PROTECTED THEATER CONFIGURATIONS

Once you have the Protected Theater and Actor set up, there are additional items to set up in the Director. These configurations help provide additional details for tests run. This includes:

- Creating Action User Profiles
- Adding Ignored Connections
- Viewing Protected Rulesets
- Adding Protected Theater Rules
- Configuring Protected Theater Settings

Create Action User Profiles for the Protected Actor

Actions processed by the host operating system image in the Protected Theater can be run as system, domain, or local user accounts. For testing purposes, the platform continues as if the user has clicked on links and opened files that are contained in the Actions. For this to function properly, User Profiles must match the user accounts you created on the host image.

Local user accounts are not required, you can run everything as system. However, using a non-system account allows you to see screenshots and the command line input. You also are not testing against your standard user profiles or access levels.

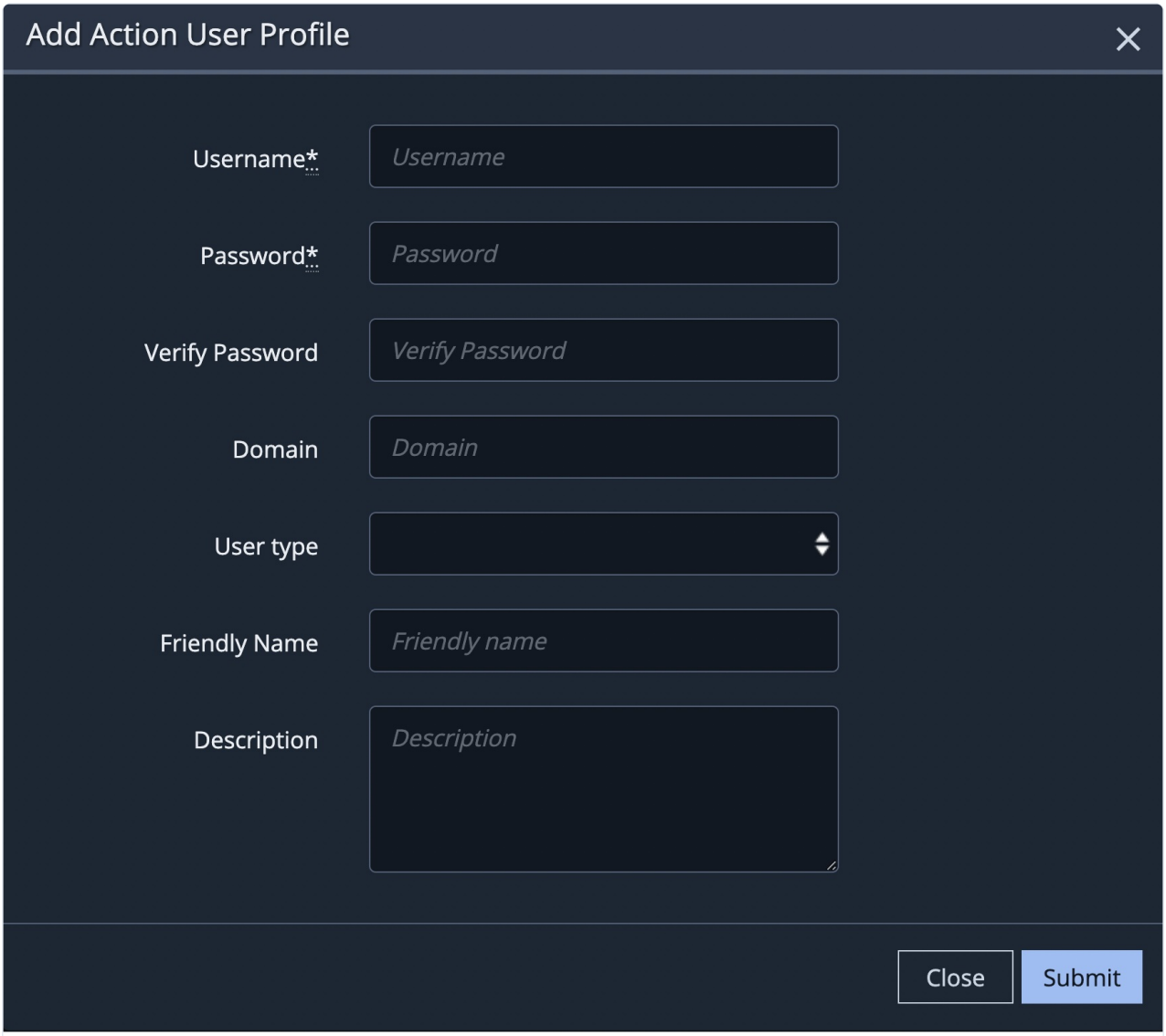
> Local Accounts are recommended over Domain Accounts when running destructive Host CLI Actions in Protected Theater. This removes the need for a communication rule to allow access to the domain, thus limiting the potential exposure if a rule is misconfigured.

