IBM Resilient

Security Orchestration, Automation and Response Platform

MAAS360 INTEGRATION GUIDE v1.0

Resilient Security Orchestration, Automation and Response (SOAR) Platform MaaS360 Integration Guide

Version	Publication	Notes
1.0	June 2019	Initial release.

Table of Contents

1. Overview **5**
1.1. Use cases 5
2. Installation **6**
3. Package contents **7**
4. Custom layout **8**
5. MaaS360 Basic Search function **9**
6. Create Artifact for Device ID Script **10**
7. MaaS360 Action function **12**
8. Create Artifact for App ID Script **14**
9. **MaaS360 Stop App Distribution function** **16**
10. **Delete App function** **17**

1. Overview

The MaaS360 function package enables users to perform the following Mobile Device Management (MDM) actions:

- Basic device search.
- Get a list of software and versions installed on a device.
- Locate a device.
- Lock a device.
- Wipe a device.
- Cancel a pending wipe.
- Stop app distribution across specific target devices.
- Delete an app from the MaaS360 catalog.

This guide provides a description of the functions and components within the function package, any additional requirements, and a list of settings that need to be added to the Resilient Circuits app.config file.

2. Installation

You download the function package to a Resilient integration server, and from there you deploy the functions and components to a Resilient platform. These procedures are provided in the Resilient Integration Server Guide (PDF).

The functions included this package have the following requirements, which are above and beyond those listed in the *Resilient Integration Server Guide*.

- Resilient platform is version 31 or later.
- A new incident tab is needed in the Layouts section of the Resilient platform to contain two custom data tables.

After installing the package, Resilient Circuits creates a new section, fn_maas360, in the app.config file. You need to edit the following settings in that section.

```
[fn_maas360]

# Authentication settings
maas360_host_url=
maas360_billing_id=
maas360_platform_id=
maas360_app_id=
maas360_app_version=
maas360_app_access_key=
maas360_username=
maas360_password=
maas360_auth_url=/auth-apis/auth/1.0/authenticate/

# Basic Search Fn settings
maas360_basic_search_url=/device-apis/devices/2.0/search/customer/
# Limit number of devices returned at one time. Allowed page sizes: 25, 50, 100,
200, 250. Default value: 250
maas360_basic_search_page_size=25
# Optional - Match 0 (Default) indicates Partial match for Device Name, Username,
Phone Number. Match 1 indicates Exact match.
#maas360_basic_search_match=0
# Optional - Sort attribute. Possible values: lastReported (Default) or
installedDate
#maas360_basic_search_sort_attribute=lastReported
# Optional - Sort Order. Possible values: asc or dsc (Default)
#maas360_basic_search_sort_order=dsc

# Action Fn settings
maas360_locate_device_url=/device-apis/devices/1.0/locateDevice/
maas360_get_software_installed_url=/device-apis/devices/1.0/softwareInstalled/
maas360_lock_device_url=/device-apis/devices/1.0/lockDevice/
maas360_wipe_device_url=/device-apis/devices/1.0/wipeDevice/
# Required - Whether to notify the administrator on successful device wipe. “yes”
value enables this flag
maas360_wipe_device_notify_me=Yes
# Required - Whether to notify the user on successful device wipe. “yes” value
enables this flag.
maas360_wipe_device_notify_user=No
# Required - Comma separated list of other email addresses to notify on successful
device wipe
maas360_wipe_device_notify_others=email1, email2
maas360_cancel_pending_wipe_url= /device-apis/devices/1.0/cancelPendingWipe/

# Stop App Distribution Fn settings
maas360_stop_app_distribution_url=/application-
```

```
apis/applications/1.0/stopAppDistribution/

# Delete App Fn settings
maas360_delete_app_url=/application-apis/applications/1.0/deleteApp/

# Search Installed Apps Fn settings
maas360_search_installed_apps_url=/application-apis/installedApps/1.0/search/
# Limit number of devices returned at one time. Allowed page sizes: 25, 50, 100,
200, 250. Default value: 50
maas360_search_installed_apps_page_size=50
```

3. Package contents

The following table lists the functions included in the package, along with associated workflows and rules.

