IBM Security

IBM Resilient SOAR Platform
QRadar Integration Guide
V3.3

Date: August 2019

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

Version	Publication	Notes
3.3.0	August 2019	Supports the Resilient MSSP add-on feature.
3.2.2	August 2019	Mask authorization fields
3.2.1	June 2019	Adjustments for automatic escalation poller
3.2.0	May 2019	Bug-fix release version
3.1.2	January 2018	Documentation update only. Added memory requirement and a note about custom artifacts in templates.
3.1.2	December 2017	Supports Resilient platform V29.
3.1.1	September 2017	Documented the ability to map multiple IDs into multiple artifacts.
3.1	June 2017	Initial publication.

Table of Contents

Overview

This document describes how to integrate the Resilient Security Orchestration, Automation and Response Platform (SOAR) with IBM QRadar to simplify and streamline the process of escalating and managing incidents. Once an incident is escalated from QRadar, the Resilient platform generates a detailed, incident-specific response plan so team members can respond quickly.

This integration provides two ways to create incidents from QRadar: manually, and automatically. In the manual escalation workflow, you can send incidents to the Resilient platform from the QRadar Offenses screen. Additionally, you can add IP address artifacts to existing Resilient incidents.

For the automatic escalation workflow, you configure the conditions for sending offenses to the Resilient platform automatically using the escalation menu.

Changes to offenses are pushed automatically to existing incidents to keep them up to date in the form of field updates and new artifacts. Notes and closing events are synchronized bi-directionally between the systems.

The integration also utilizes the Resilient Action Module to enable several custom actions. You can perform Ariel searches on artifacts and add values to QRadar Reference sets from within the Resilient platform.

Resilient Organization and MSSP

A *Resilient organization* is a self-contained area within the Resilient platform for managing incidents.

In a standard configuration, there is a single Resilient organization for all incidents. Optionally, the platform can be configured with multiple organizations for separate business divisions, as well as one organization for development and test and another for production. However, each organization is managed separately.

The Resilient for Managed Security Service Providers (MSSP) add-on is an optional deployment feature that allows multiple Resilient child organizations, which are managed from a single configuration organization. Security analysts and other users can monitor incidents in multiple child organizations.

If you are using this integration with a Resilient platform configured with the MSSP add-on, you need to enable Multiple Organization Support and map the integration to the Resilient platform's configuration organization. Whenever you make changes, a Resilient administrator need to push those changes to the child organizations. The procedures in this guide provide the details.

Installation

Before you install the IBM Resilient QRadar Integration, make sure that your environment meets the following prerequisites:

- Your QRadar version is 7.2.8 build 20160920132350, or later.
- Your Resilient platform version is 31 or later. If supporting the Resilient for MSSPs multi-organization feature, Resilient platform V33 or later is required.
- A dedicated Resilient account to use as the API user. This can be any account that has the permission to create incidents, and view and modify administrator and customization settings. You need to know the account username and password.

  NOTE: Should you later change the dedicated Resilient account to another user, the new user must also have the permission to edit incidents, in addition to the permission to create incidents and view and modify administrator and customization settings. The edit permission is necessary so that the integration can continue to modify or synchronize the incidents escalated by the original user account.

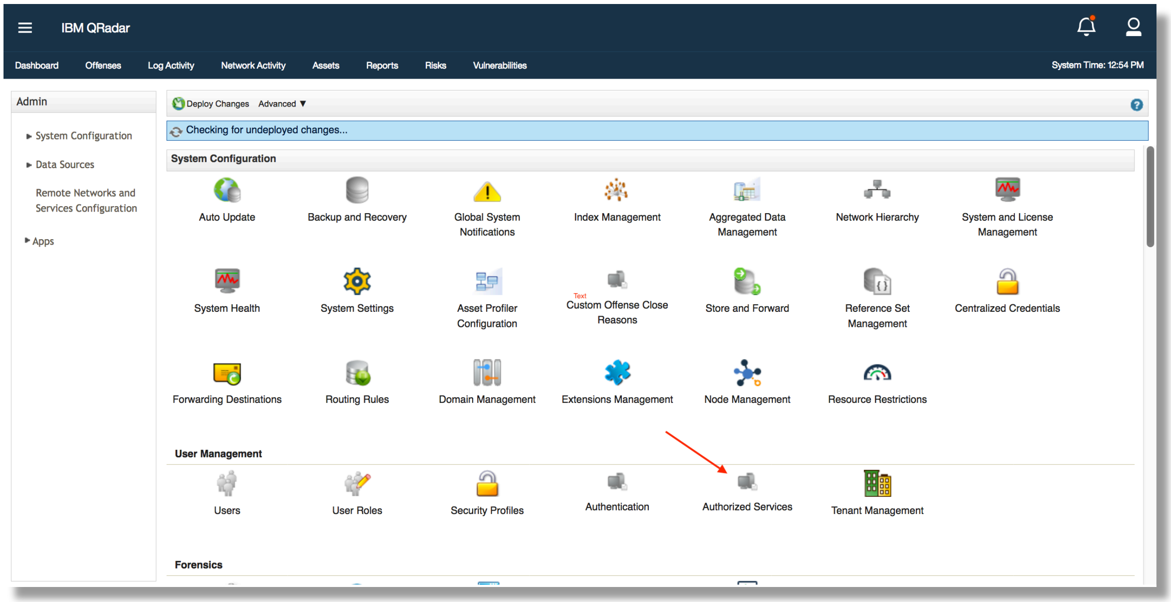
  If supporting the Resilient for MSSP feature, the Resilient account must have permission to access the configuration, global dashboard and all child organizations.
- The integration requires a minimum of 350MB memory.

