RUN ACTIONS

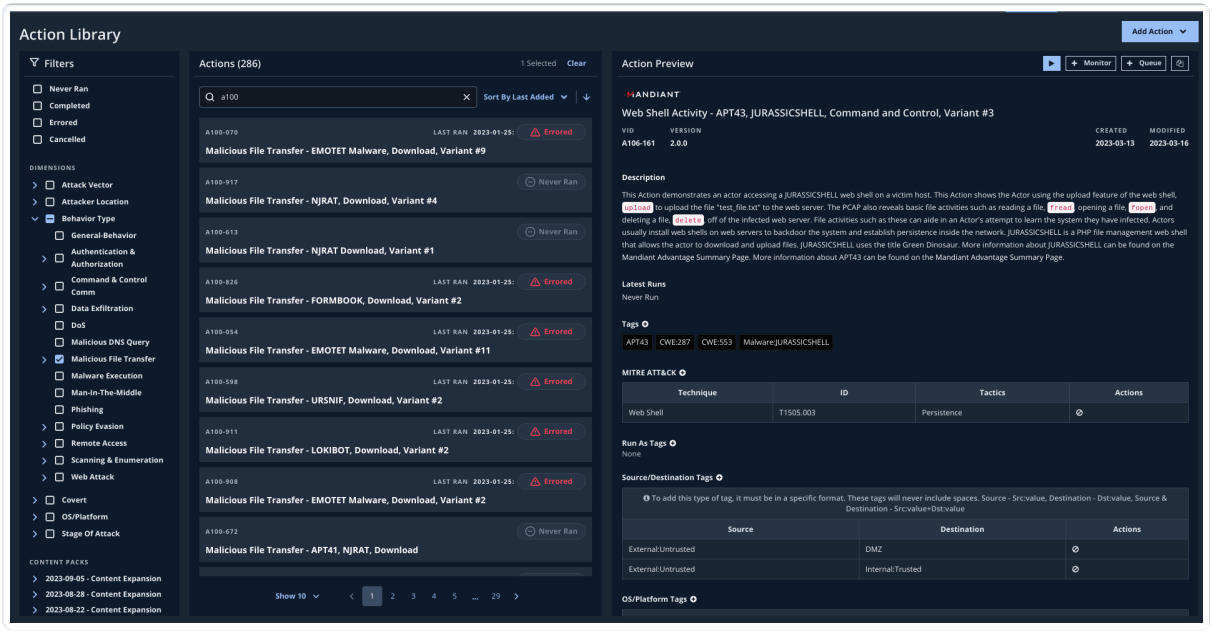
Actions are suspicious or malicious behaviors that are processed between or on Actors. Actions are designed to mimic attacker behaviors. Running Actions in your environment is a useful starting point, as they can help you understand how your environment responds to threats. As you run Actions, you can start to gather information to assess your security posture.

Action-specific prerequisites

- Before running **Captive Indicators of Compromise (IOC) Actions (https://docs.mandiant.com/home/msv-captive-ioc-actions)** to evaluate defensive performance related to blocking communication with publicly routable destination addresses for a Threat Actor, you must first configure safe URLs and communications rules. See **Captive IOC Actions Settings (https://docs.mandiant.com/home/msv-captive-ioc-actions-settings)** for more information.
- Before running **Malicious DNS Actions (https://docs.mandiant.com/home/msv-adding-malicious-dns-query-actions)** to test internal DNS capabilities (specifically the addition of known bad domains to your blocked list), you must add the DNS server you want to test to the Director and assign it to any Actors that are involved. See **Configuring DNS Settings (https://docs.mandiant.com/home/msv-dns-servers-settings)** for more information.

