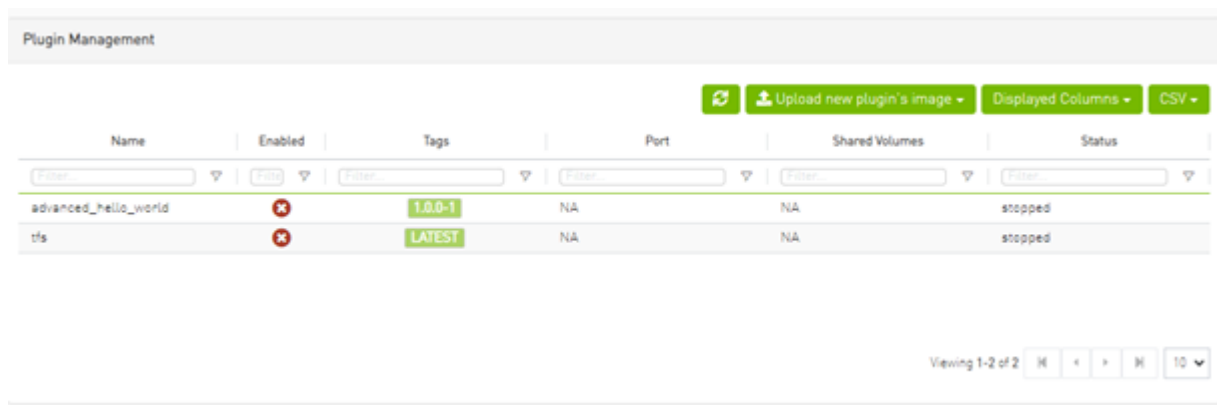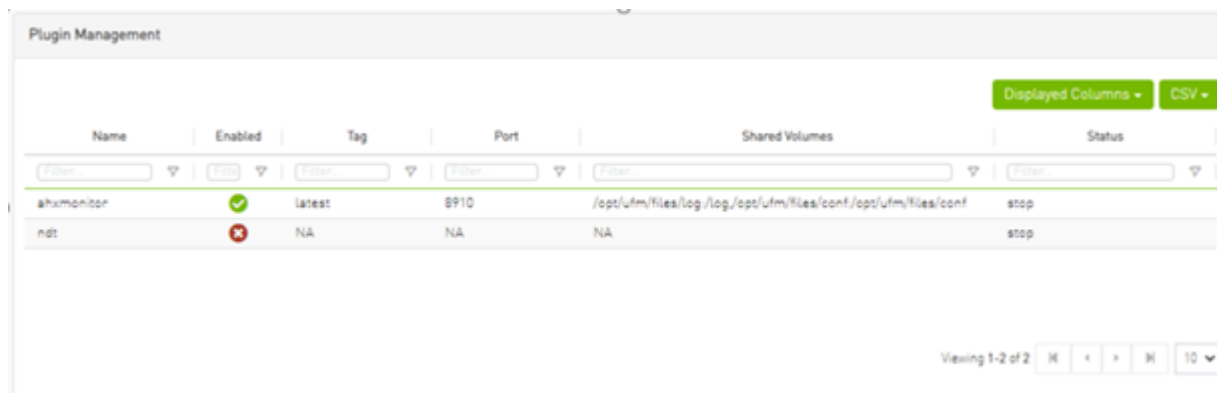# Plugin Management

Plugin management allows users to manage UFM plugins without using CLI commands. Under "Settings", there is a tab titled "Plugin Management".

The functionality of the "Plugin Management" tab is to give the user the ability to add, remove, disable and enable plugins.

Furthermore, the plugin management feature allows loading a plugin's image in two ways: either by remotely pulling it from a Docker Hub repository or by directly uploading the image file from the user's local machine.
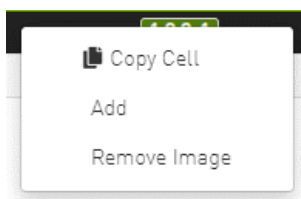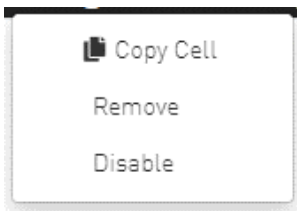

Actions:

