
TA-ms-teams-alert-action Documentation

Release 1

Guilhem Marchand

Aug 12, 2021

Contents

1 Overview:	5
1.1 About	5
1.2 Compatibility	5
1.3 Support & donate	5
1.4 Download	6
2 Deployment and configuration:	7
2.1 Deployment & Upgrades	7
2.2 Configuration and usage	8
3 Versions and build history:	15
3.1 Release notes	15

This application provides alert actions for Microsoft Teams messages publication to allows advanced messages publication from Splunk, including:

- Markdown support
- Defining options globally or on a per alert basis (per alert override)
- Defining comma separated list of fields which will be dynamically used to generated the markdown supported publication
- Choosing icon link for message publication
- Activating potential link action and defining its link

The screenshot shows the Splunk interface for the 'MS Teams alert action'. At the top, there's a navigation bar with 'Overview - Microsoft Teams messages publication' selected. Below this, a summary dashboard shows four metrics: 16 Messages Publication Successes, 26 Messages Publication Temporary Failures, 0 Messages Currently in the Replay KVStore, and 6 Messages Replay Store Temporarily Failed.

The 'Microsoft Teams channel messages creation workflow' section lists several steps:

- When a channel message creation is requested, the modular alert attempts an http POST to the channel Webhook URL, and logs its activity in `(index="_internal" OR index="cim_modactions") (source="ms_teams_publish_to_channel_modalert.log")`
- If the channel message creation is successful, the keyword **"Microsoft Teams message successfully created"** is logged
- Should the channel message creation fail for any reason, the keyword **"Microsoft Teams message creation has failed"** is logged, and the message data is stored automatically in the replay KVstore (`!inputlookup ms_teams_failures_replay | eval uuid=__key`)
- This is a temporary failure as the replay backend handles automatically failed messages stored in the KVstore, and attempts again the creation via the scheduled alert **"MS Teams - Resilient store Tracker"**
- The replay issue backend logs its activity in `(index="_internal" OR index="cim_modactions") (source="ms_teams_publish_to_channel_replay_modalert.log")`
- Messages stored in the replay KVstore are attempted when the replay alert triggers (every 5 minutes), a temporary failed message will be attempted during a **period of 3 days**
- Once the message referenced by a uuid has reached the 3 days period, it is tagged as a permanent failure, and the alert **"MS Teams - detection of permanent issue creation failure"** triggers warning about its permanent failure
- A message in a permanent failure state will not be attempted anymore, **7 days after its initial creation**, the message is finally tagged for removal and will be purged automatically from the replay KVstore
- As such, a channel message issue that initially failed to be created is **automatically retried during 3 days, and definitively purged after 7 days**

Below the workflow is a bar chart showing the status of messages over time. The y-axis is labeled 'status' and ranges from 0 to 75. The x-axis shows time intervals from 11:10 to 11:55. The chart shows several bars with different colors (green, orange, red) representing different message statuses.

The 'Status:' dropdown is set to 'ANY'. There are two tabs: 'First call activity' (selected) and 'Resilient store activity'.

The logs table below shows the following data:

_time	status	app	action_mode	sid	search_name	user	_raw
2020-04-26 12:13:10.299	✓	search	saved	scheduler__admin__search__RMD57fd780474f31ef7e_at_1587899580_1267	JIRA Qualification public addon test	admin	2020-04-26 12:13:10,299 INFO pid=88275 tid=MainThread file=cim_actions.p
2020-04-26 12:13:05.763	✓	search	saved	scheduler__admin__search__RMD57fd780474f31ef7e_at_1587899580_1267	JIRA Qualification public addon test	admin	2020-04-26 12:13:05,372 INFO pid=88275 tid=MainThread file=setup_util.py
2020-04-26 12:13:05.763	✓	search	saved	scheduler__admin__search__RMD57fd780474f31ef7e_at_1587899580_1267	JIRA Qualification public addon test	admin	2020-04-26 12:13:05,838 INFO pid=88195 tid=MainThread file=setup_util.py
2020-04-26 12:13:05.763	✓	search	saved	scheduler__admin__search__RMD57fd780474f31ef7e_at_1587899580_1267	JIRA Qualification public addon test	admin	2020-04-26 12:13:05,963 INFO pid=88195 tid=MainThread file=cim_actions.p
2020-04-26 12:12:09.800	✗	search	saved	scheduler__admin__search__RMD57fd780474f31ef7e_at_1587899520_1264	JIRA	admin	2020-04-26 12:12:09,800 INFO pid=88054 tid=MainThread file=cim_actions.p

