Mandiant

ADVANCED SETTINGS FOR SECURITY VALIDATION

The Advanced Settings page is where you edit Director, Actor, and security content settings. You must have the Settings - Edit permission to make updates on Advanced Settings. To access the Advanced Settings page, go to **Settings** > **Director Settings**. From there, select **Advanced** from the Settings menu.

To change any of the following settings, edit the info in the fields or select or clear the appropriate radio buttons. Save your changes by clicking **Update Advanced Settings** at the bottom of the page.

Field	Value format / Options	Details
AEDA Dashboard Refresh Rate	seconds	This setting controls how often AEDA dashboard page automatically refreshes in seconds. The default for this setting is 30 seconds.
Actor Info Refresh Rate	hours	The time in hours that Actor information is automatically updated. This information can be updated manually at any time by selecting **Environment > Actors**. For the Actor you want to refresh, click the ellipses ⋮ icon, in the Actions column; then, click **Edit**. Click **Refresh Actor Info**. The default for this setting is 24 hours.
Maximum Size for Data Exfil and Malicious Files	bytes	Controls the maximum single file size allowed for files contained in the file transfer library. The default for this setting is 300 MB (provided in bytes: 314572800). It's only recommended to adjust this setting under the direction of Mandiant Support.
Size to Allow Variable TCP Information in PCAPs and Streamer	bytes	Some PCAPs and streams optionally allow variable padding bytes that can be used to increase the overall packet size used to stream the data. The default for this setting is 0. It's only recommended to adjust this setting under direction of Mandiant Support.
Time Paused Between Job Actions	seconds	Controls the overall pause time (in seconds) between multiple job Actions in an Evaluation or Simulation Job Action Group. This setting can be overridden at the job level as well. This pause is to allow your environment time to process and generate related events through integrations. If there are significant delays in the local environment (for example, high delay network links), this value may need to be increased. The default for this setting is 3 seconds.

Field	Value format / Options	Details
Additional time added to all Job Action timeouts	seconds	The default for this setting is 0 seconds.
Host CLI Actions - Additional wait time (e.g., for event logging) for all actions	seconds	This setting lets you increase the baseline sleep time for all commands run in the Action and anywhere else that the Action may invoke sleep. Changing this setting is useful for systems and environments which might take longer to respond than more optimized systems. The default for this setting is 0 seconds.
Host CLI Actions - Additional wait after file dependency delivery	seconds	This setting lets you increase the file write period before an Action starts. This setting applies to files that are attached to the Action.
Timeout for Attacker Polling Target Status	seconds	Number of seconds the attacking Actor should continue to check the target Actor to update its results, once the attacker has completed the simulation. The default for this setting is 100 seconds. It's only recommended to adjust this setting under direction of Mandiant Support.
Timeout for Director Polling Job Status	seconds	Number of seconds the planner must not be able to communicate with the Actor before the Director cancels a job. The default for this setting is 900 seconds. It's only recommended to adjust this setting under direction of Mandiant Support.
Timeout for Monitor Event Detection	seconds	Amount of time the Monitor waits for Events to come in before it determines whether the Monitor has passed or failed. The default for this setting is 900 seconds. The time value should always be the same or greater than the Query time for the platform Integrations.

Field	Value format / Options	Details
Sleep before Prepare Action Retry (seconds)	seconds	Controls the amount of sleep time between these retries. The Prepare Action phase preps the platform to run the Action and can include larger datasets. The platform retries this phase 3 times before it faisl the Action. The default for this setting is 60 seconds. This value can be increased to provide additional time between retries.
Interval Between Polling Push Actors for Job Status	seconds	Number of seconds to wait between communication attempts to the Actor to get status updates on running Actions. The default for this setting is 1 second.  It's only recommended to adjust this setting under direction of Mandiant Support.
Interval for Actor checking Job Status	seconds	Amount of time the Actor waits when asking for the status of a running Action, while it checks to see whether the Action has completed. The default for this setting is 5 seconds.  The Interval Between Polling Actor's Job Status and Interval for Actor checking Job Status settings allow users to optimize their settings. For example, lower number settings get sresults of Actions faster at the expense of increasing the amount of communication between Director and Actor, whereas higher number settings are slower at getting the results of Actions but can decrease the amount of communication significantly, especially for longer running Actions.
Sleep Before Reverting Snapshot to Allow Integrations to Communicate	seconds	When running Protected Theater Actions, the Protected Actor reverts to known state snapshot at completion. This delay allows any integrations to finish communicating events related to an Action before reverting the Actor to its previous snapshot. The default for this setting is 60 seconds. This value can be increased if local integrations need more processing time before reverting the Actor to its previous snapshot.
Delete Old Job Notifications	days	Push notifications for Jobs are removed after this time in days. The default for this setting is 14 days.  If Notifications have been deleted because of the Delete Old Job Notifications setting, they are not available.
Delete Old Job Debug Logs	days	Controls how long Debug Log files are retained. The default for this setting is 0 days, which means Debug Logs are not removed. This value can be adjusted to remove old Debug files older than this value in days.