Install the IBM Resilient QRadar Integration from the IBM Security App Exchange. Make sure to clear the cache after installation, as advised by IBM QRadar.

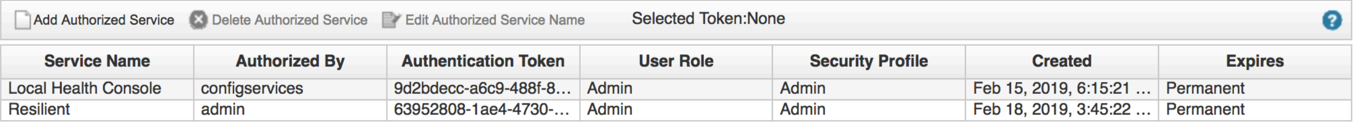
Configuration

Creating Service Token

The integration requires an Authorized Service Token in order to access the QRadar API. To create the token, go to the **Admin** tab and open the **Authorized Services** menu under **User Management**.



From there, click on **Add Authorized Service** and create a new service called **Resilient** with Admin Security Profile and User Role.



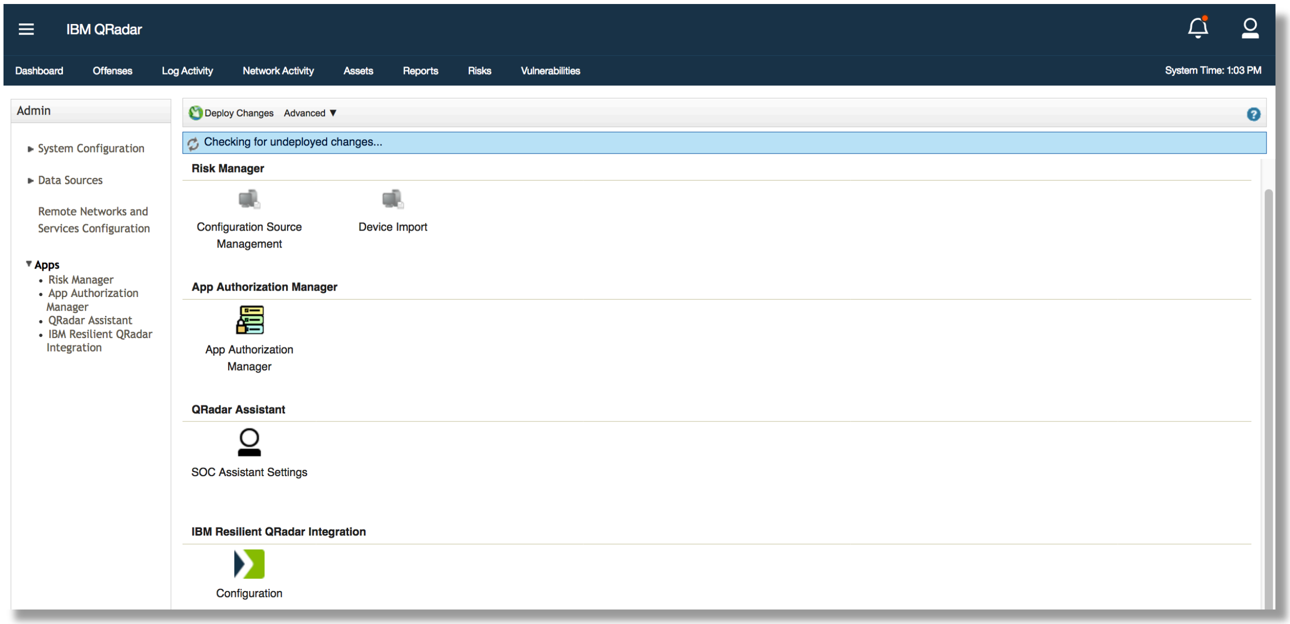
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
Local Health Console	configservices	9d2bdecc-a6c9-488f-8…	Admin	Admin	Feb 15, 2019, 6:15:21 …	Permanent
Resilient	admin	63952808-1ae4-4730-…	Admin	Admin	Feb 18, 2019, 3:45:22 …	Permanent

This token is copied in the Resilient configuration screen in the next step.

If supporting the Resilient for MSSP feature, this token must have permission to access all the domains used in the mapping.

