IBM Resilient SOAR Platform
Web URL Integration Guide
V34

Date: August 2019

IBM **Security**

**Resilient SOAR Platform
Web URL Integration Guide**

Platform Version	Publication	Notes
34.0	August 2019	Initial publication.

Contents

Chapter 1. Overview

The Resilient Security, Orchestration and Response (SOAR) Platform supports a rich variety of programmable interfaces that can be used for integration with other systems. The simplest of these interfaces is the Web URL.

By directing a user's browser to specially-constructed Web URLs, the user can be guided through automatic creation of an incident, and other functions.

A typical use case for this integration is in manually creating Resilient incidents from within another system, such as a SIEM. This streamlines the process of escalation to the incident response team. For example, you can extend the SIEM's user interface to add custom commands and configurations. In these configurations, a simple customization creates a direct link from the user interface where users can immediately create and enrich incidents in the Resilient platform.

This document provides details and examples of the URL syntax, including examples of how to use them in practical integrations.

Chapter 2. Web URL methods

There are two methods for Web URL integration:

- **#external/new_by_url**: Creates a new incident.
- **#external/add_artifacts_by_url**: Adds artifacts to an existing incident.

The full URL for these is based at the Resilient platform normal address. For example, for server hostname, app.resilientsystems.com, and the default SSL port 443, the full URLs are as follows:

```
https://app.resilientsystems.com/#external/new_by_url?...
https://app.resilientsystems.com/#external/add_artifacts_by_url?...
```

The query-string parameters after '?' are documented in the following sections.
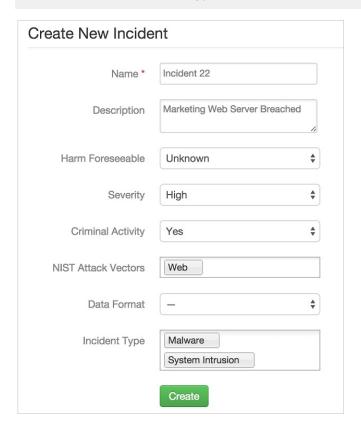
Chapter 3. New incident by URL

Opens a form for creating a new incident. The URL specifies which fields should be displayed on the form layout, and optional values for those fields. If a value is omitted, the field is shown on the form layout, but has no default value.

```
#external/new_by_url?field=[value]&field=[value]...
```

A full example is shown below, from the following URL:

```
https://app.resilientsystems.com/#external/new_by_url?name=Incident%2022&description=Marketing
%20Web%20Server
%20Breached&harmstatus_id=Unknown&severity_code=high&crimestatus_id=Yes&nist_attack_vectors=
Web&data_format=&incident_type_ids=19,20
```


Field names

Fields are specified by their "API name". Every field in the Resilient platform has a unique API name.

Fields in the form layout appear in the order that they are specified in the URL.

If a field name is specified in the URL but does not exist in the platform, it is ignored.

If a required field (for example 'name', or a custom field) is not specified in the URL, it appears in the "Review Fields" dialog, where it must be completed before the incident can be saved.

Field values

Values for fields with enumerated options. For example, you can specify "incident type" and "country", by their ID value or by the full text value; the enumerated code for country Belgium is 1038, so these two are equivalent.

```
#external/new_by_url?country=Belgium
#external/new_by_url?country=1038
```

Refer to the Chapter 6, "Standard fields and values," on page 11 table for the list of standard fields, and numeric IDs for standard enumerated values.

Some fields support multiple values. In these cases, the URL can include multiple values separated by a comma. For example, multiple incident types would be specified as:

```
incident_type_ids=18,19,22
```

Text in field values should be URL-encoded ("percent-encoded"), to allow inclusion of special and non-URL-safe characters.

To specify a value for a field without showing the field on the form layout, the value can be enclosed in a JSON block that includes "hidden":true. The URL-encoded JSON block below shows an example where the "name" field is specified but hidden, and so is not editable by the user when creating the incident.

```
#external/new_by_url?name={%22value%22:%22Incident%20X%22,%22hidden%22:true}
```

Time/date field values are specified in milliseconds of the Unix epoch. In the external application, this might be generated using for example the JavaScript 'Date.now()', Python 'time.time()', or the bash 'date + %s' (seconds) followed by three zeros.

Chapter 4. Add artifacts by URL

This allows you to open a form for adding new artifacts to an existing incident. The URL specifies a list of artifacts, each entry having an artifact type, value, and a description (optional).

```
#external/add_artifacts_by_url?artifacts[]=type,value,description
```

The resulting page shows a dropdown list of incidents, and the supplied artifacts.