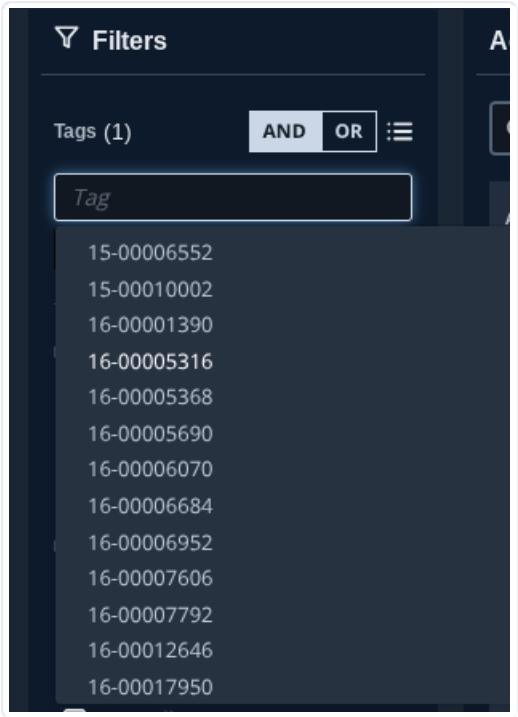
Run an Action

1. In the Director, go to **Library > Actions**. Filters appear next to the search.
   You can use the **Filters** (any mix of **Tags**, **Content Source**, **Last Run Status** with **AND**/**OR** operators), or search functionality to help identify the specific content that you want to run. You can use the **Sort By** option to reorder the results by **Name**, **VID**, **Modified**, **Last Added**, **Last Run**, or **Total Runs**.



The Action Library

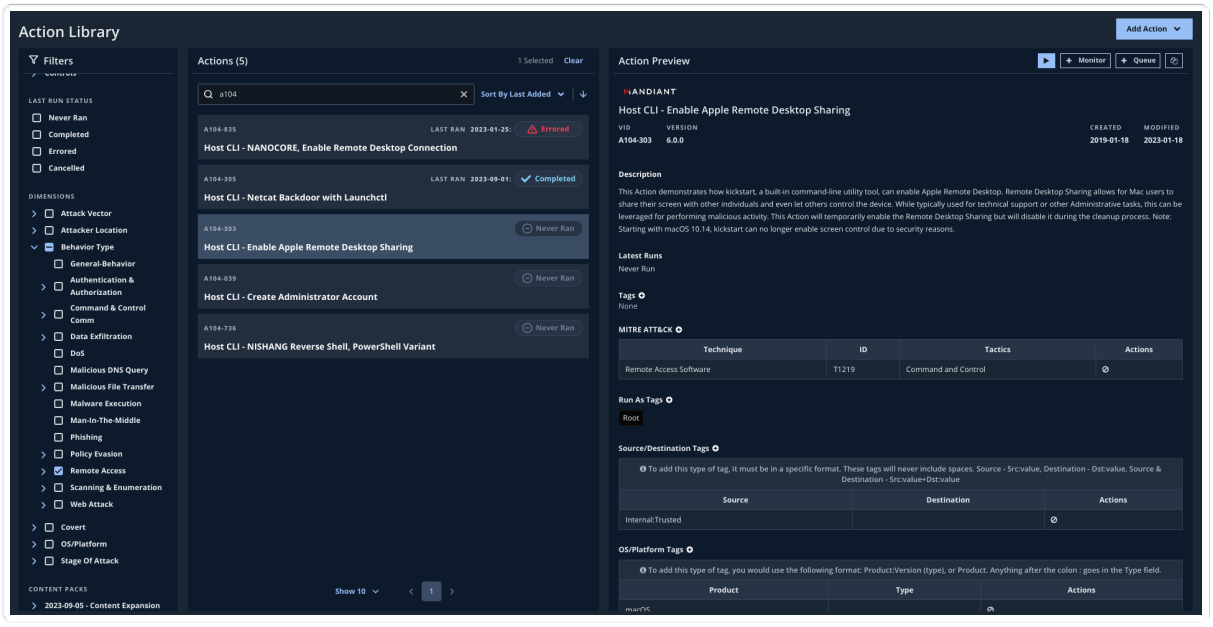
2. Optional: Refine search results by using the following steps:
   - From the Filters pane, add one or more tags. When you point to the field, some suggestions appear.



You can also click **Tags Available to the System** to see a list of Validation Tags and User Tags to choose from.

- Select one or more Filters. This changes the Actions pane to reflect the selections by using an AND operator, wherein the Action must match all top-level Dimensions. If you select sub-Dimensions, the Actions pane filters Actions with an OR operator, wherein the Action must match only one of the sub-Dimensions.
- Enter a search phrase, as needed, to further limit the results.