CREATING ACTION USER PROFILES

1. Go to **Environment > Action User Profile**.
2. Click **Add Action User Profile**.
3. In the Add Action User Profile form, enter the necessary information, and then click **Submit**.
    - **Username**: Specify the account you created on your gold image for the Director to use to run Actions.
    - **Password**: Specify the password for the username entered above.
    - **Domain**: (Optional) Enter the domain the user is represented.

      > You should always enter a valid domain in the Domain field, otherwise it can cause errors. For example, adding a `.` in this field causes the User Profile to try to logon to the local system account for the user, which prevents it from logging in automatically when you are running Host CLI Actions. See **Issues with Action User Profiles (https://docs.mandiant.com/home/issues-with-action-user-profiles)**for more information.

    - **User Type:** Select Admin, Root, or User, matching the type of user on the OS.
    - **Friendly Name**: (Optional) Enter an alternate name for the Action User profile. When populated, this name will be displayed for the user in an Action's runtime parameters and on the Job Results page.
    - **Description**: (Optional) Enter additional information about the User Profile.



Add Action User Profile form

Add Ignored Connections

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click *Add Ignored Connections*.
4. Enter a *name*.
5. Select *the Protocol*.
6. Enter the *Destination IP/Host* and *Destination Port*.
7. Click **Create Ignored Connection**.

Viewing Protected Rulesets

If any Protected Rulesets are enabled in your Director for your Protected Theater communications, you can view them on the Protected Theaters page by clicking **Environment > Protected Theaters**. These rulesets allow specific wildcard DNS rules to communicate out of the Protected Theater.

Protected Rulesets

MSV Defined Rulesets for Accessing Specific Assets

Rule ID	Name	Port(s)/Protocol	Domains
2213	FireEye Helix	80,443/TCP	*.fireeye.com, *.apps.fireeye.com, *.ingest.apps.fireeye.com
2222	Mandiant Authentication	443/TCP	app.validation.mandiant.com, login.mandiant.com, mdlogin.fireeye.com, auth.fireeye.com, auth.mandiant.com
2	Microsoft Defender	80,443/TCP	*.wdcp.microsoft.com, *.wdcpalt.microsoft.com, *.wd.microsoft.com, *.update.microsoft.com, *.delivery.mp.microsoft.com, *.windowsupdate.com, *.download.microsoft.com, *.download.windowsupdate.com, *.blob.core.windows.net, *.data.microsoft.com, *.notify.windows.com, *.wns.windows.com, *.dm.microsoft.com, *.securitycenter.windows.com, *.smartscreen-prod.microsoft.com, *.smartscreen.microsoft.com, *.checkappexec.microsoft.com, *.urs.microsoft.com, go.microsoft.com, www.microsoft.com, msdl.microsoft.com, crl.microsoft.com, definitionupdates.microsoft.com, login.microsoftonline.com, login.live.com, login.windows.net, packages.microsoft.com, enterpriseregistration.windows.net, winatp-gw-cus.microsoft.com, winatp-gw-eus.microsoft.com, winatp-gw-cus3.microsoft.com, winatp-gw-eus3.microsoft.com, winatp-gw-neu.microsoft.com, winatp-gw-weu.microsoft.com, winatp-gw-neu3.microsoft.com, winatp-gw-weu3.microsoft.com, winatp-gw-uks.microsoft.com, winatp-gw-ukw.microsoft.com