The URL parameter ends with a numeric artifact type, the artifact itself, then a description if present. The following example shows the URL when specifying an IP address artifact type (1), an IP address of 192.168.1.2, and a description, "originating address".

```
https://server/#external/add_artifacts_by_url?artifacts[]=1,192.168.1.2,originating address
```

Artifact types include IP addresses, DNS names, URL's, and other types. Refer to the Chapter 7, "Artifact type IDs," on page 23 table for the complete list of artifact types.

If known, the URL can specify the incident ID. This selects the given incident in the dropdown list:

```
#external/add_artifacts_by_url?incident_id=1234&artifacts[]=type,value,description
```

Multiple artifacts can be specified in one URL. To do this, repeat the **artifacts** parameter as many times as required. For example, the following command produces the results shown in the Resilient Add Artifacts screenshot.

```
https://server/#external/add_artifacts_by_url?
artifacts[]=1,18.181.2.75&artifacts[]=2,rtfm.mit.edu&artifacts[]=9,sender@example.com
```

Chapter 5. Authentication

When opening a browser window with one of these URLs, a login prompt appears if the user is not already logged in to the Resilient platform. This login prompt requires the user's normal credentials (email address and password). If SAML authentication or two-factor authentication is configured, it also applies to the URL integration methods.

Chapter 6. Standard fields and values

name	Name	Text field
exposure_individual_name	Individual Name	Text field
addr	Address	Text field
zip	Zip	Text field
city	City	Text field
reporter	Reporting Individual	Text field
country	Country	1017 Afghanistan
		1261 Āland Islands
		1018 Albania
		1019 Algeria
		1020 American Samoa
		1021 Andorra
		1022 Angola
		1023 Anguilla
		1024 Antarctica
		1025 Antigua and Barbuda
		1026 Argentina
		1027 Armenia
		1028 Aruba
		1029 Ascension and Tristan Da Cunha Saint Helena
		1262 Asia
		1030 Australia
		1031 Austria
		1032 Azerbaijan
		1033 Bahamas
		1034 Bahrain
		1035 Bangladesh
		1036 Barbados
		1037 Belarus
		1038 Belgium
		1039 Belize
		1040 Benin
		1041 Bermuda

Field (API Name)	Description	Available Values
		1042 Bhutan
		1043 Bolivarian Republic of Venezuela
		1044 Bosnia and Herzegovina
		1045 Botswana
		1046 Bouvet Island
		1047 Brazil
		1048 British Indian Ocean Territory
		1049 British Virgin Islands
		1050 Brunei Darussalam
		1051 Bulgaria
		1052 Burkina Faso
		1053 Burundi
		1054 Cambodia
		1055 Cameroon
		1001 Canada
		1056 Cape Verde
		1057 Cayman Islands
		1058 Central African Republic
		1059 Chad
		1060 Chile
		1061 China
		1062 Christmas Island
		1063 Cocos (Keeling) Islands
		1064 Colombia
		1065 Comoros
		1066 Congo
		1067 Cook Islands
		1068 Costa Rica
		1074 Côte d'Ivoire
		1069 Croatia
		1070 Cuba
		1071 Curaçao
		1072 Cyprus
		1073 Czech Republic
		1075 Democratic People's Republic of Korea
		1076 Denmark
		1077 Djibouti

Field (API Name)	Description	Available Values
		1078 Dominica
		1079 Dominican Republic
		1080 Ecuador
		1081 Egypt
		1082 El Salvador
		1083 Equatorial Guinea
		1084 Eritrea
		1085 Estonia
		1086 Ethiopia
		1002 Europe
		1087 Falkland Islands (Malvinas)
		1088 Faroe Islands
		1089 Federated States of Micronesia
		1090 Fiji
		1091 Finland
		1092 France
		1093 French Guiana
		1094 French Polynesia
		1095 French Southern Territories
		1096 Gabon
		1097 Gambia
		1098 Georgia (Country)
		1099 Germany
		1100 Ghana
		1101 Gibraltar
		1102 Greece
		1103 Greenland
		1104 Grenada
		1105 Guadeloupe
		1106 Guam
		1107 Guatemala
		1108 Guernsey
		1109 Guinea
		1110 Guinea-Bissau
		1111 Guyana
		1112 Haiti
		1113 Heard Island and Mcdonald Islands