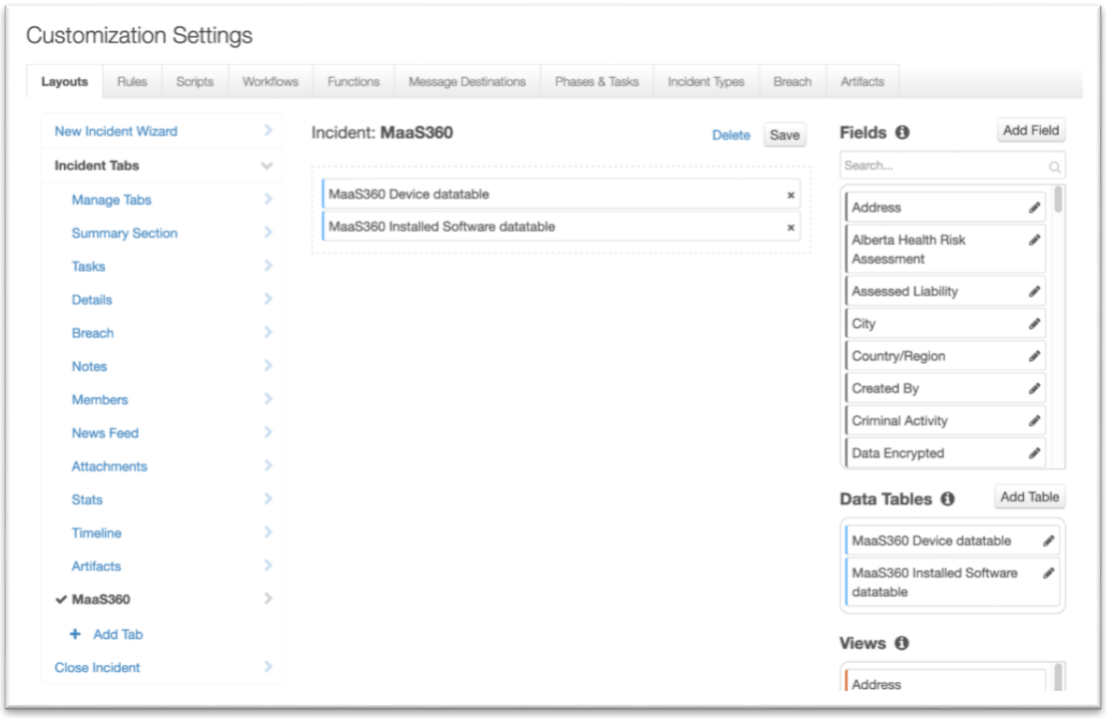
Function	Workflow/Script	Rule
MaaS360 Basic Search	Example: MaaS360 Basic Search Workflow	Example: MaaS360 Basic Search
MaaS360 Action	Example: MaaS360 Locate Device Workflow	Example: MaaS360 Locate Device
	Example: MaaS360 Lock Device Workflow	Example: MaaS360 Lock Device
	Example: MaaS360 Wipe Device Workflow	Example: MaaS360 Wipe Device
	Example: MaaS360 Cancel Pending Wipe Workflow	Example: MaaS360 Cancel Pending Wipe
	Example: MaaS360 Get Software Installed Workflow	Example: MaaS360 Get Software Installed
MaaS360 Stop App Distribution	Example: MaaS360 Stop App Distribution Workflow	Example: MaaS360 Stop App Distribution
MaaS360 Delete App	Example: MaaS360 Delete App Workflow	Example: MaaS360 Delete App
	Example: Create Artifact for App ID Script	Example: Create Artifact for App ID
	Example: Create Artifact for Device ID Script	Example: Create Artifact for Device ID

The package also requires that the following objects are created in the Resilient platform:

- Action fields:
  Device Group ID
  App type
  Device ID
  Device name
  Email
  Imei/Meid
  Phone no
  Platform name
  Username
  Target devices
- Data tables:
  MaaS360 Device data table
  MaaS360 Installed Software data table
- Incident artifact types:
  MaaS360 App ID
  MaaS360 Device ID

4. Custom layout

To use the functions, the Resilient playbook designer needs to create a new Incident tab containing the two data tables. The examples in this guide assume that the incident tab is named MaaS360. For example:



