Concept of Advance Configuration (Refer to Technician Manual for detail configuration)

Advance configuration enables the agent to react autonomously in different conditions, to fulfill the need to obtain valuable evidences while remaining stealth at all times.

Advance configuration is based on Events and Actions model. Events are conditions that the device is subjected to. Some events are generated by the device (i.e. going into screen saver mode), while others may be introduced externally (i.e. when the device is plugged into AC power) or based on natural course (i.e. everyday at 12pm). Action is triggered by event and it determines the behavior of the agent. Modules are functions and capabilities of the agent with regards to evidence collection.

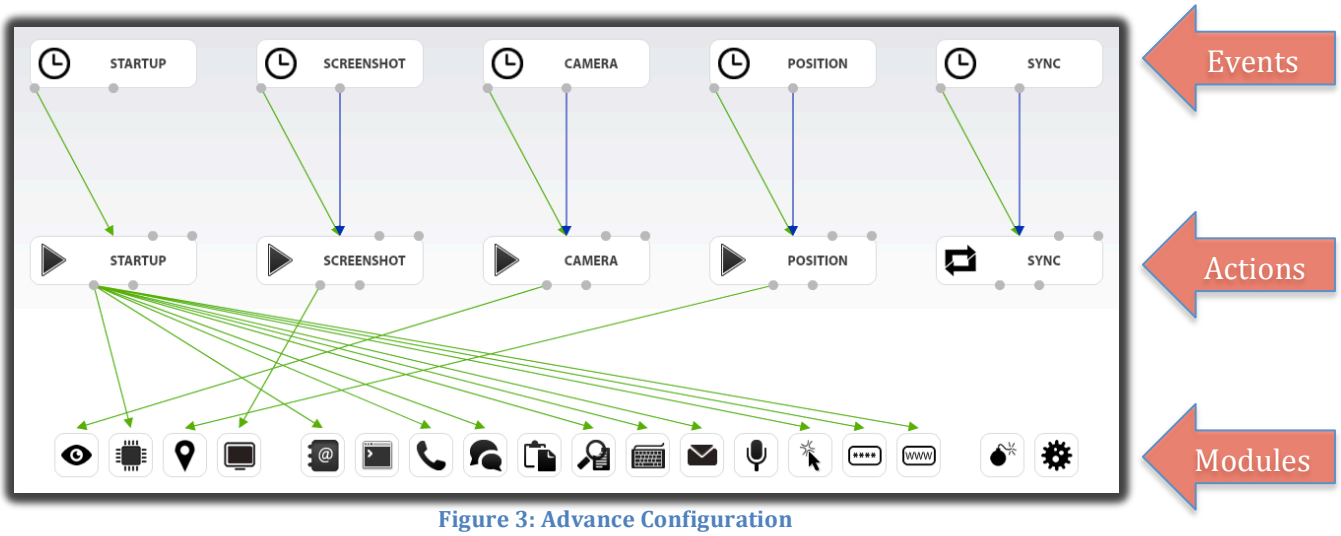


Figure 3: Advance Configuration

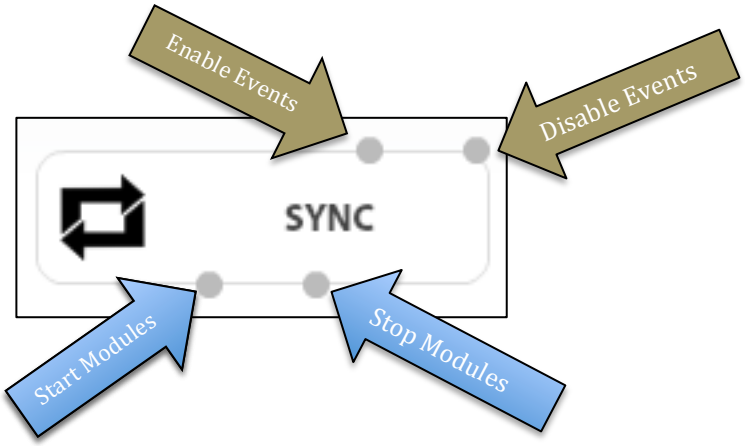
Above is an example of an advance configuration. Notice that there are 3 distinct rows. The top row indicates all the events, the middle row is all the actions and the bottom row shows all the modules supported by the agent. Note that Events, Actions and Modules for desktop and mobile vary because of the nature of the type of device. Events, Actions and Modules are joined by Green (Start/Enable), Blue (Repeat) and Red (End/Disable) lines depending on the configuration. Note that Events cannot be joined to the Modules directly. It must go through an Action.

Events

An event consists of 3 possible configurations, **Start**, **Repeat** and **End**. Some events do not have an End configuration.

Actions

Actions are behavior of the agent and it is triggered only by events. With regards to joining to Event or Module, there are 4 possibilities.

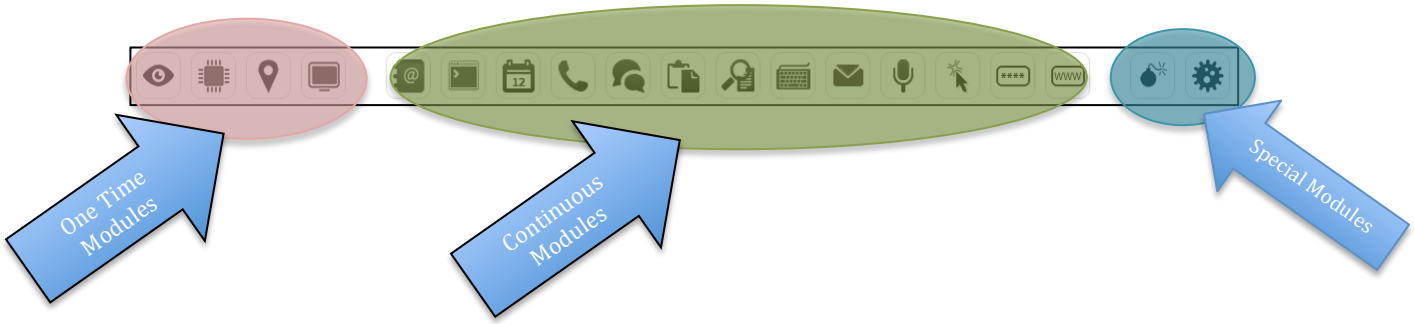


Besides starting actions like synchronization, uninstallation etc, Action can also start or stop Modules. The top row determines whether an event is disabled or enabled when this action is triggered. This is typical used to collect specific evidence(s) based on multiple dependent events. Bottom row allows the collection of specific evidenc(e) depending on whether the respective Module is started or stopped.

]HackingTeam[

Modules

Modules are the capabilities of an agent and its ability to collect evidence. There are generally 3 categories of Modules, separated by space.



One Time Modules: These modules once started have a definite stop. It will get one piece of evidence of its type when started, after which it will automatically stop. For a number of evidences of the specific type, you need to start the respective Module a number of times

Continuous Modules: These modules continuously monitor for the specific evidences once started and will never stop until it is configured to stop.

Special Modules: These modules controls the behavior of the agent enable it to be more stealth.