Field (API Name)	Description	Available Values
		1114 Holy See (Vatican City State)
		1115 Honduras
		1116 Hong Kong
		1117 Hungary
		1118 Iceland
		1119 India
		1120 Indonesia
		1121 Iraq
		1122 Ireland
		1123 Islamic Republic of Iran
		1124 Isle of Man
		1125 Israel
		1126 Italy
		1127 Jamaica
		1128 Japan
		1129 Jersey
		1130 Jordan
		1131 Kazakhstan
		1132 Kenya
		1133 Kiribati
		1134 Kuwait
		1135 Kyrgyzstan
		1136 Lao People's Democratic Republic
		1137 Latvia
		1138 Lebanon
		1139 Lesotho
		1140 Liberia
		1141 Libya
		1142 Liechtenstein
		1143 Lithuania
		1144 Luxembourg
		1145 Macao
		1146 Madagascar
		1147 Malawi
		1148 Malaysia
		1149 Maldives
		1150 Mali

Field (API Name)	Description	Available Values
		1151 Malta
		1152 Marshall Islands
		1153 Martinique
		1154 Mauritania
		1155 Mauritius
		1156 Mayotte
		1157 Mexico
		1158 Monaco
		1159 Mongolia
		1160 Montenegro
		1161 Montserrat
		1162 Morocco
		1163 Mozambique
		1164 Myanmar
		1165 Namibia
		1166 Nauru
		1167 Nepal
		1168 Netherlands
		1169 New Caledonia
		1170 New Zealand
		1171 Nicaragua
		1172 Niger
		1173 Nigeria
		1174 Niue
		1175 Norfolk Island
		1176 Northern Mariana Islands
		1177 Norway
		1178 Oman
		1016 Other
		1179 Pakistan
		1180 Palau
		1181 Panama
		1182 Papua New Guinea
		1183 Paraguay
		1184 Peru
		1185 Philippines
		1186 Pitcairn

Field (API Name)	Description	Available Values
		1187 Plurinational State of Bolivia
		1188 Poland
		1189 Portugal
		1190 Province of China Taiwan
		1191 Qatar
		1192 Republic of Korea
		1193 Republic of Moldova
		1197 Réunion
		1194 Romania
		1195 Russian Federation
		1196 Rwanda
		1198 Saint Barthélemy
		1199 Saint Kitts and Nevis
		1200 Saint Lucia
		1201 Saint Martin (French Part)
		1202 Saint Pierre and Miquelon
		1203 Saint Vincent and the Grenadines
		1204 Samoa
		1205 San Marino
		1206 Sao Tome and Principe
		1207 Saudi Arabia
		1208 Senegal
		1209 Serbia
		1210 Seychelles
		1211 Sierra Leone
		1212 Singapore
		1213 Sint Eustatius and Saba Bonaire
		1214 Sint Maarten (Dutch Part)
		1215 Slovakia
		1216 Slovenia
		1217 Solomon Islands
		1218 Somalia
		1219 South Africa
		1220 South Georgia and the South Sandwich Islands
		1221 South Sudan
		1222 Spain
		1223 Sri Lanka

Field (API Name)	Description	Available Values
		1224 State of Palestine
		1225 Sudan
		1226 Suriname
		1227 Svalbard and Jan Mayen
		1228 Swaziland
		1229 Sweden
		1230 Switzerland
		1231 Syrian Arab Republic
		1232 Tajikistan
		1233 Thailand
		1234 The Democratic Republic of the Congo
		1235 The Former Yugoslav Republic of Macedonia
		1236 Timor-Leste
		1237 Togo
		1238 Tokelau
		1239 Tonga
		1240 Trinidad and Tobago
		1241 Tunisia
		1242 Turkey
		1243 Turkmenistan
		1244 Turks and Caicos Islands
		1245 Tuvalu
		1246 Uganda
		1247 Ukraine
		1248 United Arab Emirates
		1249 United Kingdom
		1250 United Republic of Tanzania
		1000 United States
		1251 United States Minor Outlying Islands
		1252 Uruguay
		1253 Uzbekistan
		1254 Vanuatu
		1255 Viet Nam
		1256 Wallis and Futuna
		1257 Western Sahara

Field (API Name)	Description	Available Values
		1258 Yemen
		1259 Zambia
		1260 Zimbabwe
exposure_type_id	Exposure Type	1 Unknown
		2 External Source/Vendor
		3 Individual
data_source_ids	Source of Data	CUSTOM #
data_format	Data Format	0 Electronic
		1 Paper
		2 Oral
exposure_dept_id	Department	CUSTOM #
exposure_vendor_id	Vendor	CUSTOM #
state	State, or Province for Canada	1 Alabama
		2 Alaska
		4 Arizona
		5 Arkansas
		6 California
		7 Colorado
		8 Connecticut
		9 Delaware
		10 District of Columbia
		12 Florida
		13 Georgia
		15 Hawaii
		16 Idaho
		17 Illinois
		18 Indiana
		19 Iowa
		20 Kansas
		21 Kentucky
		22 Louisiana
		23 Maine
		25 Maryland
		26 Massachusetts
		27 Michigan