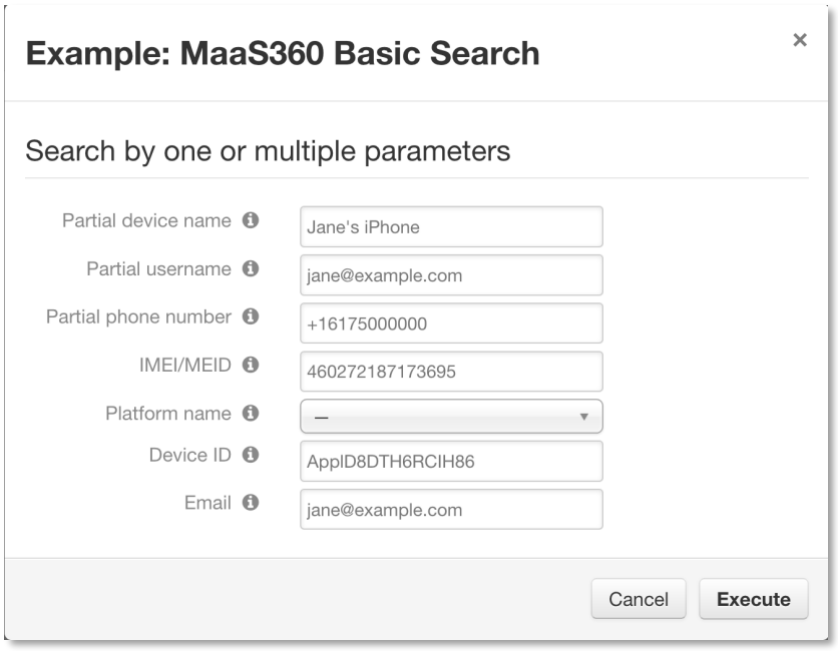
5. MaaS360 Basic Search function

The Basic Search function searches for MaaS360 devices by Device Name, Username, Phone Number, Platform, Device Status and other Device Identifiers. It supports partial match for Device Name, Username, and Phone Number.

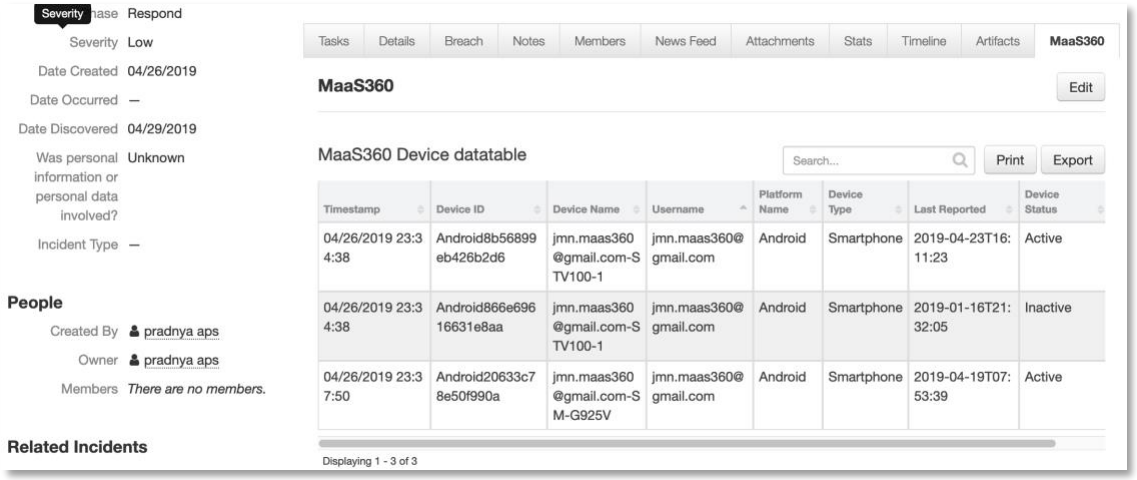
The function uses the following input parameters:

- maas360_partial_device_name: Partial or full Device Name string to be used in the search.
- maas360_partial_username: Partial or full Username string to be used in the search.
- maas360_partial_phone_no: Partial or full Phone Number to be used in the search.
- maas360_imei_meid: Full IMEI or MEID of the device.
- maas360_platform_name: Name of the operating system, such as Windows, Mac, iOS, BlackBerry, Android, Windows Mobile, Symbian, Windows Phone 7 or Others.
- maas360_device_id: Full MaaS360 Device ID string to be used in the search.
- maas360_email: Full Email address string to be used in the search.

The input fields are populated by the workflow, “Example: MaaS360 Basic Search”. The workflow sets the function’s input fields to values a user provides as part of an action initiated by the rule, “Example: MaaS360 Basic Search”. For example:

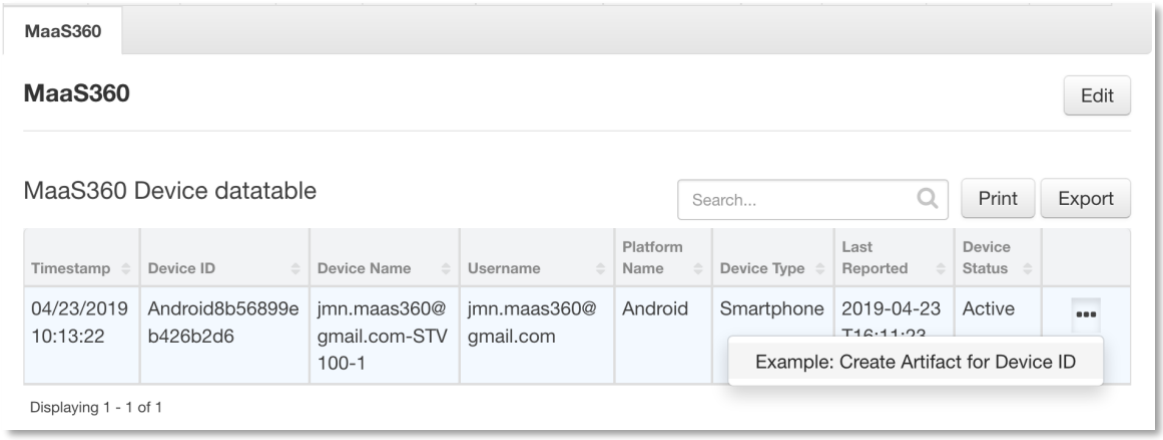


The workflow uses the results to populate the “MaaS360 Device datatable”. For example:

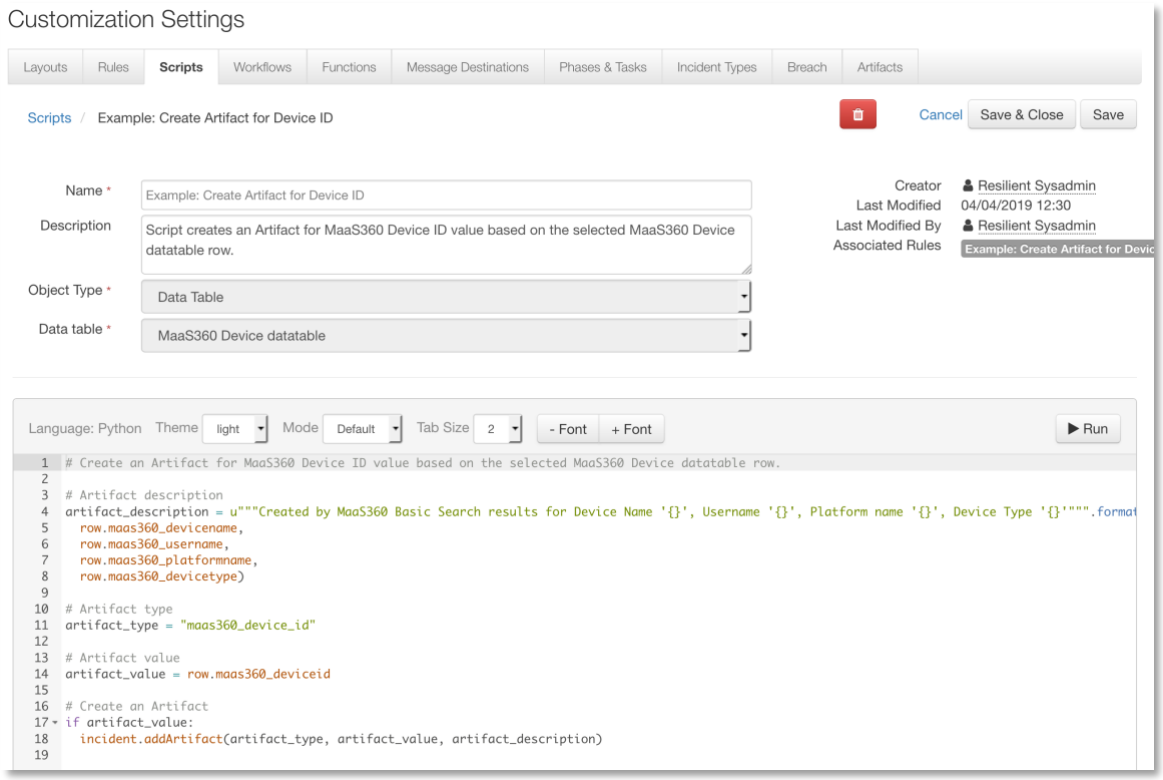


6. Create Artifact for Device ID Script

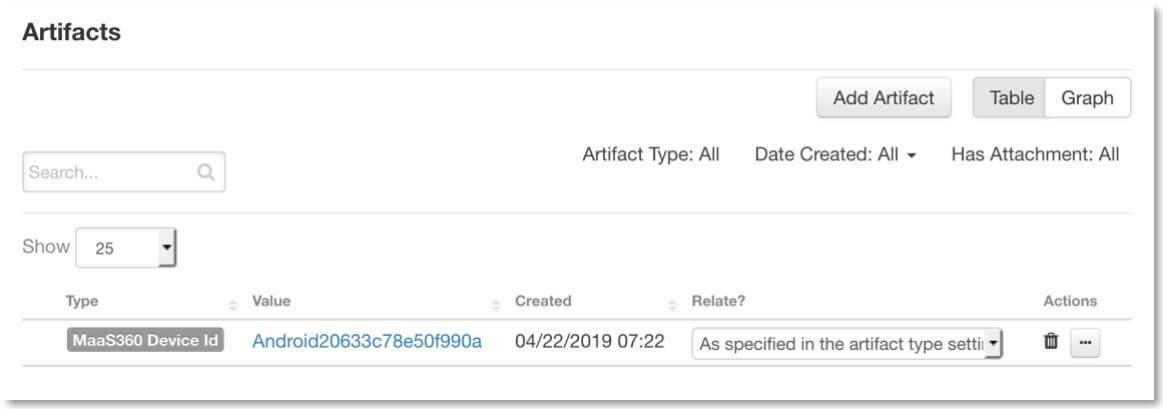
A user can execute the “Example: Create Artifact for Device ID” rule on selected row of “MaaS360 Device datatable”.