Protected Rulesets

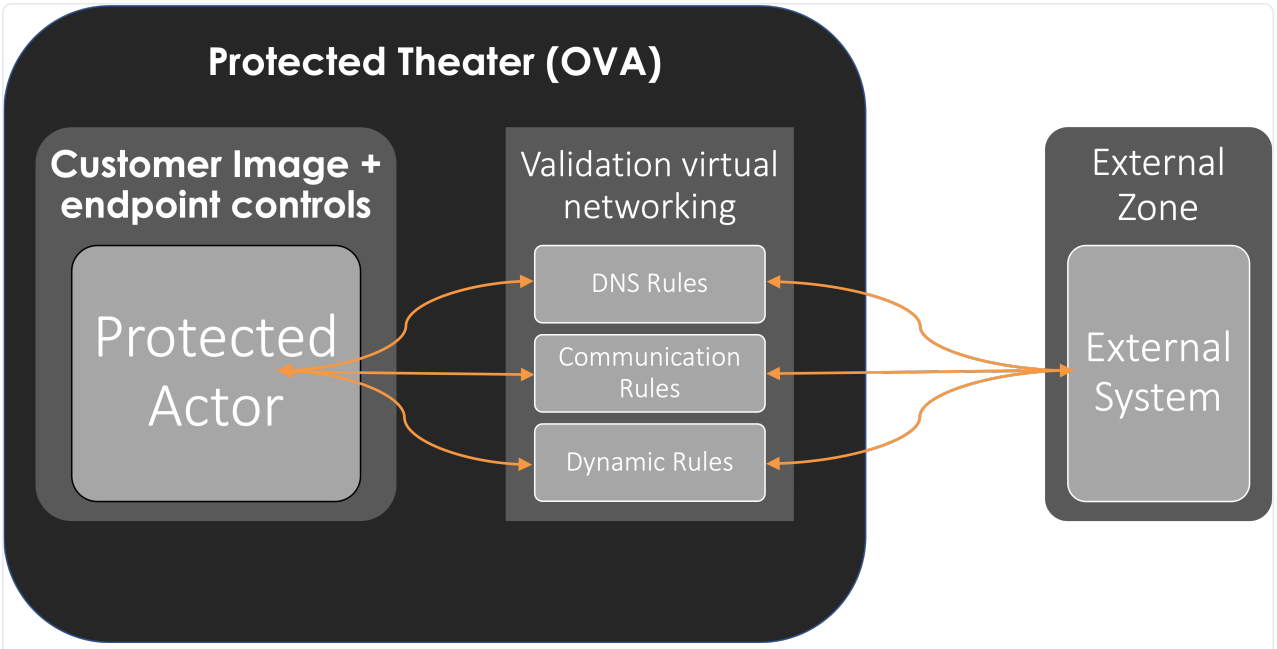
Adding Protected Theater Rules

To permit host-based controls to communicate with other controls on the internet (e.g. Cylance) or in the internal network (e.g. McAfee ePO), Protected Rules must be explicitly created. There are three different types of Protected Rules that may be created:

- **Communication Rules**, which define protocol, destination IP, and port
- **DNS Rules**, which instruct the Protected Theater to resolve defined domains to IP addresses
- **Dynamic Rules**, which instruct the Protected Theater to periodically query DNS to resolve domains, update communication rules dynamically, and display the current resolved information; the actual resolution is completed on the Director and then passed to the Protected Theater

Once the rules are created, you **assign the rules** to the PT, Protected Actor, or both.

> Care should be taken when defining Protected Theater Rules to ensure only the communication absolutely required to validate the controls being tested is allowed. Allowing more than this communication for outbound data transfer from the Protected Theater (for example, Windows domain services) could expose systems beyond the Protected Theater to malicious communication.



Overview of PT Communication with external systems

Protected Communication Rules

Create one or more protected communication rules to allow communication between your network and the Protected

Theater or Protected Actor. Rules created should be very specific and locked down. Potential Rules include communication that allows the endpoint to receive updates or send events and open a connection to security technologies.

> Traffic to and from the Director is automatically allowed with no additional configuration required, unless your Director is in the Cloud. When the Director is in the Cloud, you must add a rule to allow the Protected Actor to talk to the Director.

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click **Add Protected Communication Rule**.
4. Enter a *name, protocol, destination IP, and port*.
5. Click **Create Protected Rule**.

Protected DNS Rules

Use DNS rules to resolve domains to IP addresses. For example, if an Action requests a specific domain, add a DNS rule to specify what IP you want to send that traffic to.

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click **Add Protected DNS Rule**.
4. Enter a *name, domain, and IP address* for the domain to resolve to.
5. Click **Create Protected Rule**.

Protected Dynamic Rules

If you have technologies that are cloud-based or that change IP addresses frequently, it is better to set up a Dynamic Rule. The Dynamic Rule combined with the DNS information configured within the Director allows the system to regularly lookup and update the IP information for the provided domain.

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click **Add Protected Dynamic Rule**.
4. Enter a *name, domain, protocol, destination port, and refresh rate*.
5. Select or clear the **Unresolvable domains should return NXDOMAIN** checkbox.
6. Click **Create Protected Rule**.

Add Protected Rule Assignments

Once the protected rules are created, they need to be assigned. Each rule assignment can include one or more rules and be assigned to the Protected Theater, Protected Actor, or both.

1. Launch the Director & sign in.
2. Click **Environment** > **Protected Theaters**.
3. Click **Add Protected Rule Assignment**.
4. Enter a *name and description*.
5. Select the *Protected Theater, the Protected Actor, or both*.
6. Select *one or more Rules*.
7. Click **Create Protected Rule Assignments**.