SECURITY ORCHESTRATION PLAYBOOK

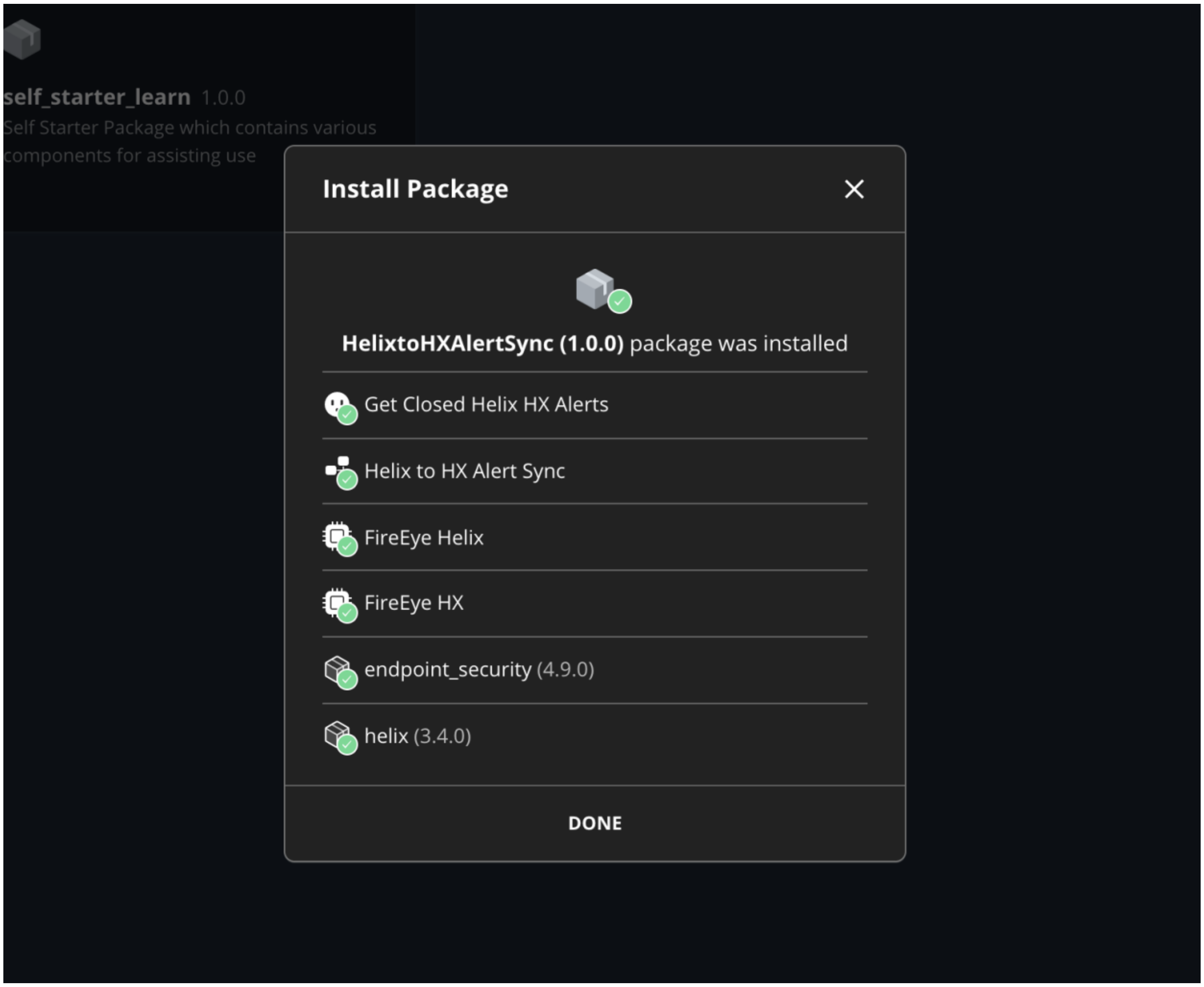
FIREEYE HELIX | ENDPOINT SECURITY (HX) SYNC

USER GUIDE (v1.0.0)

Helix | Endpoint Security (HX) Sync:

This package contains a playbook which, when triggered, synchronizes alerts between FireEye Endpoint Security (HX) and FireEye Helix. The playbook is triggered periodically by an adapter that requests closed HX alerts from Helix. HX is then instructed to suppress alerts already closed in Helix.