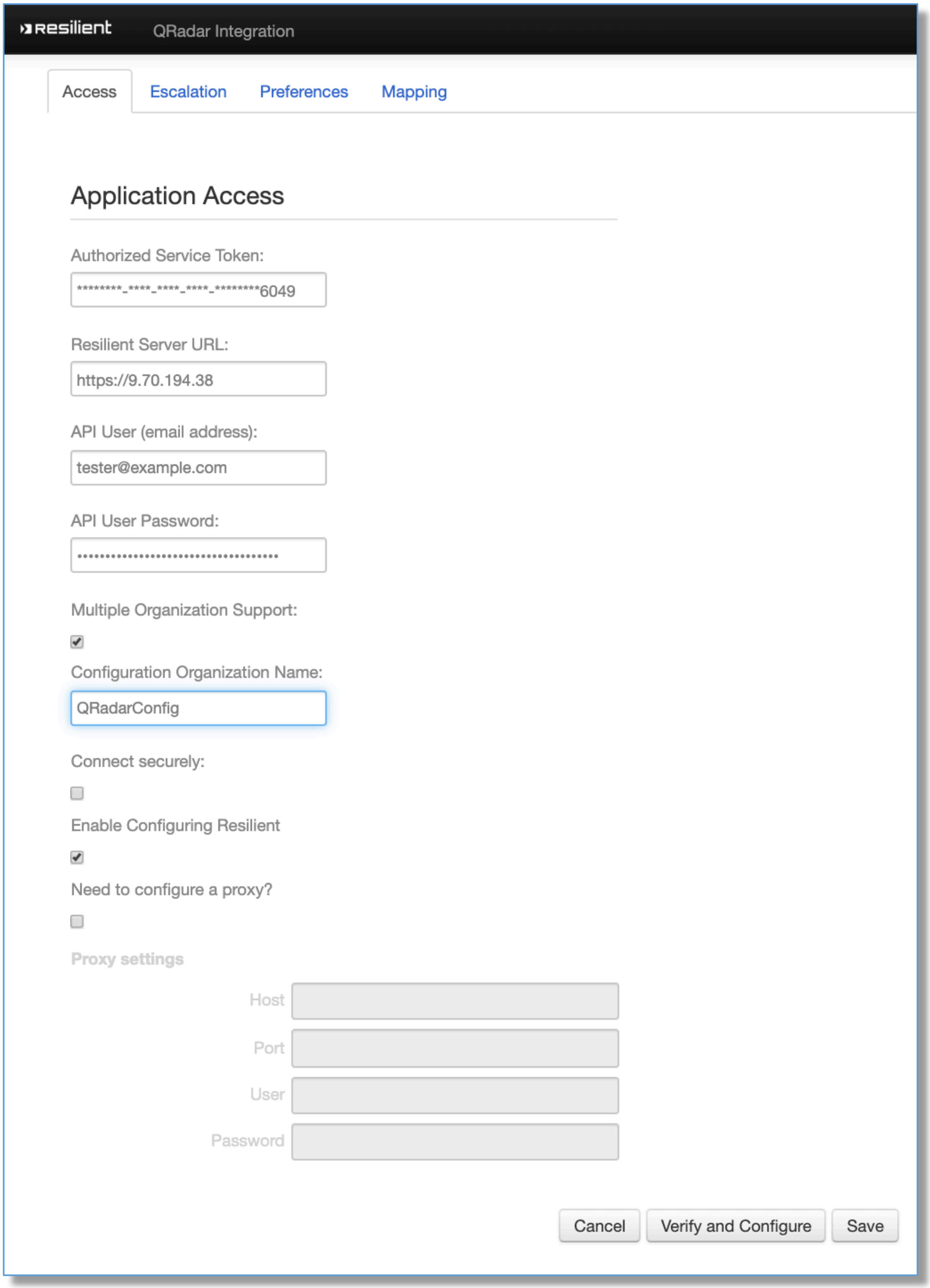
Configuring the Integration

The integration requires you to set configuration parameters. Go to the Admin tab then click Plug-Ins in the navigation bar on the left. Find and click the IBM Resilient icon, **Configuration**, at the bottom of the screen.



Checking for undeployed changes...

This opens a popup window for configuring the integration.



Application Access

Authorized Service Token: ********-****-****-****-********6049

Resilient Server URL: https://9.70.194.38

API User (email address): tester@example.com

API User Password: ••••••••••••••••••••••••••••••••••••

Multiple Organization Support: ☑

Configuration Organization Name: QRadarConfig

Connect securely: □

Enable Configuring Resilient ☑

Need to configure a proxy? □

Proxy settings

Host

Port

User

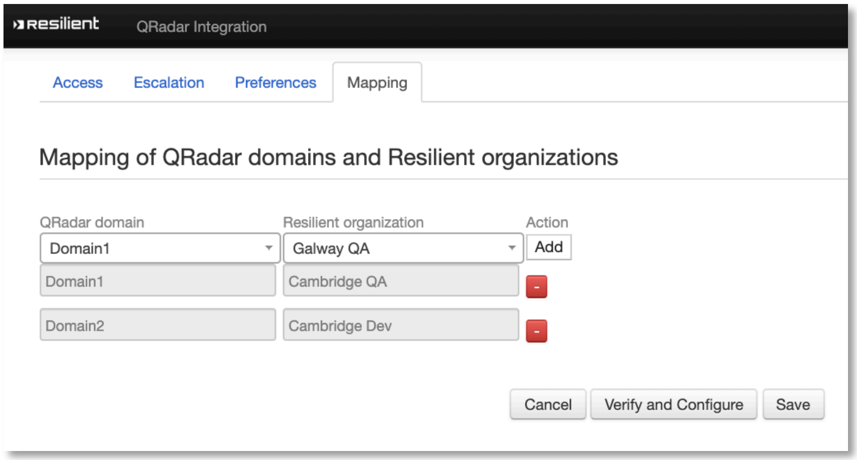
Password

The **Access** tab contains settings for configuring the connection between QRadar and the Resilient platform. The following describes each field:

- Authorized Service Token: An authorized service token used for API access.
- Resilient Server URL: URL of your Resilient platform server, the URL string has to start with “http://” or “https://”.
- API User (email address): Email address of the Resilient account used for this integration.
- API User Password: Password for the API user.
- Multiple Organization Support: Check if supporting mapping between QRadar domains and multiple Resilient organizations.
- Organization Name: Name of your Resilient organization. If connecting to a Resilient platform configured with the MSSP add-on, this must be the configuration organization.
- Connect Securely: If checked, SSL certificates are verified. For on-premises deployments that use self-signed SSL certificates or that have SSL certificate problems, you may need to deselect Connect Securely to allow the integration to make a connection successfully.
- Automatically Configure Resilient: If checked, the application creates in the Resilient platform all required fields, actions, and message destinations that are needed for the integration to work.
- Proxy settings: Check this box if your configuration requires a connection through a proxy server. Enter the host name as a URL address and port number. If the scheme is not provided for the proxy host, https:// is used by default. If your proxy connection requires authentication, enter the username and password. The proxy features use the basic authentication method to support authentication.

Click the **Verify and Configure** button to test that a connection can be made to the Resilient Server URL. This also tests whether a **QRadar ID** field is present in your Resilient platform, the authorized service token is valid, and if using a proxy, the proxy connection.

If Multiple Organization Support is enabled, this also fetches all the QRadar domains and Resilient child organizations. They are then shown in the Mapping tab where the user can select the mapping.

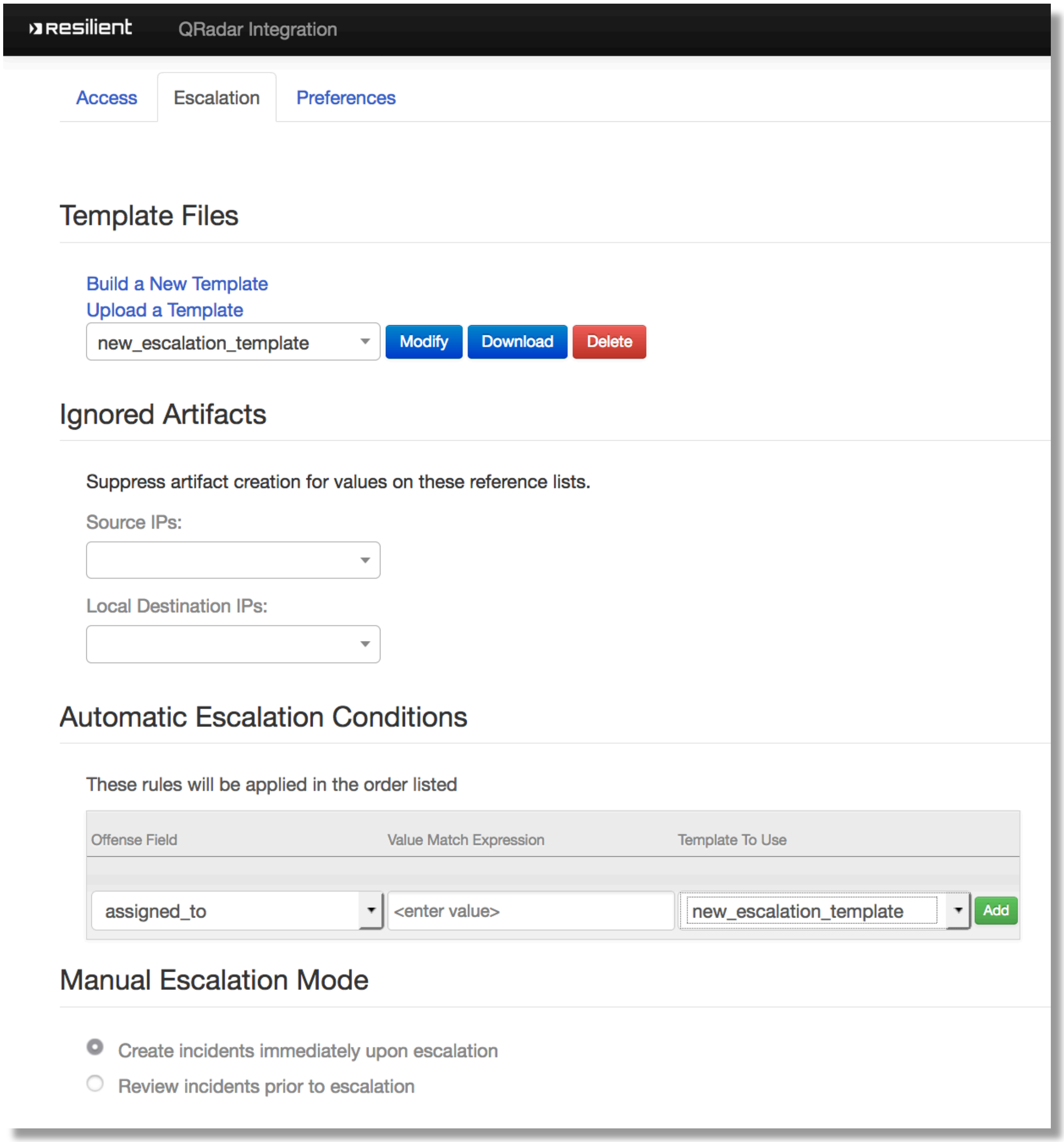


Mapping of QRadar domains and Resilient organizations

QRadar domain	Resilient organization	Action
Domain1	Galway QA	Add
Domain1	Cambridge QA	-
Domain2	Cambridge Dev	-

Before clicking **Save**, a Resilient administrator must log in to the Resilient platform and perform a push operation from the configuration organization. This pushes the configuration information to all the child organizations. Once this operation completes successfully, you can click the **Save** button from this window.

