# SMG Utilities

This Package is for the use of integrate with SMG “Symatec Messaging Gateway” and take some actions on it,

### Currently the functionality is as follows:

- Block IP Address in SMG.
- Block Domain Name in SMG.

### The Package “smg_utilities.tar.gz” Includes the following:

- Two Functions: “Utilities SMG Domain” and “Utilities SMG IP”.
- Two Workflows: “SMG Block Domain” and “SMG Block IP”.
- Two Menu Item Rules: “Example: smg Block Domain” and “Example: smg Block IP”.
- Message Destination: “fn_smg”.

Every Function is to be used in its workflow, Rule is customized to take the action and be the trigger engine of the workflow.

### Description on how to use functions:

Analyst has an Incident with Malicious Domain Name Artifact and need to take the proper action to block it in SMG,

“Example: smg Block Domain” is the rule action on the Artifact and this rule will trigger the Workflow “SMG Block Domain” which is configured to take the Artifact in its function “Utilities SMG Domain” as input to be send to SMG.

Workflow Post-Script returns the result of the SMG HTML Page as an Incident Note.

Note: Same scenario concept is used for Blocking IP Address in SMG.

## Prerequisites:

- SMG URL.
- SMG User with privilege of the functionality required.
- Python 3 installed in Resilient Integration Server.
- Resilient Circuits at least version 30 is to be installed in the integration Server.
- Install Packages : (requests, BeautifulSoup4, contextlib and redirect_stdout) in Resilient Integration Server using the Command “pip install Package name”

# Installation:

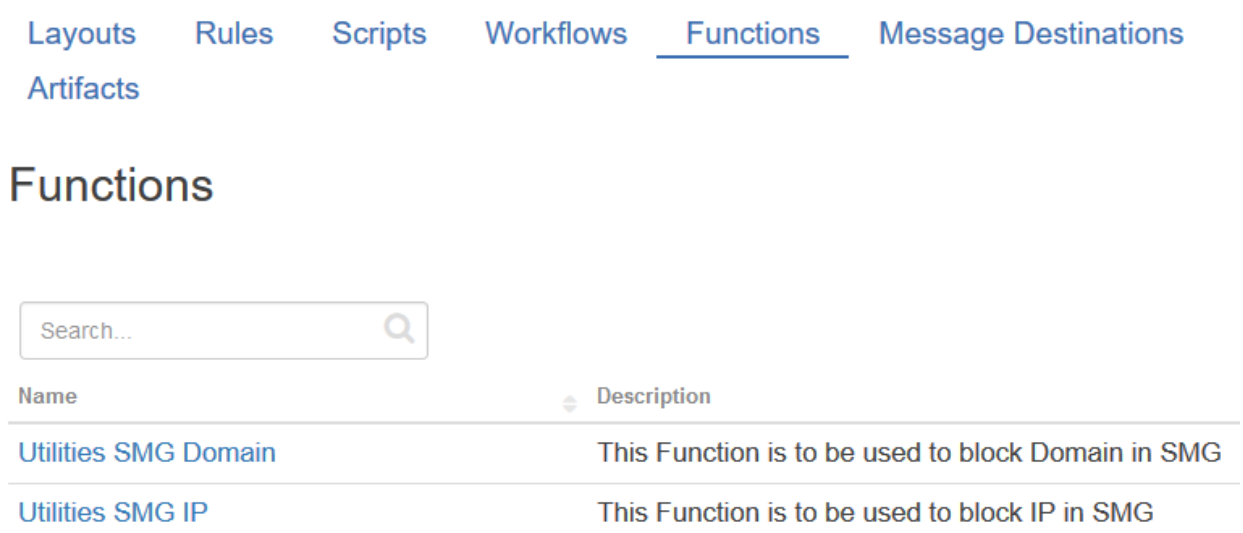
1- **Ensure that the environment is up-to-date, as follows:**
   **sudo pip install --upgrade pip**
   **sudo pip install --upgrade setuptools**
   **sudo pip install --upgrade resilient-circuits**

2- **Run the following command to install the package:**
   **sudo pip install smg_utilities.tar.gz**
3- **Use one of the following commands to create or update the resilient-circuits configuration file. Use –c for new environments or –u for existing environments:**
   **resilient-circuits config –c**
   **or**
   **resilient-circuits config -u**
4- **In the app.config at [smg_utilities] section, edit the settings as follows:**

   smg_url=https://”smg ip”
   smg_username=username
   smg_password=password
   smg_log=/var/smg.log
   note: smg_log is to set here the directory to the log file you want in your integration server.

5- **Deploy customizations to the Resilient platform:**
   **resilient-circuits customize**
6- **Run the integration framework:**
   **resilient-circuits run**

# Function Descriptions:




## Utilities SMG Domain:

This function allows blocking any Domain Name in SMG.

## Utilities SMG IP:

This function allows blocking any IP Address in SMG.