Begin by installing the package fireeye.helix_hx_sync-x.x.x.package by navigating to
Manage Content (left column) -> Install (top right) -> Choose File (center), then selecting the fireeye.helix_hx_sync-x.x.x.package package from your local file system. Results should resemble Figure 1.



self_starter_learn 1.0.0
Self Starter Package which contains various components for assisting use

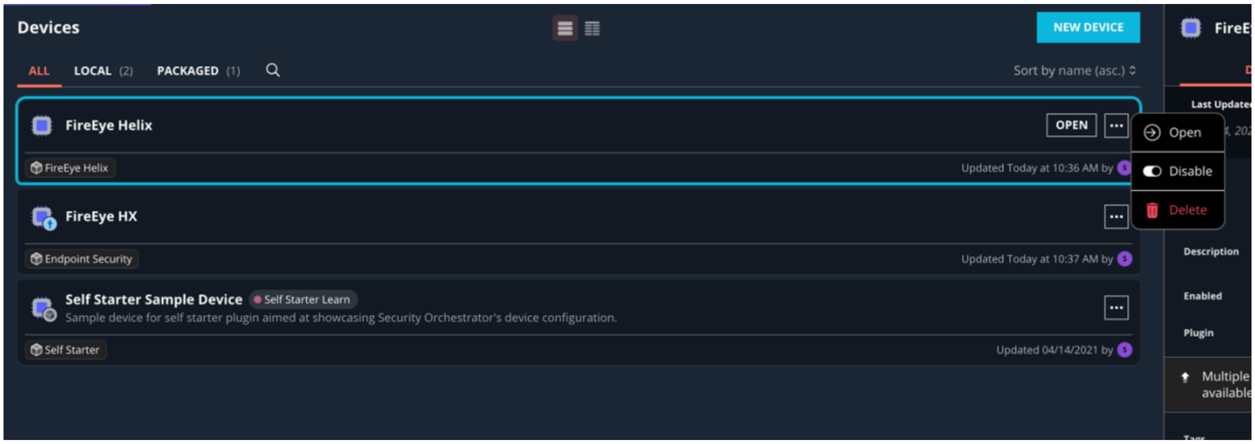
Install Package

HelixtoHXAlertSync (1.0.0) package was installed

- Get Closed Helix HX Alerts
- Helix to HX Alert Sync
- FireEye Helix
- FireEye HX
- endpoint_security (4.9.0)
- helix (3.4.0)

Figure 1, Package Installation

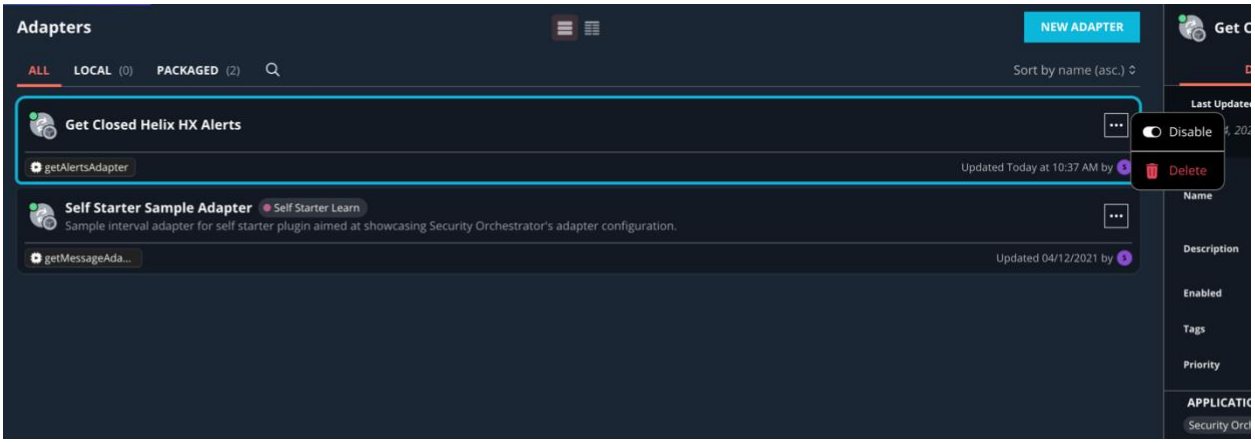
Configure and enable required devices by going to
Configure (left column) -> **Devices** (left column) -> device to configure and enable (center)
Once a device is configured, enable it by clicking the ⋯ button to the right of the device as pictured in Figure 2.