Configuration

Set up your add-on

Proxy Logging **Teams Add-on configuration**

Default MS team channel:
Webhook URL. (https enforced, can be overridden on a per alert basis)

Default MS teams image link:
Picture URL (can be overridden on a per alert basis)

URL regex compliancy checker:
You can define a regular expression used to verify that URL is compliant with your rules

SSL certificate validation:
Check this box to perform SSL certificate validation

Save

When triggered
MS teams publish to channel Remove

Override default Webhook URL:

Enter the Webhook URL to be used for this alert, this overrides any global setting defined in the addon. (https is enforced and will be added automatically if necessary, can be overridden on a per alert basis)

Message Activity Title *

Enter the Activity Title for this message, this can include dynamic results. (\$result.field\$) This field is required.

Message fields list *

Enter the comma separated list of fields to include in the message. Each field has to be a field resulting from the search.

Override MS teams image link for publication:

URL of the picture to be used for messages publication for this alert.

Potential Action Name:

Enter the name of the potential action that will be made available in the channel message.

Potential Action URL:

Enter the value for the potential action URL that will be made available in the message.

1.1 About

- Author: Guilhem Marchand, Splunk certified consultant and part of Splunk Professional Services
- First release published in January 2020
- License: Apache License 2.0

1.2 Compatibility

1.2.1 Splunk compatibility

Since the version 1.1.x, the application is compatible with Splunk 8.0.x and later only.

The latest release available for Splunk 7.x is the release 1.0.20.

1.2.2 Web Browser compatibility

The application can be used with any of the supported Web Browser by Splunk:

<https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements>

1.3 Support & donate

I am supporting my applications for free, for the good of everyone and on my own private time. As you can guess, this is a huge amount of time and efforts.

If you enjoy it, and want to support and encourage me, buy me a coffee (or a Pizza) and you will make me very happy!

This application is community supported.

To get support, use of one the following options:

1.3.1 Splunk Answers

Open a question in Splunk answers for the application:

- <https://answers.splunk.com/app/questions/4855.html>

1.3.2 Splunk community slack

Contact me on Splunk community slack, and even better, ask the community!

- <https://splunk-usergroups.slack.com>

1.3.3 Open a issue in Git

To report an issue, request a feature change or improvement, please open an issue in Github:

- <https://github.com/guilhemmarchand/TA-ms-teams-alert-action/issues>

1.3.4 Email support

- guilhem.marchand@gmail.com

However, previous options are far better, and will give you all the chances to get a quick support from the community of fellow Splunkers.

1.4 Download

The Splunk application can be downloaded from:

1.4.1 Splunk base

- <https://splunkbase.splunk.com/app/4855>

1.4.2 GitHub

- <https://github.com/guilhemmarchand/TA-ms-teams-alert-action>

Deployment and configuration:

2.1 Deployment & Upgrades

2.1.1 Deployment matrix

Splunk roles	required
Search head	yes
Indexer tiers	no

If Splunk search heads are running in Search Head Cluster (SHC), the Splunk application must be deployed by the SHC deployer.

2.1.2 Dependencies

There are currently no dependencies for the application.

However, if you deploy the `Splunk_SA_CIM` package, make sure you have declared the `cim_modactions` index as the Add-on logs would automatically be directed to this index if the SA CIM application is installed on the search heads.