3. Click an Action in the Actions pane. The Action Preview pane is updated with information about the Action.



Action Library - Dimensions selected and Action Preview pane populated

4. Read the Action information to make sure it's a good match for the goal you're trying to accomplish.

5. Click ▷ **Run**. The **Select Actors** form appears.

   If your license includes TAAM, when running PCAP Actions with HTTP traffic, you can also click **Run as Captive IOC Action**.

6. Optional: Expand **Advanced options** and enter information as necessary:
   a. **Job name**: This information is displayed on the Job Status page instead of using the name of the security content and is displayed on the Job Details page.
   b. **Use interface type**: This field defaults to Test but can be changed to Monitor if you configured a separate interface for running Monitors.
   c. **Extra sleep time**: Enter, in seconds, additional time you want to wait before checking for events.

      This field only applies to Host CLI Actions. It should be used when your security technologies need more time to report their results after an Action is run.

7. Optional: Select the **Repeat Job** checkbox and configure the Repeat Job schedule. This schedule can be set for a time interval or a specific number of times.
8. Select a Source Actor.
   After choosing the Source Actor, the Destination Actor list automatically populates, showing Actors that the Source Actor can communicate with.

   - If you want to run tests between multiple Actors, you use the Tags option. For full details, see **Running Bulk Actions** (https://docs.mandiant.com/home/running-bulk-actions).
   - If you want the platform to automatically select the Actors, you use the Run Recommended option. This option also automatically selects all eligible users. For more details, see **Running Actions Based on Action Tags** (https://docs.mandiant.com/home/running-actions-based-on-action-tags).

9. Accept the prefilled Destination Actor or select a different one.

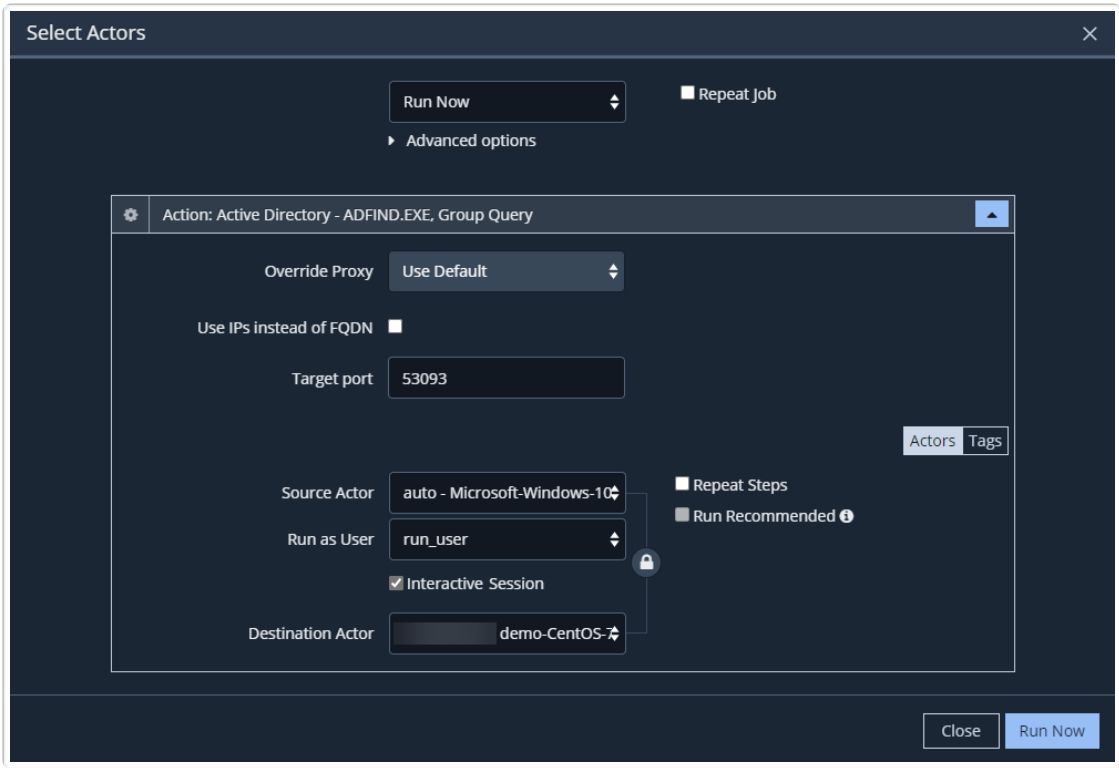
   You can click the Lock icon to enable all Actors, not just the ones that can communicate with the Source Actor.

