PROTECTED THEATER SETTINGS

The settings on this page are here to support accessing the Protected Theater and running Protected Actions on Windows.

Windows Registry Keys

To properly test Windows security technology controls when running destructive Host CLI Actions on Protected Theater, specific Windows configurations must be disabled. These configurations are enabled on most companies' gold images, so each time you run a destructive Host CLI Action, the platform automatically checks the Windows registry for specific registry keys and adds them if necessary. If your environment has different registry keys that are interfering with testing, you can add them in the Protected Theater Settings.

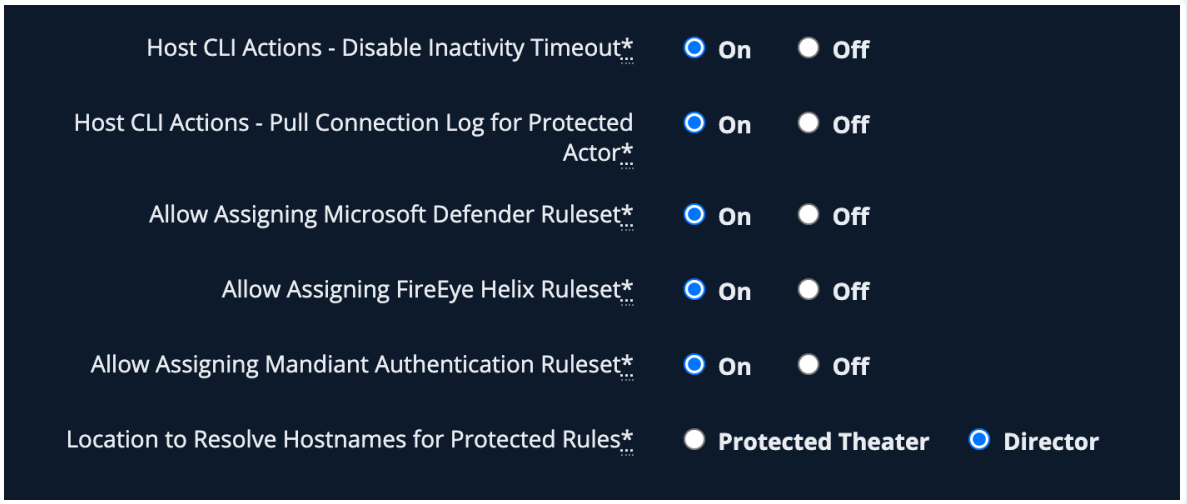
Protected Theater Settings

Running PT Actions Settings

These settings are related to when you run Protected Actions. They are enabled by default, but can be changed if necessary.

Field	Definition	Actor / Operating System
Disable Inactivity Timeout	Prevents the Windows inactivity timeout to shut down the harddrive / operating system	Windows
Pull the connection log for Protected Actors	These logs contain the outbound connections the Protected Actor has attempted. This could be useful in capturing IOCs from the malware, such as if it's connecting to a C2 server and if you've seen that in your environment before	All

Field	Definition	Actor / Operating System
Allow Assigning Microsoft Defender Ruleset	This ruleset automatically allows DNS communication to Microsoft Defender, allowing the Defender to receive updates. When enabled, the ruleset appears on the Protected Theater page above the Ignored rules.	Windows
Allow Assigning Trellix (FireEye) Helix Ruleset	This ruleset automatically allows DNS communication to Microsoft Defender, allowing the Defender to receive updates. When enabled, the ruleset appears on the Protected Theater page above the Ignored rules.	Windows
Allow Assigning Mandiant Authentication Ruleset	This ruleset automatically allows DNS communication to Microsoft Defender, allowing the Defender to receive updates. When enabled, the ruleset appears on the Protected Theater page above the Ignored rules.	Windows
Location to Resolve Hostnames for Protected Rules	Allows you to determine if the Protected Theater or the Director is used to resolve domain names when you have protected rules configured. If you are are using MSV, it can be set to either, based on your needs. If you are using MA-SV, you will want this set to Protected Theater.	All



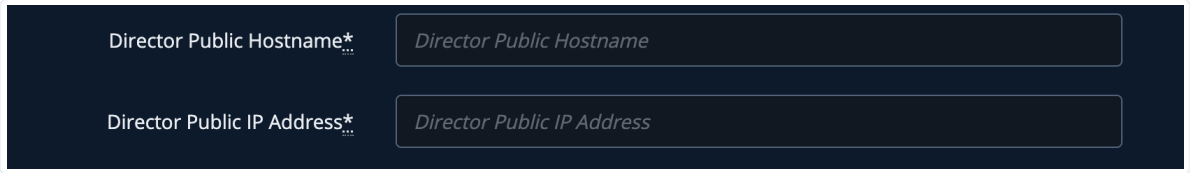
Protected Theater Settings

Communication Rule Creation

In some cases, communication rules must be created to allow your Protected Actor to communicate with your Director on an IP Address other than the private IP Address of the Director. For example, this would be the case if your Director was hosted in the cloud or if you are using the SaaS version of Security Validation. These two fields allow you to provide information about your Director, which will then create and apply the necessary rules each time you run protected Actions..

IMPORTANT: If your Protected Actor can communicate with the Actor on the Director's private IP Address, leave these fields blank.

Field / Fields populated	What happens / what rules are created	Notes
Director Public Hostname and Director Public IP Address	• A DNS rule is created and sent to the Protected Theater to resolve the provide Hostname to that IP Address • A communication rule is created to allow communication on port 443 to that IP Address (so the Protected Actor can reach the Director)	
Director Public Hostname only	• The Director will attempt to resolve any hostname entered • A DNS rule is created to resolve the provided Hostnames to the identified IP addresses • A communication rule is created for every resolved IP to allow communication on port 443 to that IP Address	Can be a comma delimited list of hostnames
Director Public IP Address only	A communication rule is created to allow communication on port 443 to that IP Address	



Protected Theater Settings

To update your Protected Theater Settings

1. Go to **Settings > Director Settings**.
2. Select **Protected Theater**.
3. Optional: Enter Registry Keys for Registry Key fields.
4. Optional: Populate the Director Hostname and IP Address.

   This information is used to create DNS and Communication rules on the fly when a Protected Action is run.
5. Optional: Update the Settings for the other Protected Theater Settings Fields.
6. Click **Update Protected Theater Settings**.