If the `Splunk_SA_CIM` is not installed, the Add-on logs will be generated in the `_internal` index. (This is a normal behaviour for Add-on developed with the Splunk Add-on builder that provide adaptive response capabilities)

2.1.3 Initial deployment

The deployment of the Splunk application is very straight forward:

- Using the application manager in Splunk Web (Settings / Manages apps)
- Extracting the content of the `tgz` archive in the “apps” directory of Splunk

- For SHC configurations (Search Head Cluster), extract the tgz content in the SHC deployer and publish the SHC bundle

2.1.4 Upgrades

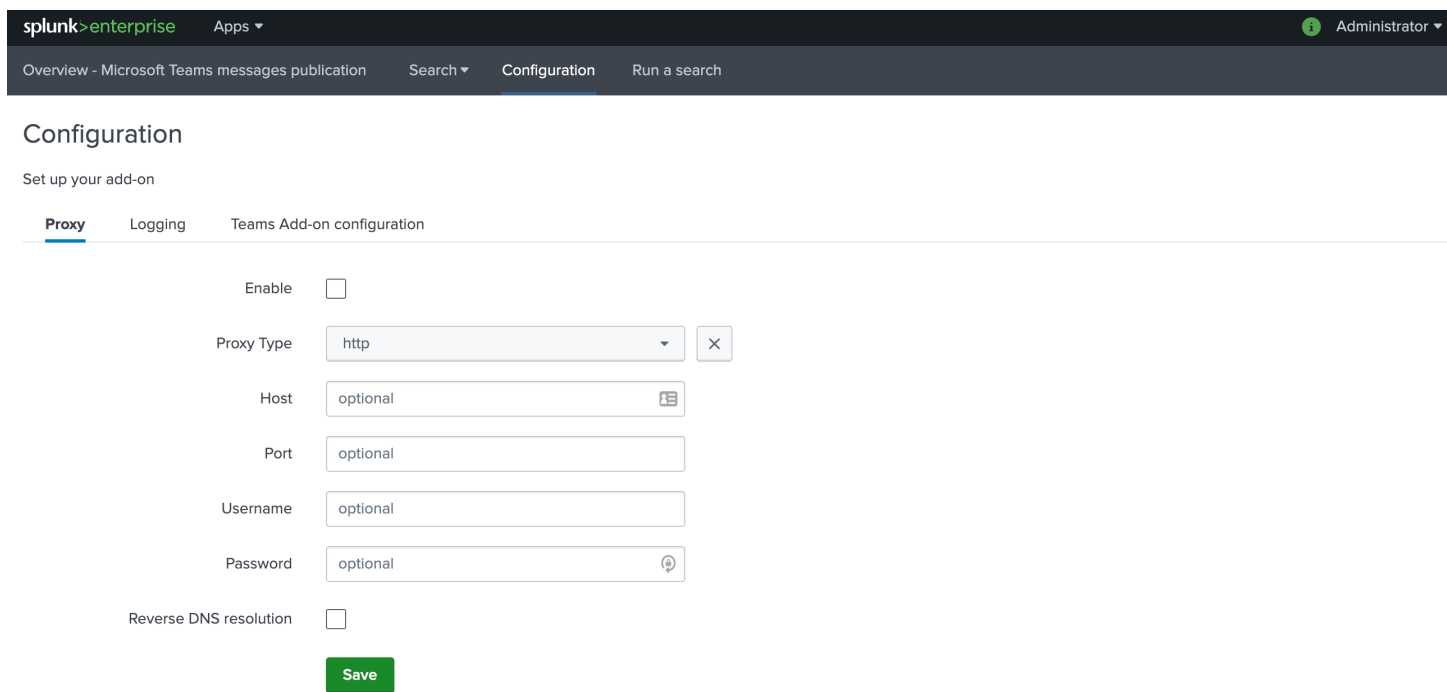
Upgrading the Splunk application is pretty much the same operation than the initial deployment.