10. Optional: If needed for the Action you're running, select a user profile from the **Run as User** menu and enable or disable **Interactive Session**.

    - Certain Actions (Network, DNS, Host CLI) can be run as a specified user, rather than the default system user. If you choose a Windows Actor as a source and run one of these Actions, you can choose a different user account under **Run as User** and specify whether this user should sign in using an **Interactive Session**.
    - The Interactive Session setting may already be checked by default, depending on the Action being run and your global Actor settings. When enabled, the selected user account can sign into the Windows Actor so that supported Actions can run. See **Actor Communication Settings** (https://docs.mandiant.com/home/msv-settings-actors) for more information on global default settings for Actors.
    - An interactive session supports certain Host CLI commands that won't run successfully without a desktop. This session is needed for Host CLI commands that need to get window titles.
    - An interactive session is required for testing certain security controls.

- An interactive session signs out anyone else who is currently using the Windows Actor system.
- On Windows Actors, non-System users may have insufficient privileges to run DNS tunneling actions.

See **Actions with Interactive Sessions** for more information.



Select Actors form with Run as User, Interactive Desktop Session, and expanded Runtime Parameters

11. Optional: If running a Captive IOC Action, and your Actor uses a Proxy, enter the **Captive IOC Proxy**.
12. Optional: Select ▾ to expand the Runtime Parameters view where you can set additional parameters, as needed. The parameters that display depend on the type of Action selected.
13. Optional: Select **Repeat Steps** and configure the Repeat Step schedule. This schedule can be set for a time interval or a specific number of times.

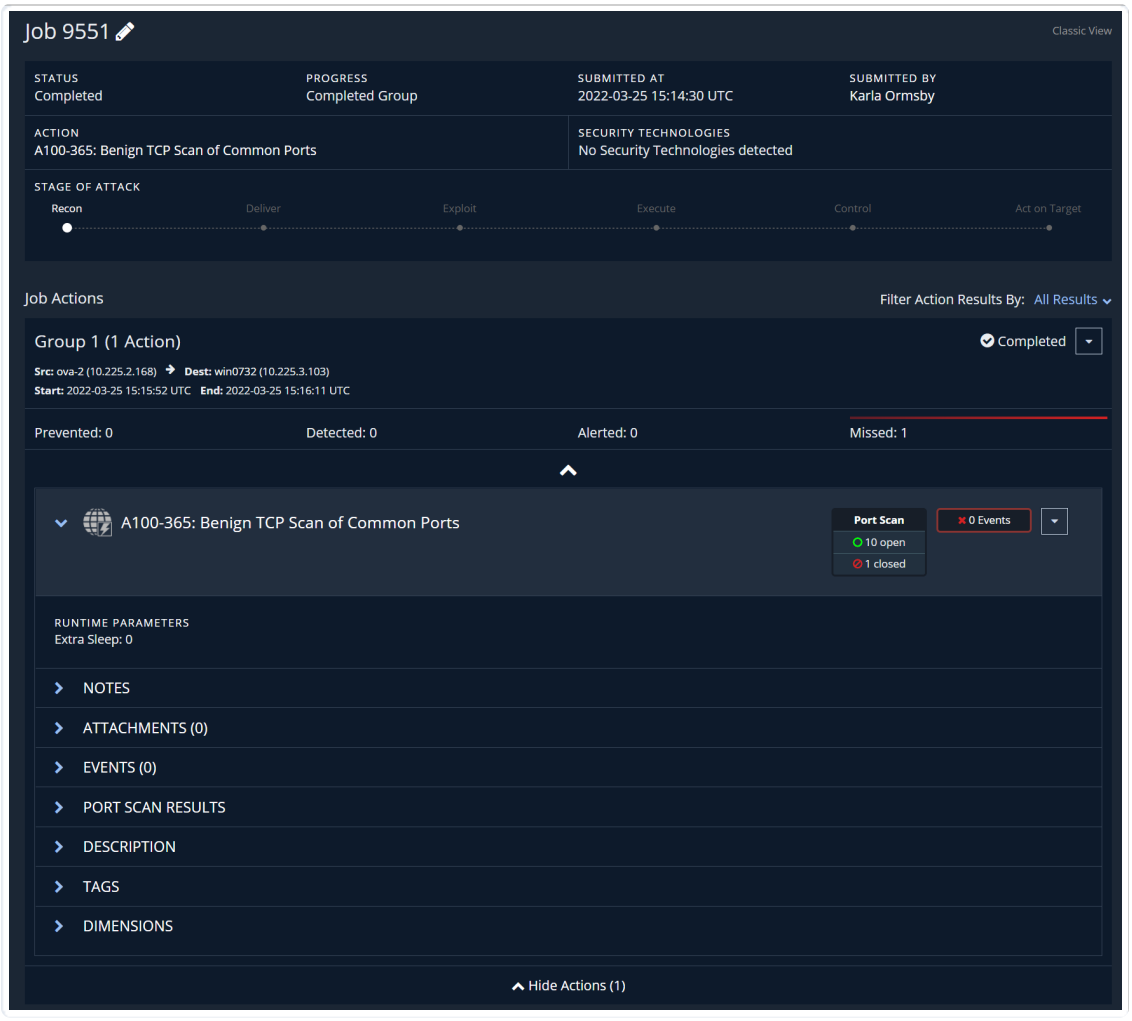
    - When configured, the Job does not complete until the Repeat Step has completed.
    - When an Action User's permissions in an Action User Profile are restricted by a Windows Group Policy Object (GPO) to prevent that user from launching a command (CMD) or PowerShell (PS) session, these Actions are reported as Blocked when initiated by that user.
    - For Host CLI Actions where a command times out, an error appears and any subsequent commands are skipped.