The **Escalation** tab contains settings for configuring how offenses are sent to the Resilient platform.



Template Files

Build a New Template
Upload a Template
new_escalation_template

Ignored Artifacts

Suppress artifact creation for values on these reference lists.

Source IPs:

Local Destination IPs:

Automatic Escalation Conditions

These rules will be applied in the order listed

Offense Field	Value Match Expression	Template To Use
assigned_to	<enter value>	new_escalation_template

Manual Escalation Mode

● Create incidents immediately upon escalation
○ Review incidents prior to escalation

The following describes each section:

- Template Files. A template maps fields from the QRadar offense to the Resilient incident. You can create custom templates as described in Custom Templates.
- Ignored Artifacts. You can define those artifacts that you do not wish to send to the Resilient platform as part of the incident. These might include source and local destination addresses on an offense, which may be known addresses of internal systems. You can reference this set of ignored artifacts in a template, as described in Mapping Incident Artifacts.
- Automatic Escalation Conditions. You can add rules under which offenses can be escalated. A background task continuously polls QRadar offenses to be considered as candidates for automatic escalation. See Automatic Escalation for details.

- Manual Escalation Mode. Allows you to determine whether or not the information is sent immediately to the Resilient platform when a user escalates an offense. With either manual escalation option listed below, the Resilient platform creates the incident, which can be edited in the Resilient platform.
    - The **Create incidents immediately upon escalation** option sends the offense directly to the Resilient platform. Up to 5 IP addresses of each type (source/destination) are added as artifacts during the incident creation process. If, in the following update cycle, there are still IP addresses left to translate, they are mapped as artifacts in the corresponding incident, with a limit of 15 of each type (source/destination). The limit of 20 total IP addresses is configurable in the app.config file. You should choose the **Create incidents immediately upon escalation** option if you have an environment where multiple users are likely to respond to the same offense and inadvertently create multiple incidents instead of one.
    - The **Review incidents prior to escalation** option requires that users review the details before escalating the offense to the Resilient platform. IP addresses are not translated as artifacts during the incident creation process. Instead, in the following update cycle, if there are IP addresses to translate, they are mapped as artifacts in the corresponding incident up to a limit of 20 of each type (source/destination). The limit of 20 total IP addresses is configurable in app.config file.

  NOTE: This setting applies to all escalations. If Multiple Organization Support is enabled, this setting applies to all QRadar domains.

The Preferences tab is described in Custom Actions.

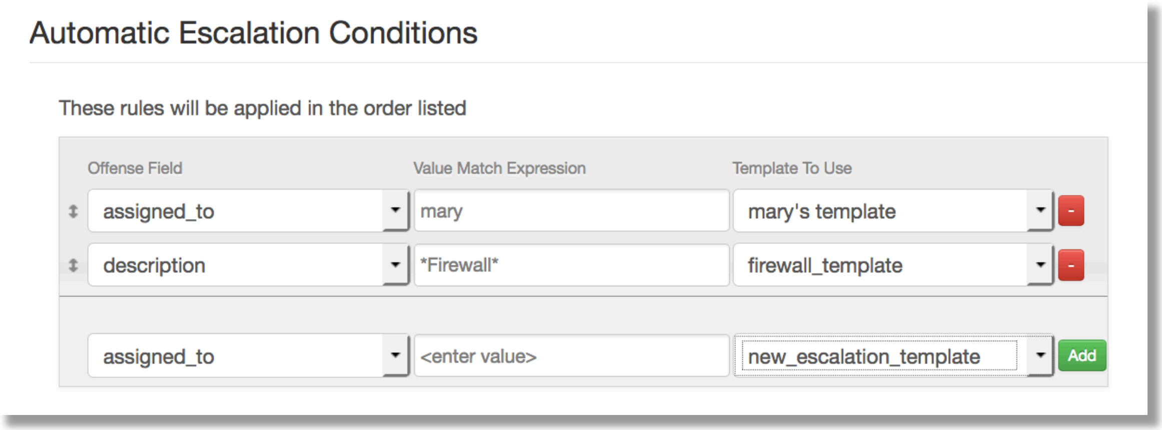
Automatic Escalation

This section describes how to send QRadar offenses to the Resilient platform automatically.

When an administrator adds escalation rules, a background task continuously finds QRadar offenses and considers them as candidates for automatic escalation. These are added on the **Escalation** tab in the configuration dialog.

The background task finds offenses where:

- The offense is Open.
- The offense matches an escalation rule. In the event that an offense matches more than one rule, the first rule matched is used.



Automatic Escalation Conditions

These rules will be applied in the order listed

Offense Field	Value Match Expression	Template To Use
assigned_to	mary	mary's template
description	*Firewall*	firewall_template
assigned_to	<enter value>	new_escalation_template

For each offense, it searches the Resilient platform for an open incident that was previously escalated using this offense ID. If none is found, it creates a new incident. In this way, new offenses are automatically and continuously mapped to new Resilient incidents.

➢ **IMPORTANT**: Automatic escalations run against new and existing open offenses in QRadar. Any open offenses that match your selection criteria should be closed prior to enabling automatic escalation if you do not want an incident created for them.