2.2 Configuration and usage

2.2.1 Global configuration

Once the application has been deployed, you can access to the main standard configuration and the app related items by opening the app and accessing to the configuration navigation bar menu:

Configuration home page:



The screenshot shows the Splunk configuration interface for the Teams Add-on. The top navigation bar includes 'splunk > enterprise', 'Apps', and 'Administrator'. The main navigation bar shows 'Overview - Microsoft Teams messages publication', 'Search', 'Configuration', and 'Run a search'. The 'Configuration' section is active, displaying 'Set up your add-on' and three tabs: 'Proxy', 'Logging', and 'Teams Add-on configuration'. The 'Proxy' tab is selected, showing the following configuration options:

- Enable:
- Proxy Type:
- Host:
- Port:
- Username:
- Password:
- Reverse DNS resolution:

A green 'Save' button is located at the bottom of the configuration form.

Add-on settings:

The screenshot shows the Splunk configuration interface for the 'TA-ms-teams-alert-action' add-on. The breadcrumb trail is 'Overview - Microsoft Teams messages publication > Search > Configuration > Run a search'. The user is logged in as 'Administrator'. The 'Configuration' section is titled 'Set up your add-on' and has three tabs: 'Proxy', 'Logging', and 'Teams Add-on configuration' (which is selected). Under the 'Teams Add-on configuration' tab, there are four settings:

- Default MS team channel:** A text input field containing 'optional'. Below it, a note states: 'Webhook URL. (https enforced, can be overridden on a per alert basis)'. The field is marked as optional.
- Default MS teams image link:** A text input field containing 'optional'. Below it, a note states: 'Picture URL (can be overridden on a per alert basis)'. The field is marked as optional.
- URL regex compliancy checker:** A text input field containing '.*'. Below it, a note states: 'You can define a regular expression used to verify that URL is compliant with your rules'.
- SSL certificate validation:** A checkbox that is checked. Below it, a note states: 'Check this box to perform SSL certificate validation'.

A green 'Save' button is located at the bottom of the configuration area.

Default MS team channel

This defines a default Webhook URL to be used by default for the publication of messages.

The Webhook URL can be defined with or without `https://`, therefore https is enforced for certification compliance purposes and non SSL traffic is not allowed.

Finally, the default channel Webhook URL can be overridden on a per alert basis, this global configuration is only used if the per alert URL is not set.

This setting is optional and can be let unset in the global app configuration.

Default MS teams image link

In a similar fashion, this defines the icon link to be used by default when publishing to channels, this setting can be overridden on a per alert basis as well.

This setting is optional and and can be let unset in the global app configuration.

URL regex compliancy checker

To avoid allowing the target URL to be set to a free value, and prevent data exfiltration, you use this option to define a valid regular expression that will be applied automatically when the alert action triggers.

If the regular expression does not match the target URL, the alert action will be refused and the Python backend will not proceed to the Webhook call.

For instance, you can include a simple literal expression to match your tenant ID:

<https://mydomain.ic365.webhook.office.com/webhookb2/>

If an alert is attempting to publish a message that does not comply with the regex check, the Add-on logs will return an error and the publication will not be executed:

i	Time	Event
>	06/08/2021 06:40:01.094	2021-08-06 06:40:01,094 ERROR pid=7134 tid=MainThread file=cim_actions.py:message:280 : liancy check setting defined in the global configuration, therefore the operation cannot min__search__RMD5b459547088ed72c1_at_1628232000_29" rid="0" app="search" user="admin" ac host = splunk source = /opt/splunk/var/log/splunk/ms_teams_publish_to_channel_modalert.log

SSL certificate validation

If the option is checked, the Python backend will require the SSL certificate to be a valid certificate.

2.2.2 Per alert configuration

When activating the Microsoft Teams channel publication alert action, different options are made available:

When triggered	<div style="display: flex; justify-content: space-between; align-items: center;"> MS teams publish to channel Remove </div> <div style="margin-top: 10px;"> <p>Override default Webhook URL: <input type="text" value="https://webhook.site/f0bf62c0"/></p> <p>Message Activity Title * <input type="text" value="Brand new MS teams addon fr"/></p> <p>Message fields list * <input type="text" value="time,action,user,message"/></p> <p>Override MS teams image link for publication <input type="text" value="http://i.imgur.com/c4jt321l.png"/></p> <p>Potential Action Name <input type="text" value="Open in Splunk"/></p> <p>Potential Action URL <input type="text" value="https://www.splunk.com"/></p> </div>
----------------	--

Override default Webhook URL

This defines the Webhook URL for the message publication, and will override any existing global configuration.

