

Run v1.0

Grasshopper Component User

Guide

DRAFT



CL BY: 2355679
CL REASON: Section
1.5(c),(e)
DECL ON: 20351003
DRV FRM: COL 6-03

1 Description

Run is a Grasshopper component that provides a simple way to drop and execute and Windows executable.

The Run component writes its input payload to the file system at a specified location and executes it with the provided command line arguments. If the directory specified for the payload does not exist, it is created.

2 Usage

2.1 Builder Command Line

add component run [-a ARGS] PATH

PATH path to the payload on target
 ARGS arguments to the payload upon execution

Example

(gh) add component run "c:\windows\drop.exe" -a "do the thing"

2.2 Supported Payload Types

Run accepts input payloads in EXE format for the x86 or x64 architectures. Run is a terminating component and does not output a payload.

Input Type	Output Type(s)
x86 EXE	None
x64 EXE	None

2.3 Uninstall Procedure

The uninstall procedure is manual and comprises two steps:

1. Kill the process executing the payload or wait for it to exit.
2. Delete the payload from the file system.

3 Footprint

File System

- Payload Executable, located at a user specified location
- Payload Directory, may have been created