An administrator can configure the mapping between properties of the offense and fields for the new incident by providing a custom template file for each incident escalation rule. This can be used to automatically determine the incident type, the assigned groups, and any other incident fields. For details of this custom template file format, see Custom Templates.

If Multiple Organization Support is enabled, automatic escalation rules apply to all QRadar domains. Also, domain information of an offense is used to look for the mapped Resilient organization. If a mapped organization is not found, the corresponding offense is not escalated even if an automatic escalation condition is met.

Manual Escalation

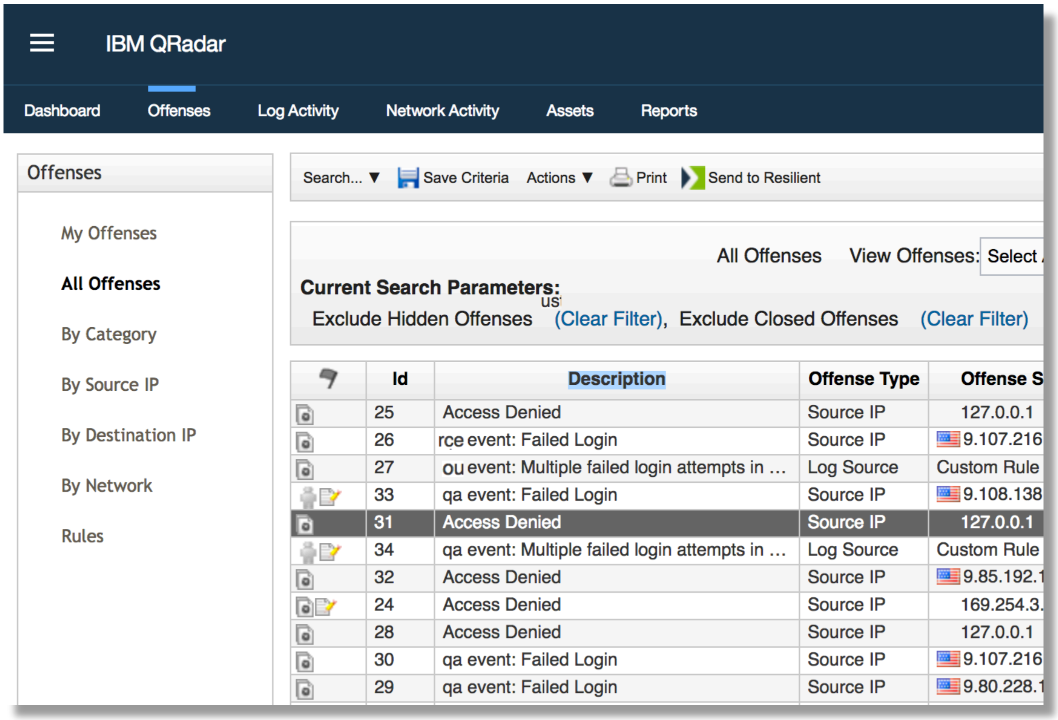
This section describes how a user can send QRadar offenses to the Resilient platform using the QRadar console user interface, as well as how to add IP addresses as artifacts to existing incidents.

To perform these procedures, you need to have the **IBM Resilient QRadar Integration** permission (as specified in User Role Management); otherwise, you do not see the **Send to Resilient** button.

Raising an Incident

To send an offense from QRadar to the Resilient platform, go to the QRadar console and perform the following.

1. Make sure that you enable popups in your browser.
2. In the QRadar console, click the **Offenses** tab.
3. From the list of offenses, select only one offense. For example:

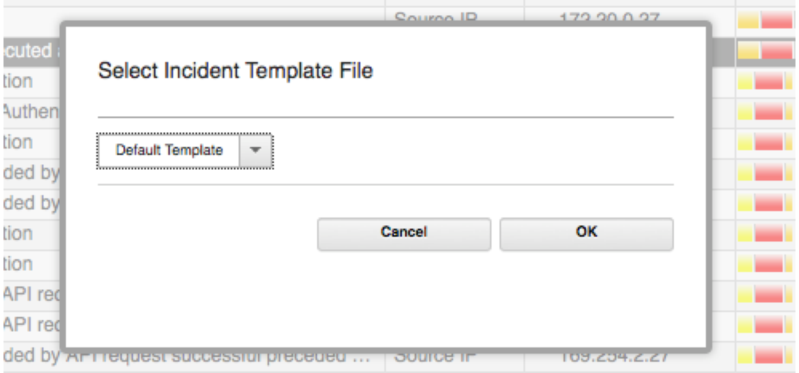


Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense S
	25	Access Denied	Source IP	127.0.0.1
	26	rce event: Failed Login	Source IP	9.107.216
	27	ou event: Multiple failed login attempts in ...	Log Source	Custom Rule
	33	qa event: Failed Login	Source IP	9.108.138
	31	Access Denied	Source IP	127.0.0.1
	34	qa event: Multiple failed login attempts in ...	Log Source	Custom Rule
	32	Access Denied	Source IP	9.85.192.1
	24	Access Denied	Source IP	169.254.3.
	28	Access Denied	Source IP	127.0.0.1
	30	qa event: Failed Login	Source IP	9.107.216
	29	qa event: Failed Login	Source IP	9.80.228.1

NOTE: If you are in the Offense Details screen, the **Send to Resilient** button is in the Details toolbar.

4. In the toolbar, click **Send to Resilient**. This opens a popup for you to select which mapping template you wish to use to generate the incident.