This item is optional only if the global equivalent has been set (obvious), similarly to global https is automatically enforced.

Message Activity Title

This defines the main title of the message to be published, this setting is required.

Message fields list

This defines a comma separated list of fields which result from the alert, these fields will be automatically extracted and formatted to be part of the published message.

This setting is required, and at least one field needs to be defined.

Override MS teams image link for publication

This defines the icon link to be used for the message publication, and will override any global setting that has been set.

Theme color

Specifies a custom brand color for the card in hexadecimal code format. (optional, defaults to 0076D7)

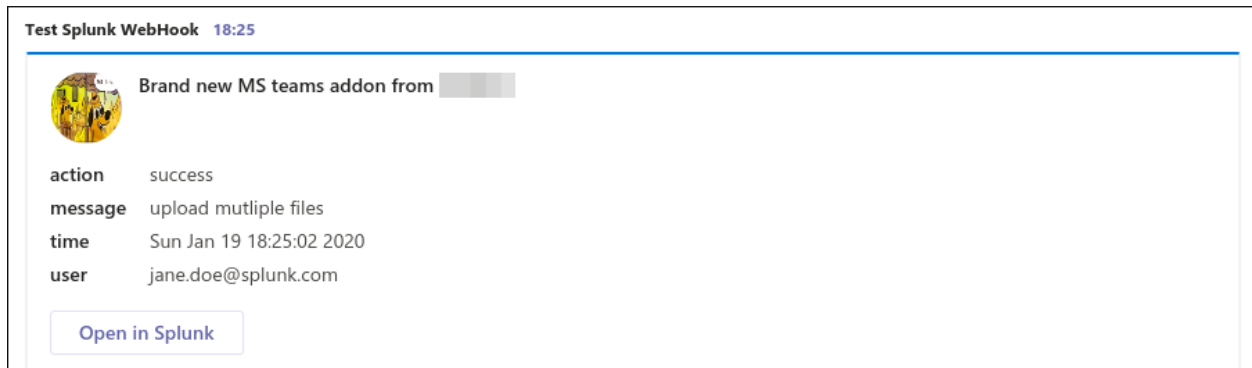
Potential Action Name and URL

These two items define the action link button and target that can automatically be added when the message is published in Microsoft Teams.

For this option to be activated, both of these items need to be configured, note that the URL can accept dynamic input fields resulting from the search.

A second OpenURI action can be added.

Message example:



HttpPOST Action

You can add an HttpPOST action which users can use directly in Microsoft Teams, this allows interacting with Splunk or an external system directly within the Teams interface.

For more information, please consult the following documentation:

<https://docs.microsoft.com/en-us/outlook/actionable-messages/message-card-reference>

2.2.3 Status dashboard

An overview dashboard is available as the home page in the application to provide a minimal view over messages successfully published, and failures if any:

Microsoft Teams channel message creation workflow:

- When a channel message creation is requested, the modular alert attempts an http POST to the channel Webhook URL, and logs its activity in `[index="internal" OR index="cim_moderations"] [source="ms_teams_publish_to_channel_modalert.log]`
- If the channel message creation is successful, the keyword `"Microsoft Teams message successfully created"` is logged
- Should the channel message creation fail for any reason, the keyword `"Microsoft Teams message creation has failed"` is logged, and the message data is stored automatically in the replay KVstore `[inputlookup ms_teams_failures_replay | eval uid="key"]`
- This is a temporary failure as the replay backend handles automatically failed messages stored in the KVstore, and attempts again the creation via the scheduled alert `"MS Teams - Resilient store Tracker"`
- The replay issue backend logs its activity in `[index="internal" OR index="cim_moderations"] [source="ms_teams_publish_to_channel_replay_modalert.log]`
- Messages stored in the replay KVstore are attempted when the replay alert triggers (every 5 minutes), a temporary failed message will be attempted during a **period of 3 days**
- Once the message referenced by a uid has reached the 3 days period, it is logged as a permanent failure, and the alert `"MS Teams - detection of permanent issue creation failure"` triggers warning about its permanent failure
- A message in a permanent failure state will not be attempted anymore, **3 days** after its initial creation, the message is finally logged for removal and will be purged automatically from the replay KVstore
- As such, a channel message issue that initially failed to be created is **automatically retried during 3 days, and definitively purged after 7 days**

