Mandiant

ADD HOST COMMAND LINE INTERFACE ACTIONS

Validation Platform Endpoint Actors can process Actions that model behaviors run at a command line level for Windows, Linux, and Mac Operating Systems. This includes the following shells: cmd.exe, PowerShell 2.0+, Python, and Bash.

When creating Host CLI Actions, keep in mind the following options and limitations:

- Commands contained in Host CLI Actions can include leading and trailing whitespace.
- Commands contained in Host CLI Actions can include variables. When variables are included, the fields appear as Runtime parameters that must be populated when the Action is run. To add a variable, use the following format:

  ```
  {{v_variable}}
  ```

  - Spaces should not be included.
  - The field name will capitalize words and replace underscores with spaces, for example *target_main* becomes *Target Main*.

  > Variables can only be used with bash, cmd, and PowerShell.

- The name of the process that runs a Job is randomized (when using Action User Profiles to run Windows Actions) by enabling the **Host CLI Actions - Windows Randomize Executables** option in Advanced settings.
- The platform does not support non-UTF8 characters. If you add any non-UTF8 characters to an Action, they will be removed when you create the Action.
- Commands that use the redirect `>` character to populate a file MUST be run in a separate subshell. Host CLI command blocks must also be separated with a blank space. For example:

  ```
  cmd /C "echo. > Empty_File.txt"
  C:\Users\Public\Documents>,4,true,60
  success_zero

  cmd /C "type C:\Windows\System32\Calc.exe > Empty_File.txt:MaliciousCalc.exe"
  C:\Users\Public\Documents>,4,true,60
  success_zero
  ```

Protected Theater Actions (https://docs.mandiant.com/home/msv-adding-protected-theater-actions) are a special type of Host CLI Action that includes destructive behaviors. These Actions can include malicious files or be completely based on code, using one of the following shells: cmd.exe, PowerShell 2.0+, Python, and Bash.

TO CREATE A HOST CLI ACTION

1. Select **Library > Actions**.
2. Click **Add Action** and select **Host CLI**.
3. Select the **Action User Profile**. This could be the System Profile or a User Profile you defined (see **Action User Profiles** (https://docs.mandiant.com/home/msv-action-user-profiles) for more information).
4. Choose whether you want Require Interactive Session set to **On** or **Off**. The default value is **Off**, which causes the action to be run as a background process launched by the selected user. If **On** is selected, the designated user is logged into an interactive session to initiate the action manually. Interactive sessions may be required to run Host CLI commands that require window titles or to test certain security controls (for example, whether Zscaler is launched automatically upon user login).

   There is a default **Interactive Login Delay** of 30 seconds to allow for delays in launching windows, etc. To change this value, go to **Settings > Director Settings > Actor Settings** (see **Actor Communication Settings**

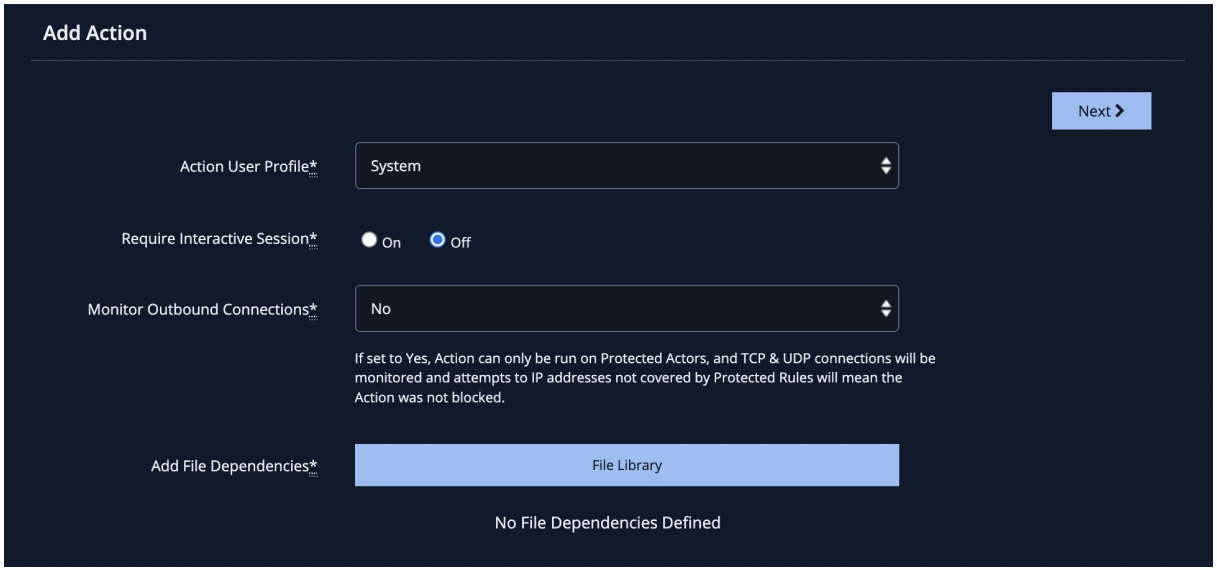
(https://docs.mandiant.com/home/msv-settings-actors).

