Mandiant

RUN EVALUATIONS

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.

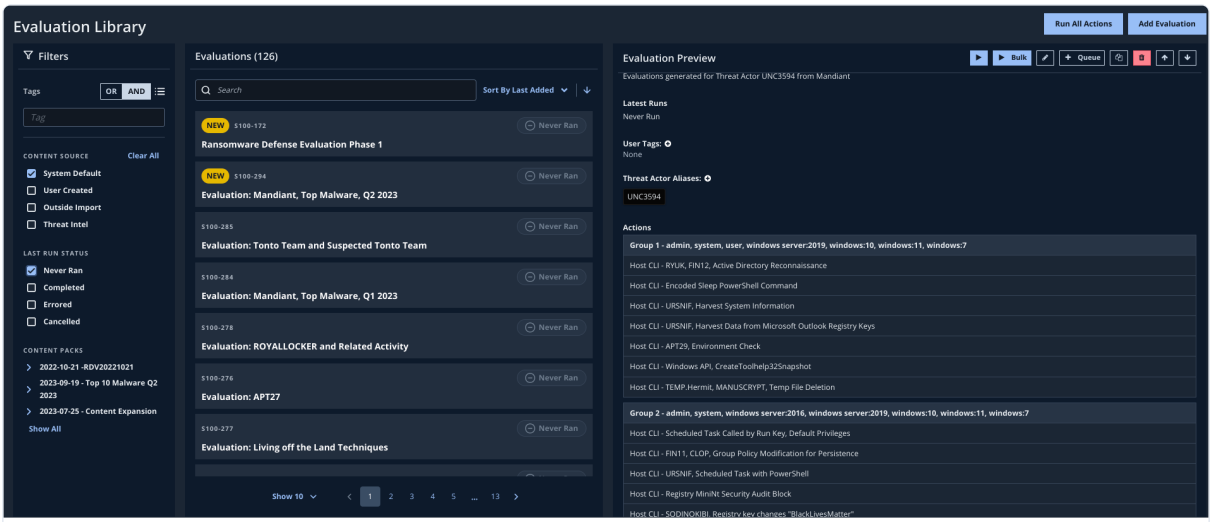
Actions may not run if you use a Windows instance that is not activated. In some cases, an Activate Windows pop-up appears just after logging into the desktop; the `explorer.exe` session is blocked until the pop-up is manually cleared. For best results, ensure that Windows is activated on Actor endpoints.

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)**

Run an Evaluation

1. Go to **Library** > **Evaluations**.
2. Select an **Evaluation**.
   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**.



Evaluations Library with Filters Applied

3. Click **Run** . The interactive Actor selection and Map appears.
4. Use the map to assign the Actors, going from Group to Group. For specific details on the functionality, see **Map - Running Sequences and Evaluations (https://docs.mandiant.com/home/map-running-sequences-and-evaluations)**.

> You can click **Run** to go to the Job Definition form and select Actors from the drop-down list if you prefer.

5. Click **Run** . The Job Definition form displays. Verify your Actor selection.
6. (Optional) If needed for the Action Groups you're running, select a user profile from the **Run as User** drop-down 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.

7. (Optional) Expand the **Runtime Parameters** for each group to set additional parameters. The parameters that display depend on the type of Actions in the group.

8. (Optional) Select **Repeat Job** and configure the Repeat Job schedule. This can be set for a time interval or a specific number of times.
9. When you have the Job configured to your specifications, click **Run Now** or **Schedule**.
    - If you choose Run now, the Job Page displays.
    - If you choose Schedule, the Scheduled Jobs page displays.

- If an Action errors, the Actions that follow are still run. If there is a problem that prevents the Job from running, no additional Actions are run.
- For example, Actions that result in a pass, fail, or error status continue to the next Action until the Evaluation is completed. However, if the Director cannot communicate with the Actor (for example, the Actor is down or experiencing a network issue), the Evaluation is interrupted. In this case, remaining Actions are marked as "Not Run."

Running Bulk Evaluations

When you want to test a large part of your environment without running individual tests, use the bulk Evaluations functionality. Bulk Evaluations allow you to choose one or more user tags for each group to identify the set of Actors that you want to use. These tag selections determine how many Jobs are created.

To avoid excess Jobs, we look at the Group that has the most Actor combinations and then reuse those combinations for the other Groups. If available, each Group will also use the same Source Actor.

Run Bulk Evaluations

1. Go to **Library** > **Evaluations**.
2. Select an **Evaluation**.
3. Click **Run Bulk** ▶ Bulk . The Run form displays, with source and destination tag selections listed for each group.
4. For each Group:
    - If the group requires one Actor (Host CLI Actions, DNS Actions, etc), select one or more **Actor Tags**
    - If the group requires two Actors, select one or more Tags for both **Source Actor Tags** and **Destination Actor Tags**.
    - (Optional, when the group requires two Actors): Clear the checkbox next to **Limit to Actors with known connectivity**

By default, the platform will only create Jobs if it knows the Actors can communicate with each other. Clear the checkbox if you want the platform to create Jobs for all pairs of Actors based on the selected Tags. This functionality allows you to run Actions across all tagged Actors, validating connectivity expectations are met.

When all Tags are selected, the max number of Jobs will appear next to the **Close** button.

5. (Optional) If needed for the Action Groups you're running, select a user profile from the **Run as User** drop-down and enable or disable **Interactive Session**.
6. (Optional) Select **Repeat Job** and configure the Repeat Job schedule. This can be set for a time interval or a specific number of times.
7. When you have the Job configured to your specifications, click **Run Now** or **Schedule**.
    - If you choose Run now: The Bulk Job result page displays. For more information, see **Viewing Bulk Job Results** (https://docs.mandiant.com/home/msv-viewing-bulk-job-results).
    - If you choose Schedule: The Scheduled Jobs page displays.

If an Action errors, no additional Actions in that Sequence will run. If there is a problem that prevents the Job from running, no additional Actions will run.

Bulk Job Error

There could be some security content you are not able to run using the Bulk Job option. If the Sequence or Evaluation includes Groups of Actions that cannot run in your environment, you may receive an error when you try to run it using the Bulk Job option. For example, the following types of Actions could be an issue:

- Windows Actions when you don't have a Window Actor
- Linux Actions when you don't have a Linux Actor
- Mac Actions when you don't have a Mac Actor
- Email Actions when you do not have Email Theater (or have not configured Actors to support Email Theater)
- Protected Actions when you do not have Protected Theater (or have not configured your Protected Actor)

If you attempt to run a Sequence or Evaluation using the Bulk Run feature that meets the above criteria, the Sequences / Evaluation library displays with an error card. To work around this issue, we suggest the following process:

1. Clone the Sequence / Evaluation.
2. Remove the Group of Actions that your environment doesn't support and save the Sequences / Evaluation.
3. Run the new Sequence / Evaluation with the Bulk Run feature.