_time	status	app	action_mode	sid	search_name	user	_raw
2020-04-26 12:13:18.299	✓	search	saved	scheduler_admin_search_09075f788474731e776_at_1587899588_1267	7394	admin	2020-04-26 12:13:18.299 INFO pid=88275 tid=MainThread file:in_actions.py:message:243 sendnotification - signature=Alert action Microsoft Teams publish to chan public addn
2020-04-26 12:13:18.763	✓	search	saved	scheduler_admin_search_09075f788474731e776_at_1587899588_1267	7394	admin	2020-04-26 12:13:18.763 INFO pid=88195 tid=MainThread file:in_actions.py:message:243 sendnotification - signature=Alert action Microsoft Teams publish to chan public addn
2020-04-26 12:13:19.088	✗	search	saved	scheduler_admin_search_09075f788474731e776_at_1587899588_1264	7394	admin	2020-04-26 12:13:19.088 INFO pid=88284 tid=MainThread file:in_actions.py:message:243 sendnotification - signature=Alert action Microsoft Teams publish to chan test

Should there be any failures in publishing messages, the related information and logs are made available easily. In addition, several reports and links provide quick access to the logs location.

2.2.4 Out the box alert for publishing failures detection

For a total operational safety, a builtin Splunk alert is provided which you can enable to get alerted if any messages failed to be published:

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

1 Alerts

i	Title	Actions	Owner	App	Sharing	Status
1	MS Teams - detection of messages publication failure	Open in Search Edit	nobody	TA-ms-teams-alert-action	Global	Disabled

This alert performs detection of MS Teams publication failures

Enabled: No. Enable

Permissions: Shared Globally. Owned by nobody. Edit

Modified: 1 Jan 1970 00:00:00

Alert Type: Scheduled. Cron Schedule. Edit

Trigger Condition: Number of Results is > 0. Edit

Actions: 1 Action Edit

🔔 Add to Triggered Alerts

Failures for publication can have different causes like network issues, typo or misconfiguration, as always the truth will be in the logs.

2.2.5 Using the alert action for non admin users

For non admin users to be able to use the alert action, the following role is provided out of the box:

- `msteams_alert_action`

This role needs to be inherited for the users, or your users to be member of this role.

The role provides:

- `capability list_storage_passwords`

- capability `list_settings`
- write permission to the resilient KVstore `kv_ms_teams_failures_replay`

Versions and build history:

3.1 Release notes

3.1.1 Version 1.1.3

- Fix - Issue #40 - SHC replication fails, server.conf config missing in package

3.1.2 Version 1.1.2

- Fix - unexpected local.meta was delivered within the tgz release archive

3.1.3 Version 1.1.1

- Fix - Upgrade of Splunk ucc-gen to release 5.5.9 to fix an issue with the notification in configuration UI when an Add-on has no account section

3.1.4 Version 1.1.0

New major release: Migration from AoB framework to splunk-ucc-generator:

- Enhancement - the migration to splunk-ucc-generator provides a better and modern framework for Add-ons
- Change - support is dropped for Splunk 7.x, version 1.1.x only supports Splunk 8.x and Python3
- Change - JQuery migration for the Overview dashboard

3.1.5 Version 1.0.20

- Change - Issue #37 - Add help-link class, open in a new window, and external icon