14. When you have the Job configured to your specifications, click **Run Now** or **Schedule** (varies based on whether a

schedule is selected).

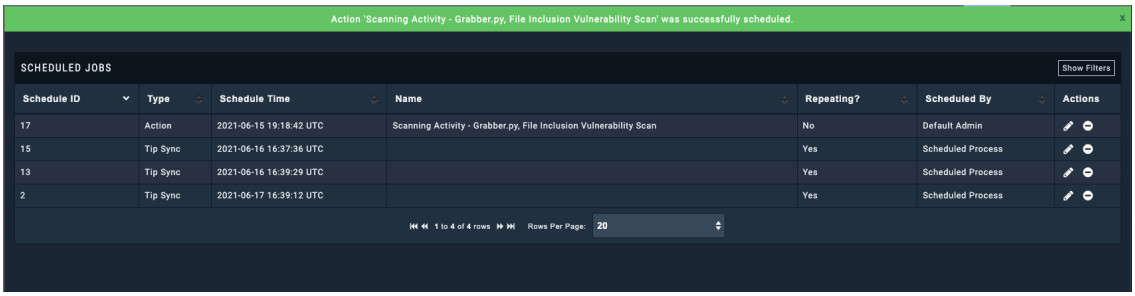
The **Job Results** page displays if you clicked **Run Now**.

- DNS Actions are marked as blocked if they time out during Job execution.
- Conversations between Source and Destination Actors are pulled when an Action is complete, which improves Integration event matching speed.
- When Actions are run, any Action destination ports are considered when completing event matching. This step allows traffic Drop messages from a Security Technology positioned between a proxy and the destination Actor to be matched.



Job Status page

The **Scheduled Jobs** page displays if you clicked **Schedule**.



