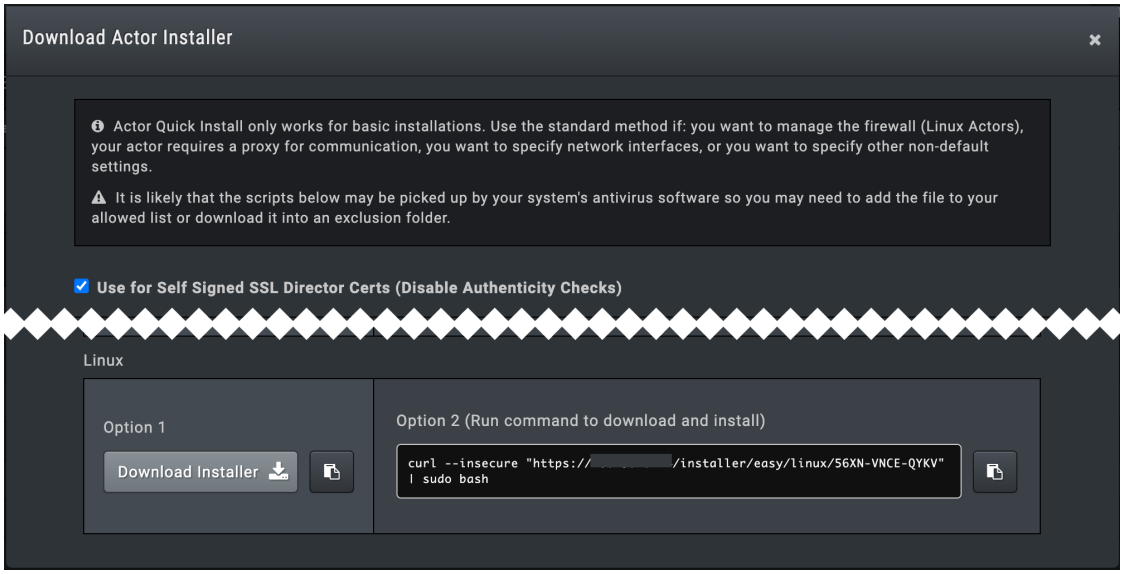
The Actor installs and registers. When it completes, the Actor is listed in the **Endpoint Actors** table.

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. When this completes, you have a registered Linux Actor that is configured with Pull Comm mode and management and test interfaces configured to use the network interface associated with the default route.

1. Launch the Director & sign in.
2. Select **Environment > Actors**.
3. Locate the token 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**.

   NOTE: Clearing this option means the install does not verify the certificate during registration and subsequently does not verify the cert when the Actor reaches out 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 and CentOS.