3.1.6 Version 1.0.19

- Change - Issue #35 - Splunk Python SDK upgrade to 1.6.15

3.1.7 Version 1.0.18

- Feature: Issue #28 - Theme Color as configurable option #28

3.1.8 Version 1.0.17

- Fix: Issue #26 - ensure aob configuration replicates in shc environment #26
- Change: For Splunk Cloud vetting purposes, ensure https check verifies the URI starts by https rather than contains https

3.1.9 Version 1.0.16

- Fix: Splunk Cloud vetting failure due to session token available in debug mode

3.1.10 Version 1.0.15

- Fix: regression introduced in version 1.0.13 with the addition parameter for SSL verification, if a deployment is upgraded from a previous version, the alert would fail until an admin enters the configuration UI and saves the configuration again

3.1.11 Version 1.0.14

- Fix: Issue #20 Provides an option to disable SSL certificate verification (but enabled by default) to avoid failures with environments using SSL interception
- Feature: Issue #17 Provides an option on a per alert basis to allow ordering of the fields in the message by using the fields list ordering rather than alphabetical ordering
- Fix: SLIM error for app vetting due to the introduction of the targetWorkloads in app.manifest which requires version 2.0.0 of the app.manifest schema

3.1.12 Version 1.0.13

- Fix: Issue #20 Provides an option to disable SSL certificate verification (but enabled by default) to avoid failures with environments using SSL interception
- Feature: Issue #17 Provides an option on a per alert basis to allow ordering of the fields in the message by using the fields list ordering rather than alphabetical ordering

3.1.13 Version 1.0.12

- Fix: Default timed out value during REST calls are too short and might lead to false positive failures and duplicated creation of messages

3.1.14 Version 1.0.11

- Change: For Splunk Cloud vetting purposes, enforce https verification in `modalert_ms_teams_publish_to_channel_replay_helper.py`
- Change: For Splunk Cloud vetting purposes, explicit Python3 mode in `restmap.conf` handler

3.1.15 Version 1.0.10

- Change: For Splunk Cloud vetting purposes, SSL verification is now enabled for any external communications

3.1.16 Version 1.0.9

- Fix: Provide an embedded role `msteams_alert_action` that can be inherited for non admin users to be allowed to fire the action and work with the resilient store feature

3.1.17 Version 1.0.8

- unpublished

3.1.18 Version 1.0.7

- Feature: Integration of the resilient store capabilities, which rely on a KVstore to automatically handle and retry temporary message creation failures with resiliency
- Feature: Overview dashboard update to reflect the resilient store integration, news reports and alerts
- Fix: Metadata avoid sharing alerts, reports and views at global level

3.1.19 Version 1.0.6

- Fix: Proxy configuration was not working and not used
- Change: Overview dashboard switched to dark theme
- Change: Configure URL message update

3.1.20 Version 1.0.5

- Fix: Global settings are not properly use and do not define default values to be overridden on a per alert basis, this release fixes these issues
- Fix: Events iteration issue, if one was defining a massive alert with no by key throttling, building the Json object would fail
- Fix: Json escape character protection for OpenURI values (Open URL potential action)

3.1.21 Version 1.0.4

- Fix: Fields resulting from the Splunk search stored in the facts section of the message card were not ordered alphabetically properly, this is now fixed and fields are systematically sorted
- Feature: Allows activating a second openURL potential action per alert
- Feature: Allows defining an HttpPOST potential action in MS Teams per alert
- Fix: Better and shorter explanation of options

3.1.22 Version 1.0.3

- Fix: Order json object alphabetically before post operation to provide ordered fields in message publication.
- Fix: Sourcetype on non CIM deployments within saved searches and overview dashboard.
- Fix: Disable markdown support for text value fields to avoid being wrongly interpreted by Teams, in the context of Splunk we most likely want potentially piece raw block of text.

3.1.23 Version 1.0.2

- Fix: Timechart not working in overview to bad field name

3.1.24 Version 1.0.1

- Fix: avoids publication failure due to json illegal characters

3.1.25 Version 1.0.0

- initial and first public release