Scheduled Jobs page

Additional information about Actions

As you become more familiar with running different Action types, see the following for more information:

Host CLI Actions

- If you're running a Host CLI Action and there is an issue with the user credential capabilities, you see the error "Actor does not support non-system users." Return to the previous step and select a user profile from **Run as User**.
- If a Host CLI Action contains variables, **Runtime Parameters** is expanded by default and you must enter values before you Run the Action.
- You can define and use a custom shell path as a runtime parameter for Windows-only Host CLI Actions.
- For Actions that require a file downloaded and then run in the Host CLI Actor memory, you can use a local web server to host and serve a file. The file can be safely requested for within the Host CLI Action that runs on that Actor. See **Host a File on a Local Web Server** **(https://docs.mandiant.com/home/msv-local-web-server-host-cli)** for more information.
- When French is both the Global language and the Actor's language, the French version of expected HOST CLI responses is used when Windows-based Host CLI Actions are run.
- MSV 4.14.6.0: For Windows Actors, you can configure a default path for Host CLI Actions. This setting (**Default Path for Host CLI Actions**) is available in the Director under **Settings > Director Settings > Advanced.**
    - This setting defines the default working directory used when launching Host CLI Actions on Windows Actors.
    - If left blank, the system defaults to using the user profile directory.
    - When running any Host CLI Action on Windows, a `Custom profile path` runtime parameter is available. This parameter automatically defaults to the value set in the **Default Path for Host CLI Actions** setting. You can override this value at runtime if needed.
    - Additionally, if a Host CLI Action includes a variable named `v_default_dir`, this variable also defaults to the value that is specified in the **Default Path for Host CLI Actions** setting.

Malicious File Transfer Actions

- The **User agent** field lets you define your own browser or client rather than the default user agent.
- **Path** refers to the path where the file is served from (the full URI for the file). By default, this value is blank.

Network Actions

- If you want to capture network traffic between Linux Actors, select **PCAP Capture Enable** to include a PCAP log in the Job results. The PCAP capture appears in the Job results. It lets you see what traffic is sent across the network (including proxy traffic) and is captured directly on the Actors while running the Action. The results can be used for troubleshooting and diagnostic purposes.
- For PCAP Capture to work between Linux Actors, tcpdump must be installed on the Linux Actors in either `/sbin/tcpdump` or `/usr/sbin/tcpdump` to enable capturing of network traffic.

Actions that require interactive sessions

This information only applies if you want to run Actions using a specific account on a Windows-based Actor. If not applicable, you can ignore this information.

By default, Actions are run as a background process. However, if the interactive sessions setting is enabled, the designated user is signed 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 a specific security techniology is launched automatically upon user sign in).

Interactive sessions require some additional configuration that the Actor automatically verifies. If any settings don't meet the criteria, the Actor returns an error message in the Job results and an `Interactive logon not supported on this host` error in the debug logs.

If the Actor is performing interactive logons, first verify the following settings on the Actor host system:

- CTRL+ALT+DEL requirement must be disabled.
- Legal Notice Caption must not be specified.
- Legal Notice Text must not be specified.

If any of the preceding conditions are present, the Actor is unable to sign in interactively as the specified user. For example, if CTRL+ALT+DEL is enabled, or a Legal Notice Caption/Text is configured, this requires manual intervention, and the user can't log on interactively.

Actions may not run if you use a Windows instance that is not activated. In some cases, an Activate Windows pop-up appears just after logging into the desktop; the `explorer.exe` session is blocked until the pop-up is manually cleared. For best results, ensure that Windows is activated on Actor endpoints.

See the following Microsoft documentation for more information:

- **Interactive logon: Do not require CTRL+ALT+DEL** (https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del)
- **Interactive logon: Message title for users attempting to log on** (https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-title-for-users-attempting-to-log-on)
- **Interactive logon: Message text for users attempting to log on** (https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on)

What to do next

This article covers the fundamentals of Actions. As you get more familiar with Actions, see the following documentation for specific use cases that you may be looking for:

- **Ransomware Defense Validation Actions** (https://docs.mandiant.com/home/msv-check-ransomware-exposure-rdv)
- **Cloud Validation Actions** (https://docs.mandiant.com/home/msv-test-cloud-controls)
- **Run Sequences** (https://docs.mandiant.com/home/msv-running-sequences)
- **Run Evaluations** (https://docs.mandiant.com/home/msv-running-evaluations)
- **Run Content from an Assessment** (https://docs.mandiant.com/home/msv-running-content-from-an-assessment)