> Initiating an Interactive Session will automatically log out any user(s) currently logged into the system.

> If the action has Require Interactive Session set to **On**, then the "require_run_as_interactive" attribute is forced to *true* AND when this action is run, the "Interactive Session" checkbox will be checked and not changeable.

- Select the **Monitor Outbound Connections** where
  a. Yes means the Action will only be available as a Protected Theater Action.
  b. No means the Action will be available for use on Endpoints.
- (Optional) Select a File to be used as File Dependencies.

> Files from the File Library will be listed. If you choose a file that is Restricted as Malicious, the Action will only be available as a Protected Theater Action.

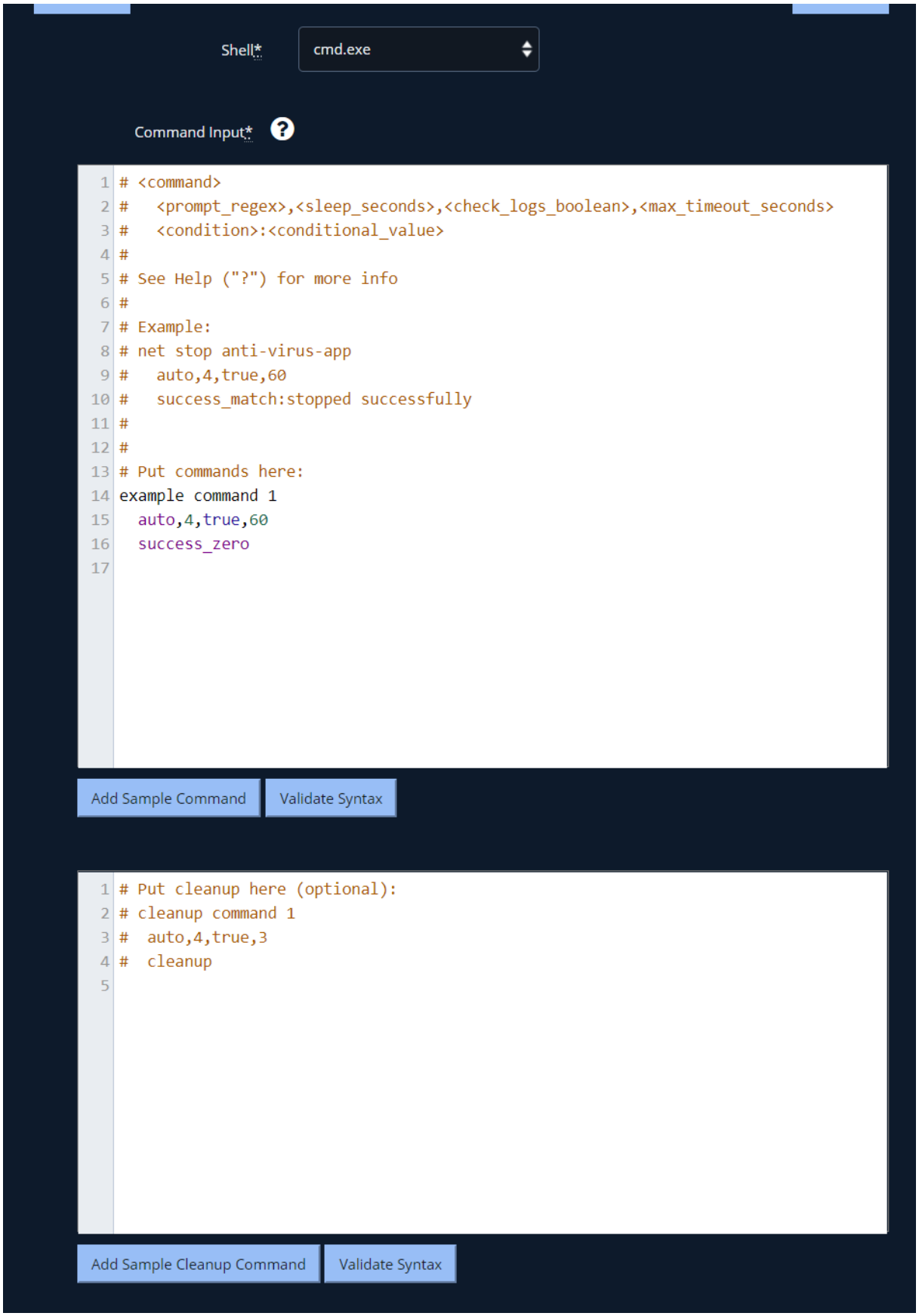


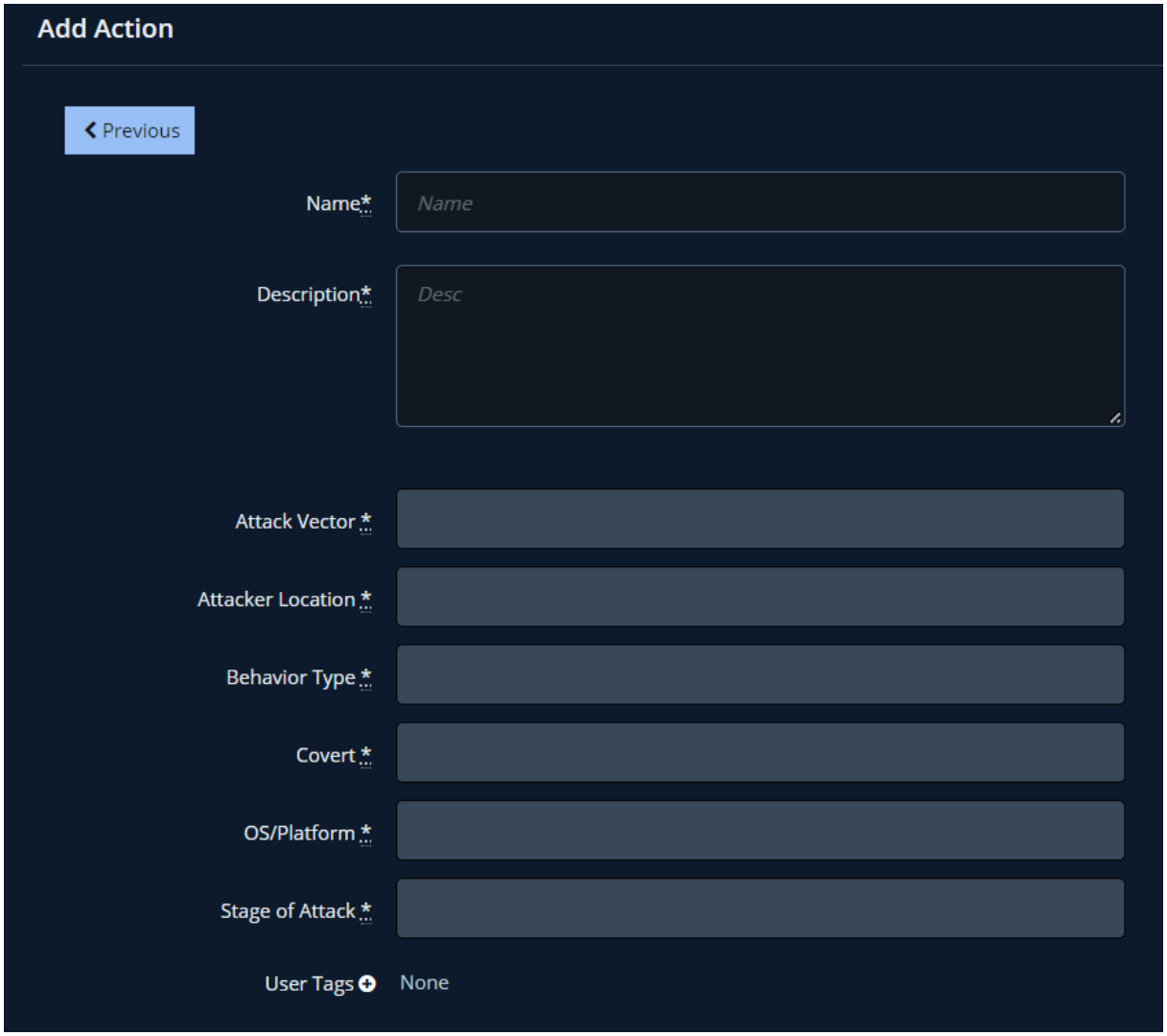
- Click **Next**.
- Select the **Shell**. Options include: cmd.exe, powershell.exe, python, and bash.

> You have the option to define and use a custom shell as a runtime parameter for Windows-only Host CLI Actions.

- Enter the **Command Input** & click **Next**. You can add commands for running the Action and then cleaning up after the Action has run.