- Add – Used to add a selected plugin, opens a model to select the needed tag.
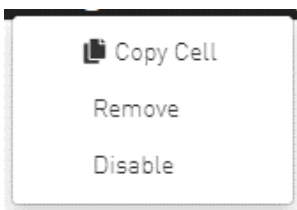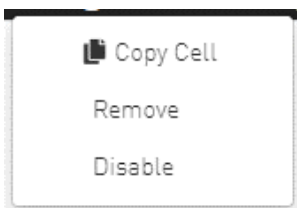
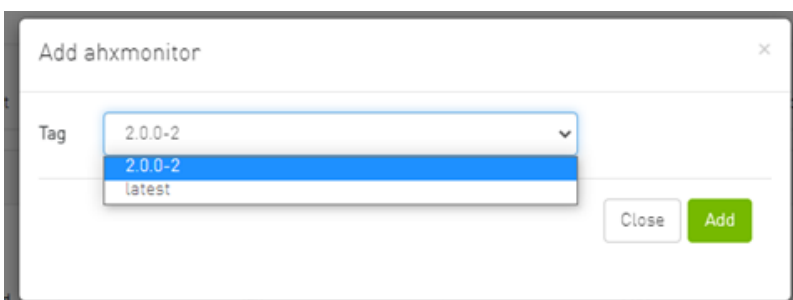- Remove – Used to remove a selected plugin.

- Disable – Used to disable a selected plugin, so the plugin is disabled once the UFM is disabled.
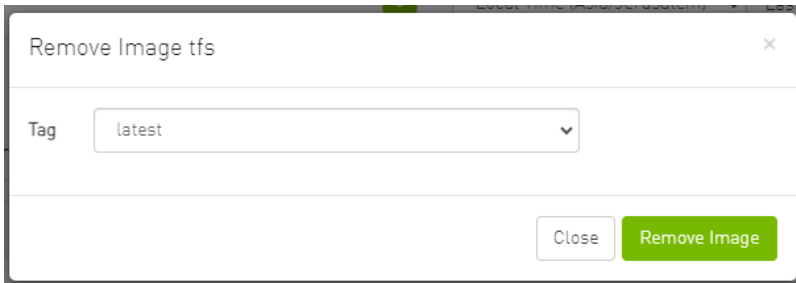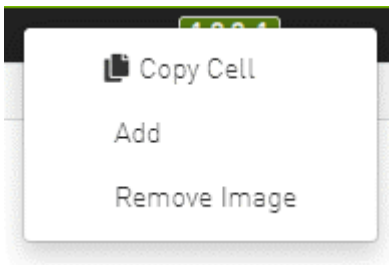

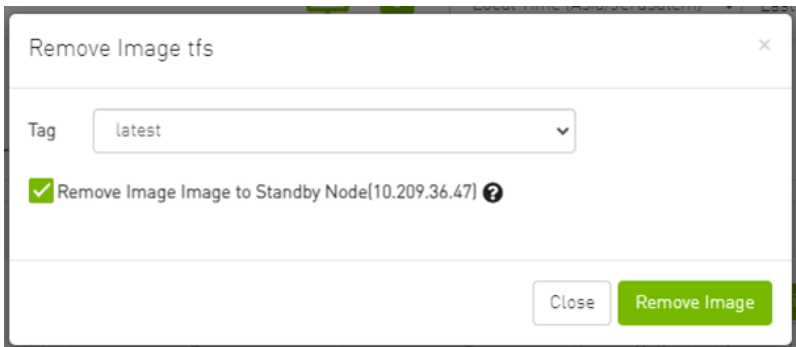- Enable – Used to enable a selected plugin, so the plugin is enabled once the UFM is enabled.

- Add ahxmonitor – Used to add a selected plugin; the action opens a modal to select the requested tag.

- Remove plugin Image – Used to remove plugin image

If the high availability (HA) mode is enabled, the user will see the option to remove the image from the standby node as well.

In cases where there is no established trust communication between the master and standby nodes, the user will be required to provide a username and password to establish an SSH connection between them.

- Pull plugin Image – Used to pull plugin image remotely (e.g. from a Docker Hub repository) or by loading it from user local machine by uploading the image file itself.

If the high availability (HA) mode is active, the user will be presented with the choice to pull the image to the standby node as well.

Once again, in the absence of trusted communication between the master and standby nodes, the user will need to input a username and password to create an SSH connection between the nodes.

- Load plugin Image: this feature allows the user to upload the image file from their local machine directly.

Similarly, if the high availability (HA) mode is enabled, the user will have the option to load the image to the standby node too.

And, as mentioned earlier, if there is no trusted communication between the master and standby node, the user will need to provide a username and password to establish an SSH connection between the nodes.