Field	Value format / Options	Details
Enable PCAP TCP Stack Replication	On/Off	Allows transmissions to be monitored and resent at the TCP socket level. The default for this setting is "On". When enabled, it uses the values specified in the "TCP Stack Resend Timeouts" setting.
TCP Stack Resend Timeouts	seconds (comma delimited)	Works along with the "Enabled PCAP TCP Stack Replication" setting to control the number of retries for transmission and the number of "backoff" seconds between each attempt. These values are typically doubled for each reach round of retransmission. The default for this setting is "1.5,3,6,12".  These values may need to be adjusted if TCP Stack Replication is enabled and Actions are resulting in an error due to communications timeout.
User Session Timeout Length	minutes	Controls how long UI sessions can remain inactive before they are closed. The default for this setting is 30 minutes.
Protected Theater Blackhole IP for Ignored Connections	IP address	IP address that is used as a "blackhole" destination for any "Ignored Connections" configured under "Environment/Protected Theaters". The default IP for this setting is "1.2.3.4".
List of IP addresses/CIDRs to allow access to Director via SSH	IP/CIDR addresses	The default for this setting is "0.0.0.0/0".
Default Language for Host CLI Actions	English, French, French Canadian, German, Spanish, Spanish Latin America	Only for Windows-based Host CLI Actions and Protected Theater Actions. This setting tells Windows to convert the language returned to English (if necessary) when running Host CLI Actions. The default for this setting is "English".
Default Path for Host CLI Actions	Windows Path	Only for Windows Actors. This setting defines the default working directory for Host CLI Actions. Leave blank to use the user profile directory. This path is used as the default value for the `Custom profile path` runtime parameter in Windows Host CLI Actions and for the `v_default_dir` variable if it's present in the Action.

Field	Value format / Options	Details
Mitre Default ATT&CK version	Supported version numbers	This setting defaults to *Default to current version (x)*. This way, it automatically updates when we update the MITRE ATT&CK version.
Allow Users to be Remembered	Yes/No	Allows a user to click "Remember me" during login, which disables the session time-out until the user logs out of the system. The default for this setting is "Yes". Some sites may want to disable this option to force all idle UI sessions to timeout.
Show deleted users	Yes/No	User accounts are generally disabled, not deleted. If you set this setting to Yes, Users are deleted and are added to a Deleted Users table on the Users page.
Enable Expanded Job Debug Log	On/Off	Controls generation and retention of the debug level Job logs in the Director database. The default for this setting is "Off". Enabling this setting increases the size of Job logging within the database, but may be useful to isolate any issues.
Enable PCAP UDP Retry Replication	On/Off	Provides the same feature as the "Enable PCAP TCP Stack Replication", however, this setting is specific to UDP based PCAP Actions. The default for this setting is "On".
Hex Actions - Retry HTTP Request when 401 Response Code is Received	On/Off	Controls when HTTP Actions receive a 401 error (unauthorized) if they should be tried again. The default for this setting is "Off". Depending on the local environment and any authentication delays, this value may need to be enabled in order to retry HTTP Actions with authentication.
Hex Actions - Update Host in HTTP Header	On/Off	This setting, when enabled, overrides the original HTTP "Host" Header in the PCAP data with the target actor's FQDN (if provided) or IP address, when running PCAP Actions. The default for this setting is "On".