> - Help with creating commands is available by clicking the **?** button.
> - When complete, the syntax of the command can be validated by clicking **Validate Syntax**.
> - If a command is to use a file dependency, you can call it by providing the path. Reviewing PT Actions created by the Validation Research Team (VRT) will provide additional details.



- Populate the Add Action form:
  a. Name
  b. Description
  c. Attack Vector
  d. Attacker Location
  e. Behavior Type
  f. Covert
  g. OS/Platform
  h. State of Attack
  i. (optional) User Tags
- 

Click **Save Action**. The Action is saved and the Action Library displays. Unlike when you create other Actions, the Action is not selected and displayed in the Action Preview because it must be approved before it will be available to run.

You can see the list of Actions that need to be approved by expanding the Content Source Dimension and selecting Pending Review.

Some users may be able to Approve Actions on creation. If that is the case, there will be a **Save and Require Protection** button, a **Save & Approve Anywhere** button (unless there is a Malicious File attached), and a **Save Action** button. If it is approved when you save it, the Action is selected and displayed in the Action preview.

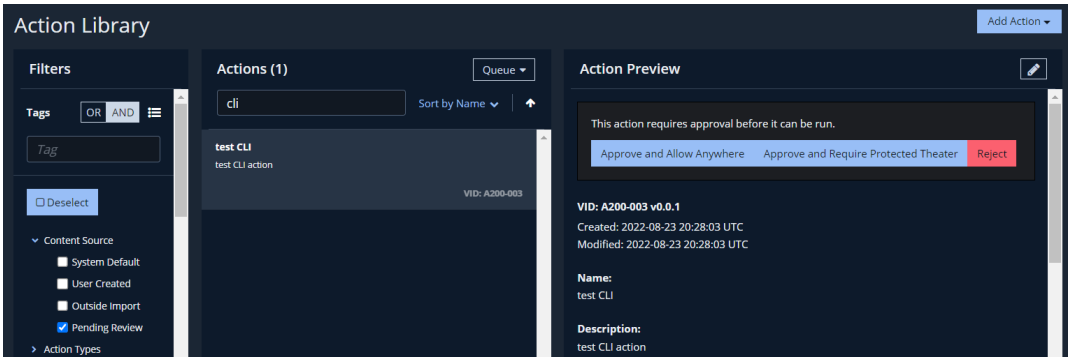
TO APPROVE A HOST CLI ACTION

The ability to approve Actions is controlled by user permissions. If you do not have the ability to Approve Actions and you should, contact your platform admin.

1. Select **Library > Actions**.
2. Expand the **Content Source** Dimension Filter and select **Pending Review**.
3. Select the Action.
4. Approve or Reject the Action.
    a. Click **Approve and Allow Anywhere** if it is a non-destructive behavior.

        This button will not appear if there is a malicious file attached.

    b. Click **Approve and Require Protected Theater** if it a destructive behavior.
    c. Click **Reject** if there is an issue with it.

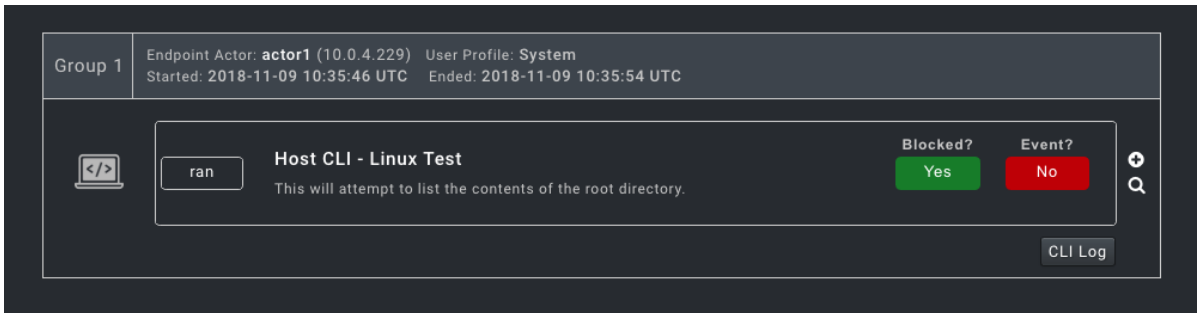


Approve or Reject Action

Bash Shell Host CLI Actions

You can create Bash Shell Host CLI Actions that are meant to run on Linux, using the Network Actors.

The Jobs page is slightly different than other Host CLI Actions. Screenshots are not available so there is not a screenshot button. However, you will be able to access the CLI log.



Mandiant

Bash shell Host CLI Action