The rule initiates the “Example: Create Artifact for Device ID” script.



The script generates an artifact of type “Maas360 Device ID” in the Artifact tab.



7. MaaS360 Action function

The Action function performs different actions based on the chosen rule. Available actions are:

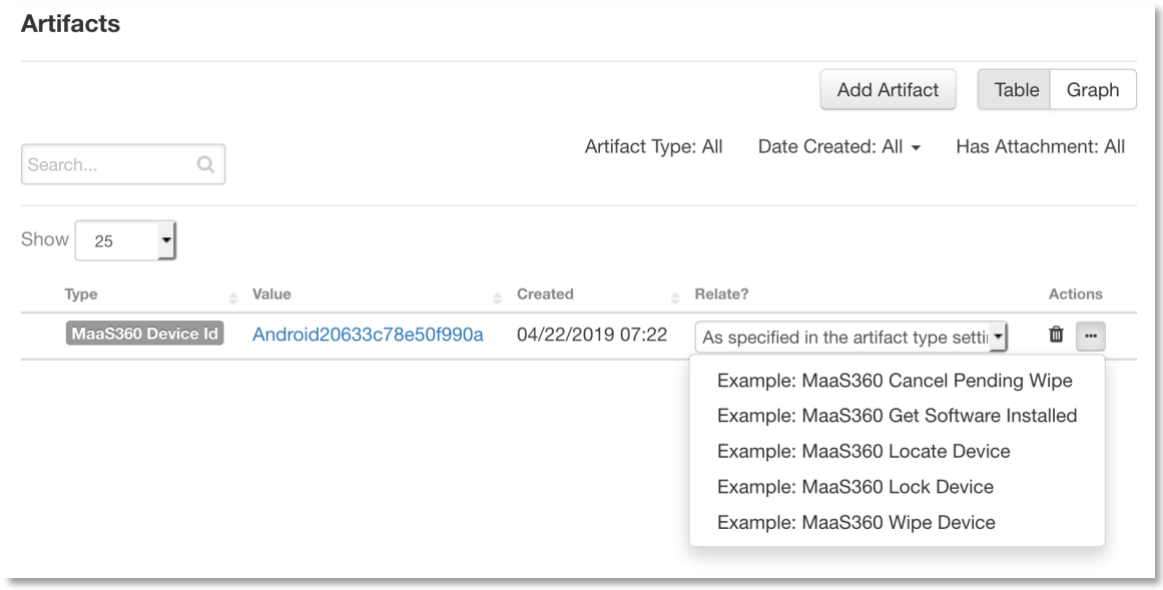
- Get Software Installed,
- Locate Device,
- Lock Device,
- Wipe Device and
- Cancel Pending Wipe.

It uses two input parameters:

- maas360_device_id: Full MaaS360 Device ID string to be used in the search.
- maas360_action_type: Field that is automatically set based on the chosen workflow action.

One of the five MaaS360 action workflows sets the function's two input fields:

- maas360_device_id is mapped to the chosen artifact value.
- maas360_action_type is the chosen Workflow action.



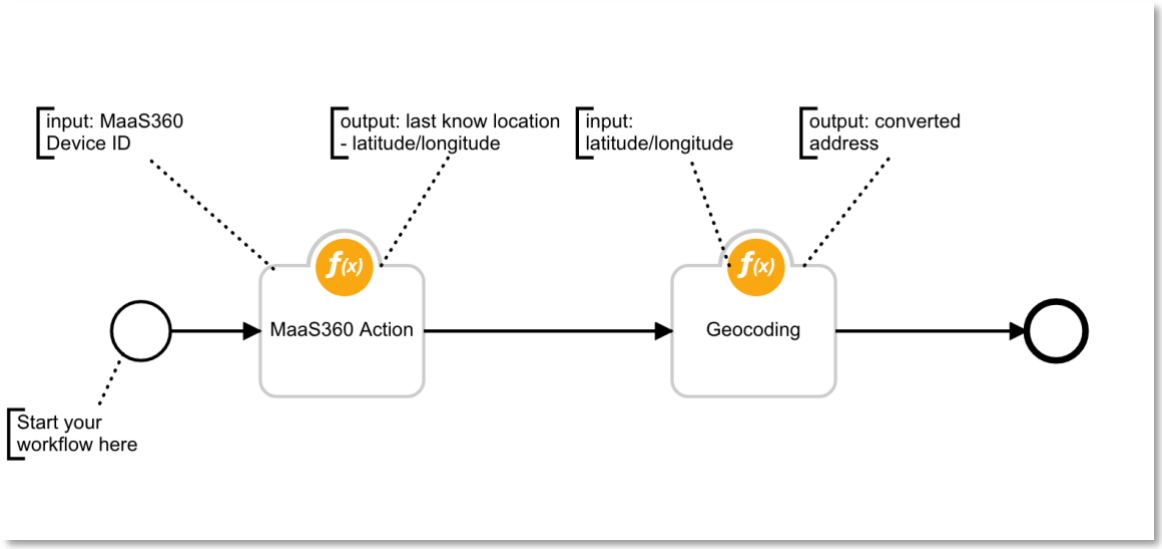
A user can select one of the actions to perform on the artifact:

- Example: Maas360 Get Software Installed Rule

  The “Example: Maas360 Get Software Installed” rule has an Artifact object type. To perform a get software installed action, the user selects this rule to initiate the workflow. The “Example: MaaS360 Get Software Installed” workflow calls a function that retrieves a list of installed software for a device. The workflow uses the results to populate the “MaaS360 Installed Software datatable”.

- Example: MaaS360 Locate Device Rule

  The “Example: MaaS360 Locate Device” rule has an Artifact object type. When users invokes this rule, it initiates the “Example: MaaS360 Locate Device” workflow. The workflow calls a function that performs a real-time lookup on Android devices or provides last known location on iOS and Windows Phone devices. The results are latitude and longitude information saved in the Notes tab. Users can chain this function with the Google Geocoding Functions for Resilient package, available on App Exchange, to provide conversion of address on latitude and longitude information.



- Example: MaaS360 Lock Device Rule

  The “Example: MaaS360 Lock Device” rule has an Artifact object type. When selected, this rule initiates the “Example: MaaS360 Lock Device” workflow, which calls a function that locks the device. A note about action response is saved in the Notes tab.

- Example: MaaS360 Wipe Device Rule

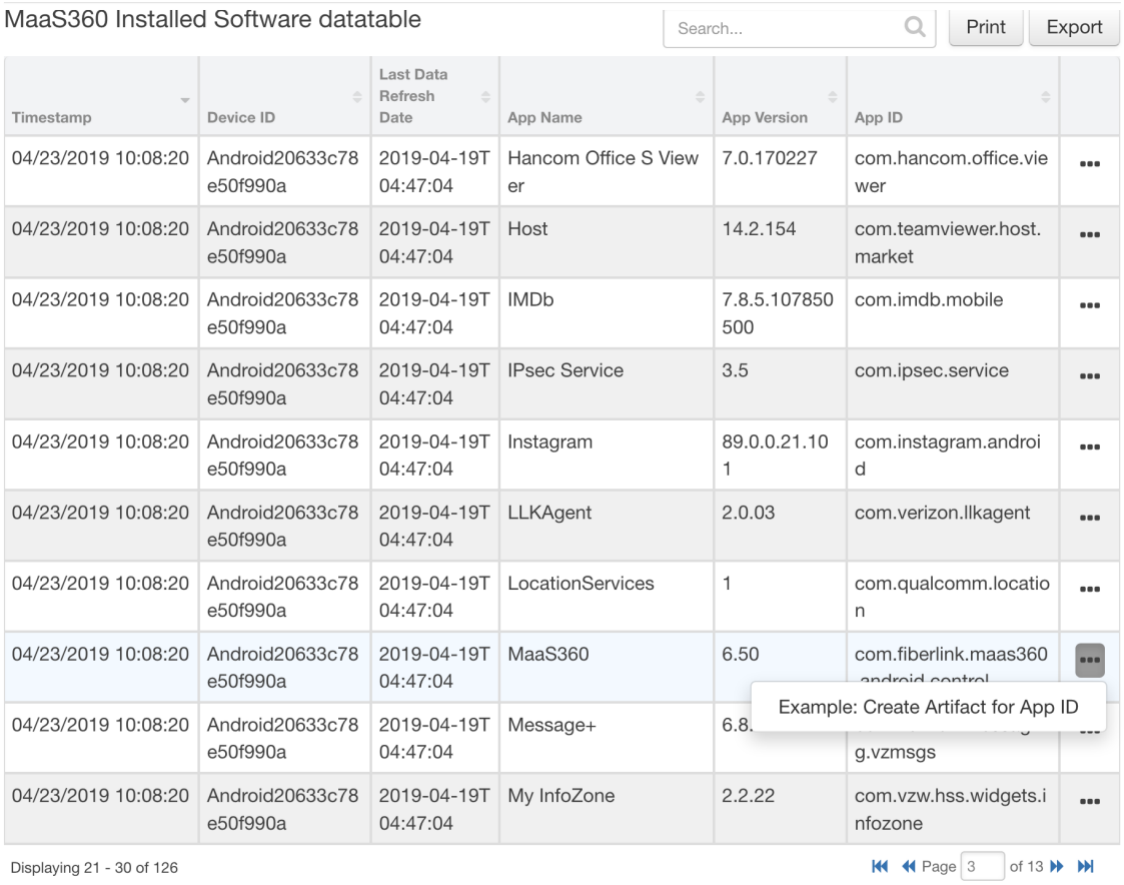
  The “Example: MaaS360 Wipe Device” rule has an Artifact object type. When selected, this rule initiates the “Example: MaaS360 Wipe Device” workflow, which calls a function that performs a remote wipe of the device. A note about action response is saved in the Notes tab.