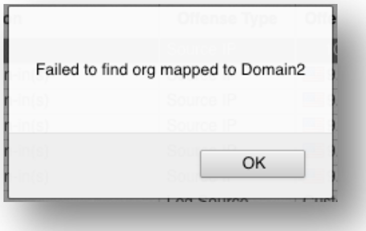


Select Incident Template File

5. Select a template from the dropdown and click OK.

While the incident is created immediately, any artifacts specified in the template are not generated until the next update cycle, which is when the app polls QRadar. Typically, this is approximately 2 minutes.

If Multiple Organization Support is enabled, the domain information of the selected offense is used to find the mapped Resilient organization. If an organization is found, the offense is escalated to that organization. If not found, an error message is shown; for example:



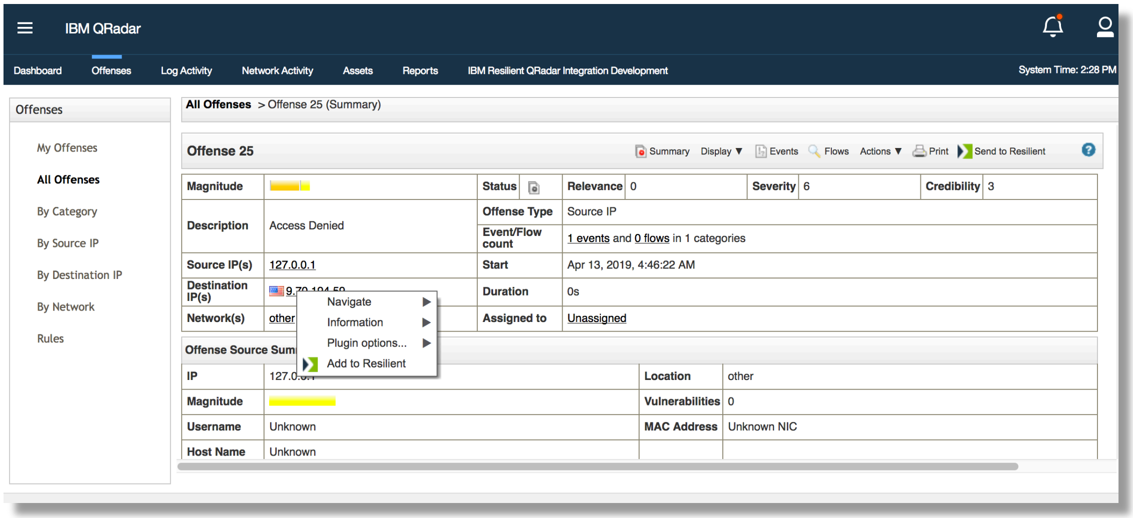
Failed to find org mapped to Domain2

NOTE: Should you log into the Resilient platform after creating an incident and see the following message, **Error: Unable to find object with ID *xxxxx***, verify that you have logged into the same Resilient organization as the one configured in the Access.

Adding Artifacts to an Incident

Perform the following to add an artifact to an incident:

1. Make sure that you enable popups in your browser.
2. In the QRadar console, click the **Offenses** tab.
3. From the list of offenses, click on an offense to open its details.
4. Right click on any IP address.
5. In the popup menu, click **Add to Resilient**.



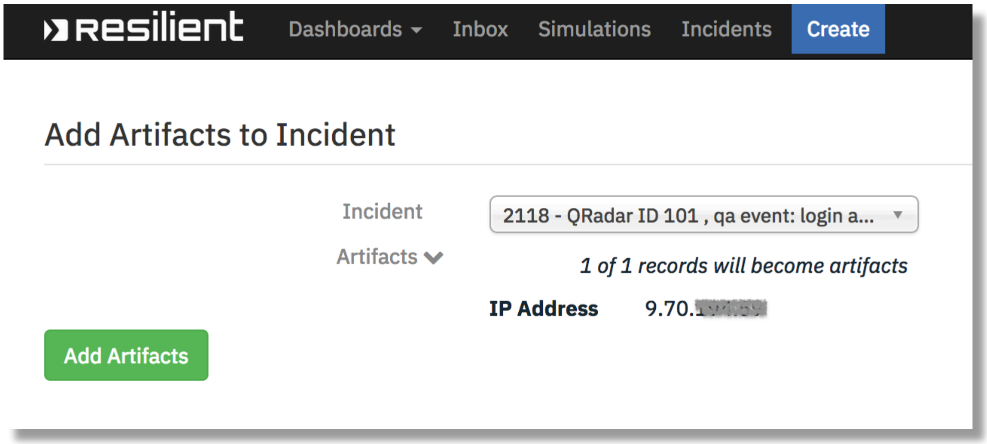
Offense 25

Magnitude		Status		Relevance	0	Severity	6	Credibility	3
Description	Access Denied	Offense Type	Source IP						
		Event/Flow count	1 events and 0 flows in 1 categories						
Source IP(s)	127.0.0.1	Start	Apr 13, 2019, 4:46:22 AM						
Destination IP(s)	9.70.104.59	Duration	0s						
Network(s)	other	Assigned to	Unassigned						

Offense Source Sum

IP	127.0.0.1	Location	other
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		

6. In the Add Artifact screen, select the incident to add this IP address.
7. Click Add Artifacts.



Add Artifacts to Incident

Incident: 2118 - QRadar ID 101 , qa event: login a... ▼

Artifacts ❯

1 of 1 records will become artifacts

IP Address 9.70.[redacted]

This feature also works on IP addresses in the **Log Activity** tab.