Field	Value format / Options	Details
Hex Actions - Clear Accept - Encoding Header	On/Off	Clears any content-based Accept-Encoding headers. It can be used to prevent intermediate network or security devices between Actors from changing data encoding during transit. The default for this setting is "Off". This option can be overridden in individual Actions and Sequences/Evaluations by checking the **Clear Encoding Header** checkbox in the Job Definition window. The default is taken from the global setting.
Hex Actions - Update Date in HTTP Header	On/Off	This setting, when enabled, overrides the original HTTP "Date" Header in the PCAP data, with the current date when running PCAP Actions. The default for this setting is "On".
Suppress Extraneous Events instead of Dropping Events	On/Off	When filtering events generated by integrations, this setting controls whether matching events are simply suppressed, rather than dropped. This setting can be overridden for each filter rule within the event filters configuration. The default for this setting is "On". Suppressed events are not used for matching Actions, but allow the user to see what events their filters would have dropped.
Include errored job actions in Integration Event querying	On/Off	Normally events from Integrations that would match Job Actions that finished in Error status is discarded. When enabled, this setting retains matching events for Actions that ran successfully or not. The default for this setting is "Off".
Include email actions in 'checking' state in Integration Event querying	On/Off	By default, integrations only consider completed Job Actions for matching, but this default configuration can miss email-related events in certain environments that have a long delay sending emails or for emails that are blocked. When this setting is enabled, events for email Job Actions that are in a “checking” state are included as a match to an integration's query. The default for this setting is "Off".
Host CLI Actions - Windows Randomize Executables	On/Off	Automatically randomizes the name of the process that runs the Job when you use an ActionUserProfile to run Actions. The default for this setting is "Off".
Host CLI Actions - Force Windows Code Page to English	On/Off	In Windows environments where the primary language is double-byte character-based, this setting forces the command output to be in English. When enabled, the CLI Log Output in Job Results displays the output in English. This setting ensures that the Job Results for these Actions are accurate after being processed by Security Validation. For MA-SV, this setting is organization-specific. That means it only applies to Windows Actors in the Security Validation organization that the admin belongs to. The default for this setting is "Off".

Field	Value format / Options	Details
Require Review of Created & Updated Endpoint Actions	Yes/No	Controls whether created/updated Actions in the library require approval by an account with the "Approve Endpoint Actions" capability. The default for this setting is "Yes".
Verify Time on Actor before Upgrading	Yes/No	Determines if the Actor has a valid timestamp before starting an Actor upgrade process. The default for this setting is "Yes".
Allow Actions between All Actors	Yes/No	Controls whether any grouping of Actors can be used for an Action regardless of the results of specific network connectivity (CTTN) checks. The default for this setting is "No".  Using the Map to select Actors when running Sequences and Evaluations, you can select all Actors. However, this approach makes it difficult to identify which Actors can communicate with each other based on the results of the CTTN checks.
Disable Download of Data Exfil Files	Yes/No	This setting controls whether potential exfiltrated data files generated on Actors is available for download. The default for this setting is "No".
Can Override Job Actions	Yes/No	Lets you override the results of Security Validation Actions by switching the status of a single Action in a Job from "blocked" to "not blocked" or from "not blocked" to "blocked." The default for this setting is "No".  This setting is disabled by default. If the setting is disabled (set to No), all user overrides are hidden in the Platform.

Field	Value format / Options	Details
Enable Content Service	Yes/No	Determines automatic reception of content from the Content Service. When disabled, you must manually apply any desired content packs. The default for this setting is "Yes", content is automatically downloaded and staged on the Director when Mandiant approves it. If your license was created or renewed after January 1, 2022, this must be set to **Yes** and cannot be modified. For these licenses, if communication doesn't occur at least once every 15 days, your Director stops running Jobs until a connection occurs. The connection tracking is included in the Operational Status monitoring. See **Operational Status (https://docs.mandiant.com/home/operational-status)** for more information.
Auto Apply Content Service Imports	Yes/No	Controls whether content downloaded via the Content Service is automatically applied to the Director after it has been staged. When set to "No", the user must manually import each staged pack in a similar fashion to manual VAS pack uploads in the application. If you select **No**, the content appears on the page in the same way as uploading a vas pack manually. By default, content updates sync once per hour. Reboot the Director or click **Check for Content** on the Content page to check for updates immediately.
Configure Content Service Sync Schedule	frequency per (minutes, hours, days)	This setting determines the frequency at which content updates are synced. The default for this setting is once per hour.
Send Data to Mandiant for Research Purposes	On/Off	Controls if telemetry data is sent to Mandiant. The default for this setting is "On".