- Example: MaaS360 Cancel Pending Wipe Rule

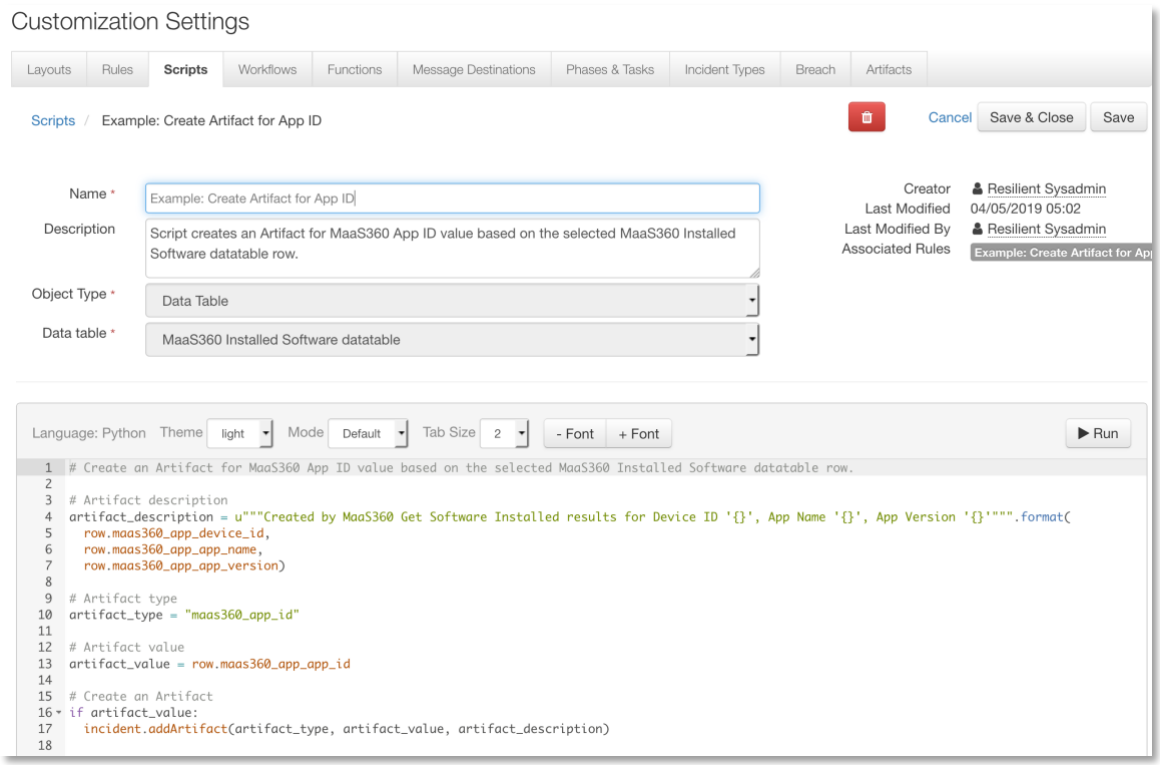
  The “Example: MaaS360 Cancel Pending Wipe” rule has an Artifact object type. When selected, this rule initiates the “Example: MaaS360 Cancel Pending Wipe” workflow, which calls a function that cancels an outstanding Remote Wipe sent to the device. A note about action response is saved in the Notes tab.