Sample device for self starter plugin aimed at showcasing Security Orchestrator's device configuration.

Figure 2, Enable Device

Configure and enable required Adapters by going to
Configure (left column) -> **Adapters** (left column) -> adapter to configure and enable (center)
Once an adapter is configured, enable it by clicking the ⋯ button to the right of the device as pictured in Figure 3.



Sample interval adapter for self starter plugin aimed at showcasing Security Orchestrator's adapter configuration.

Figure 3, Enable Adapters

Required Devices:

FireEye Endpoint Security (HX)

Required Parameters:

- Password: Credential for the HX account
- Username: Credential for the HX account
- Host address: URL for the HX instance
- All other parameters should be left default

FireEye Helix

Required Parameters:

- API Key: Credential for the Helix account
- Helix URL: URL for the Helix instance
- All other parameters should be left default

Required Adapters:

Get Closed Helix HX Alerts

Require Parameters:

- None, default vales all acceptable

Playbook Parameters:

- None, triggered by Get Closed Helix HX Alerts adapter
- When opened, playbook should resemble Figure 4

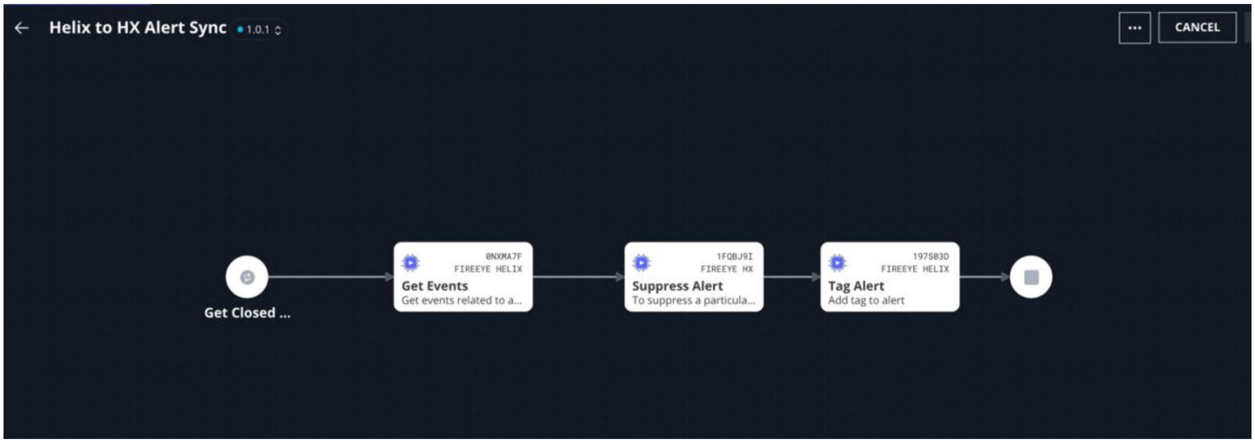


Figure 4, Helix to HX Alert Sync Playbook