Field (API Name)	Description	Available Values
		28 Minnesota
		29 Mississippi
		30 Missouri
		31 Montana
		32 Nebraska
		33 Nevada
		34 New Hampshire
		35 New Jersey
		36 New Mexico
		37 New York
		38 North Carolina
		39 North Dakota
		41 Ohio
		42 Oklahoma
		30 Missouri
		31 Montana
		32 Nebraska
		33 Nevada
		34 New Hampshire
		35 New Jersey
		36 New Mexico
		37 New York
		38 North Carolina
		39 North Dakota
		41 Ohio
		42 Oklahoma
		43 Oregon
		45 Pennsylvania
		77 Puerto Rico
		47 Rhode Island
		48 South Carolina
		49 South Dakota
		50 Tennessee
		51 Texas
		52 Utah
		53 Vermont
		55 Virginia

Field (API Name)	Description	Available Values
		54 Virgin Islands
		56 Washington
		57 West Virginia
		58 Wisconsin
		59 Wyoming
		77 Puerto Rico
		1003 Alberta
		1004 New Brunswick
		1005 Newfoundland and Labrador
		1006 Ontario
		1007 Manitoba
		1008 Quebec
		1009 Nova Scotia
		1010 British Columbia
		1011 Prince Edward Island
		1012 Saskatchewan
		1013 Yukon
		1014 Northwest Territories
		1015 Nunavut
		1106 Guam
		1176 Northern Mariana Islands
start_date	Date Occurred	Time/date
discovered_date	Date Discovered	Time/date
harmstatus_id	Harm Foreseeable	1 No 2 Unknown 3 Yes
severity_code	Severity	52 High 51 Medium 50 Low
crimestatus_id	Criminal Activity	1 No 2 Yes 3 Yes – Freeze Tasks 4 Completed 5 Unknown

Field (API Name)	Description	Available Values
confirmed	Incident Disposition	0 No 1 Yes
negative_pr_likely	Negative PR	0 No 1 Yes null = Unknown
data_compromised	Data Compromised	0 No 1 Yes null = Unknown
data_encrypted	Data Encrypted	0 No 1 Yes null = Unknown
data_contained	Exposure Resolved	0 No 1 Yes null = Unknown
employee_involved	Employee Involved	0 No 1 Yes null = Unknown
plan_status	Status	A Active C Closed
phase_id	Phase	1 Engage 2 Detect/Analyze 3 Respond 4 Post-Incident
nist_attack_vectors	NIST Attack Vectors	0 Manual Selection 1 External/Removable Media 2 Attrition (Denial-of-Service and Brute-Force Attacks) 3 Web 4 E-mail 5 Impersonation 6 Improper Usage 7 Loss or Theft of Equipment 8 Other

Field (API Name)	Description	Available Values
incident_type_ids	Incident Type	1 Lost PDA/Smartphone
		2 Reserved
		3 Lost PDA/Laptop/Tablet
		4 Lost Documents/Files/Records
		5 Reserved
		6 Improper Disposal of Digital Assets
		7 Improper Disposal of Documents/Files
		8 Lost Storage Device/Media
		9 Reserved
		10 Reserved
		11 Stolen Documents/Files/Records
		12 Stolen PC/Laptop/Tablet
		13 Stolen PDA/Smartphone
		14 Stolen Storage Device/Media
		15 Vendor/3rd Party Error
		16 TBD/Unknown
		17 Communication Error(fax;email)
		18 Other
		19 Malware
		20 System Intrusion
		21 Denial of Service
		22 Phishing
		23 Not an Issue
description	Description	Multiline text or rich-text
hard_liability	Assessed Liability	Numeric field (no "$" sign allowed)
owner_id	Owner	Email address. Must be an invited member of the Resilient organization.
members	Members	Email address(es). Must be an invited member of the Resilient organization. Multi-select allowed, separated by comma.
jurisdiction_name	Jurisdiction	Text field
inc_training	Simulation	0 No
		1 Yes

Chapter 7. Artifact type IDs

Value	Artifact types
1	IP Address
2	DNS Name
3	URL
5	Email Subject
6	Email Body
8	Email Attachment Name
9	Email Sender
13	MD5 Hash
14	Malware SHA-1 Hash
19	Email Sender Name
20	Email Recipient
22	Malware Sample Fuzzy Hash
23	User Account
24	Registry Key
25	System Name
26	Process Name
27	Port
28	Service
29	String
30	Mutex
31	File Name
32	Password
34	HTTP Request Header
35	HTTP Response Header