8. Create Artifact for App ID Script

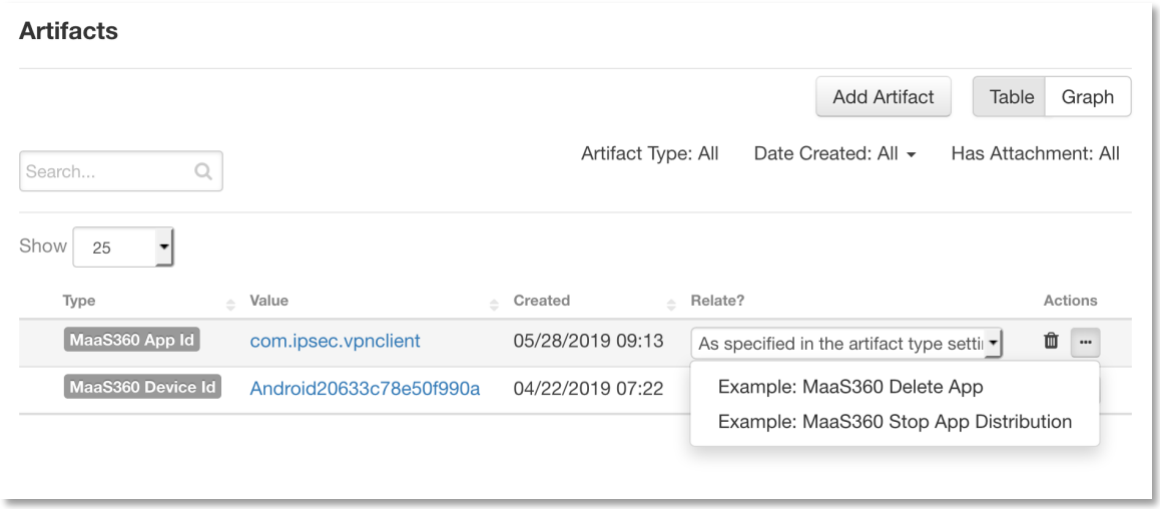
A user can execute the “Example: Create Artifact for App ID” rule on a selected row of the “MaaS360 Installed Software datatable”.



The rule initiates the “Example: Create Artifact for Device ID” script.



The script generates an artifact of type “Maas360 Device ID” in Artifact tab.



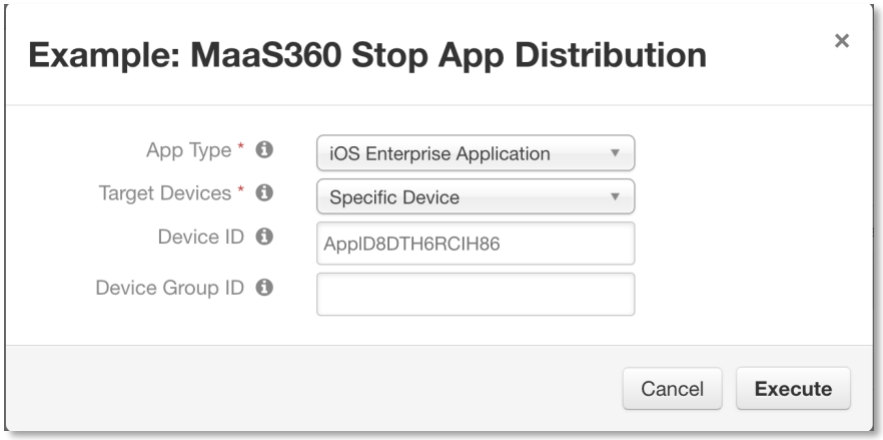
9. MaaS360 Stop App Distribution function

This function stops a distribution of an app across specific target devices. A distribution is a job scheduled to deploy an app from MaaS360 App Catalog to a group of users. Stopping a distribution cancels the distribution job. Optionally, the app could also be removed from the device (but this is dependent on how it was deployed initially and the type of device).

It uses the following input parameters:

- maas360_app_type: One of iOS Enterprise Application, iOS App Store Application, Android Enterprise Application, or Android Market Application.
- maas360_app_id: Unique ID of the application.
- maas360_target_devices: One of All Devices, Device Group, or Specific Device.
- maas360_device_id: Full MaaS360 Device ID string
- maas360_device_group_id is MaaS360 Device Group ID

The input fields are populated by the workflow, “Example: MaaS360 Stop App Distribution”. The workflow sets the function’s input fields to values a user provides as part of an action initiated by the rule, “Example: MaaS360 Stop App Distribution” available on the artifact. The “maas360_app_id” input field is mapped to the chosen artifact value. A note about action response is saved in Notes tab.



10. Delete App function

This function stops any existing distributions of the app and deletes the app from MaaS360 App Catalog. Stopping distributions cancels any existing distribution job, which in turn removes the app from the App Catalog (for user-initiated installs). Optionally, the app could also be removed from the device (but this is dependent on how it was deployed initially and the type of device). It cannot be distributed to anyone if it has been deleted.

It uses two input parameters:

- maas360_app_type: One of iOS Enterprise Application, iOS App Store Application, Android Enterprise Application, or Android Market Application.
- maas360_app_id: Unique ID of the application.

The input fields are populated by the workflow, “Example: MaaS360 Delete App”. The workflow sets the function’s input fields to values a user provides as part of an action initiated by the rule, “Example: MaaS360 Delete App” available on the artifact. The “maas360_app_id” input field is mapped to the chosen artifact value. A note about action response is saved in Notes tab.