Custom Templates

Template Creator Screen

The template creator is accessible via the escalation tab on the configuration screen. It allows mapping of fields from the QRadar offense to the Resilient incident. The incident fields displayed are pulled from the Resilient platform and updated each time this screen is accessed, so any changes to incident fields, including custom fields, are reflected here.

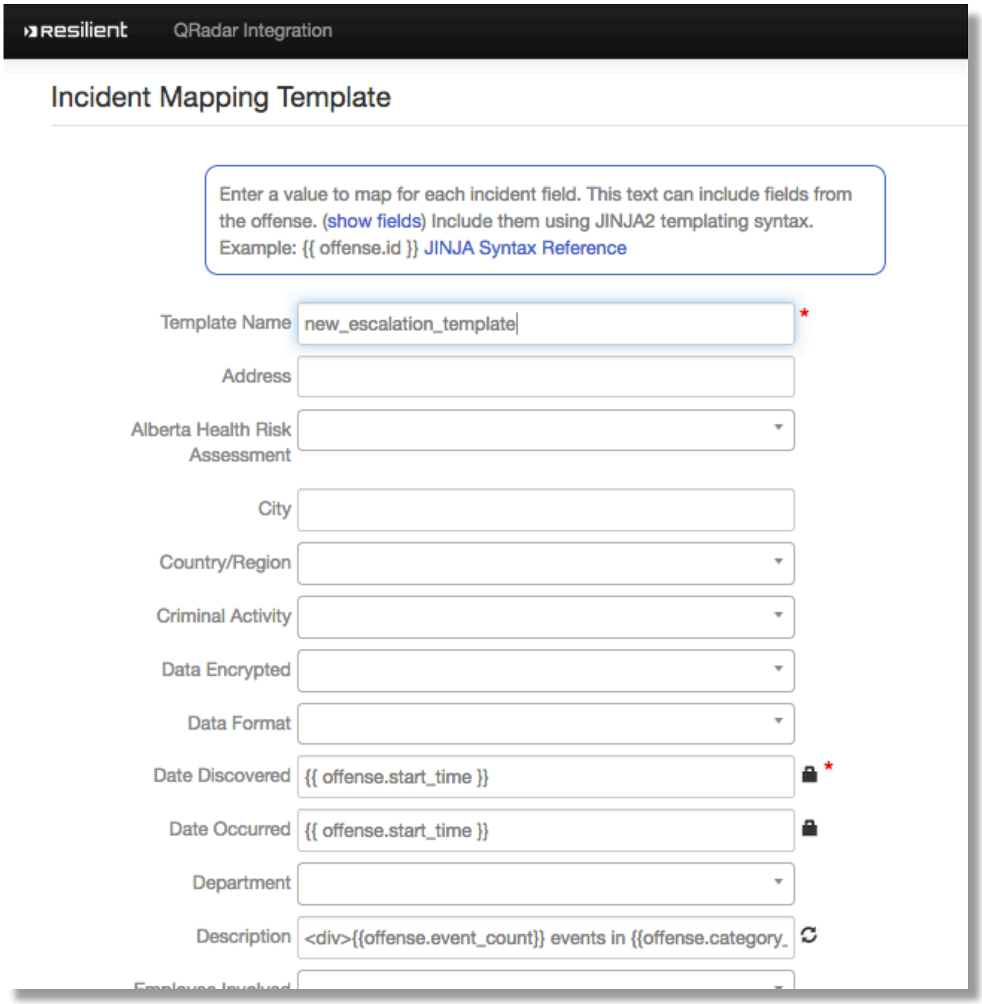
When you click Save, a template file is generated based on the mapping specified.

Mapping Incident Fields

To view the complete list of offense fields available for mapping, click **show fields** at the top of the screen. It includes all the regular offense fields, plus ones that store ID fields translated to text values. The list of valid values for selection fields is available from their drop-down lists.

The syntax to map an offense field to an incident field is `{{ offense.fieldname }}`.

A red asterisk next to a field indicates that it is required, so a mapping must be specified.



Incident Mapping Template

Enter a value to map for each incident field. This text can include fields from the offense. (show fields) Include them using JINJA2 templating syntax. Example: {{ offense.id }} JINJA Syntax Reference

Template Name	new_escalation_template *
Address	
Alberta Health Risk Assessment	▾
City	
Country/Region	▾
Criminal Activity	▾
Data Encrypted	▾
Data Format	▾
Date Discovered	{{ offense.start_time }} 🔒 *
Date Occurred	{{ offense.start_time }} 🔒
Department	▾
Description	<div>{{offense.event_count}} events in {{offense.category_ ⟳
Employee Involved	▾

When a value is added to a field, a refresh icon ↻ appears next to it. This indicates that the field is updated anytime the offense is updated. This has an effect on fields that contain an actual mapping from an offense field rather than just a static value. If updates for a particular field are not desired, you can click the icon to change it to a lock. This indicates that the incident field is locked upon creation and does not receive updates from QRadar when the offense changes. The field can still be modified from the Resilient client.

There are several JINJA "filters" available for use when mapping your fields. They are essentially functions that format or modify a value before copying it into the incident. They are called similar to: `{{ offense.<offense_field>|<filter_name> }}`

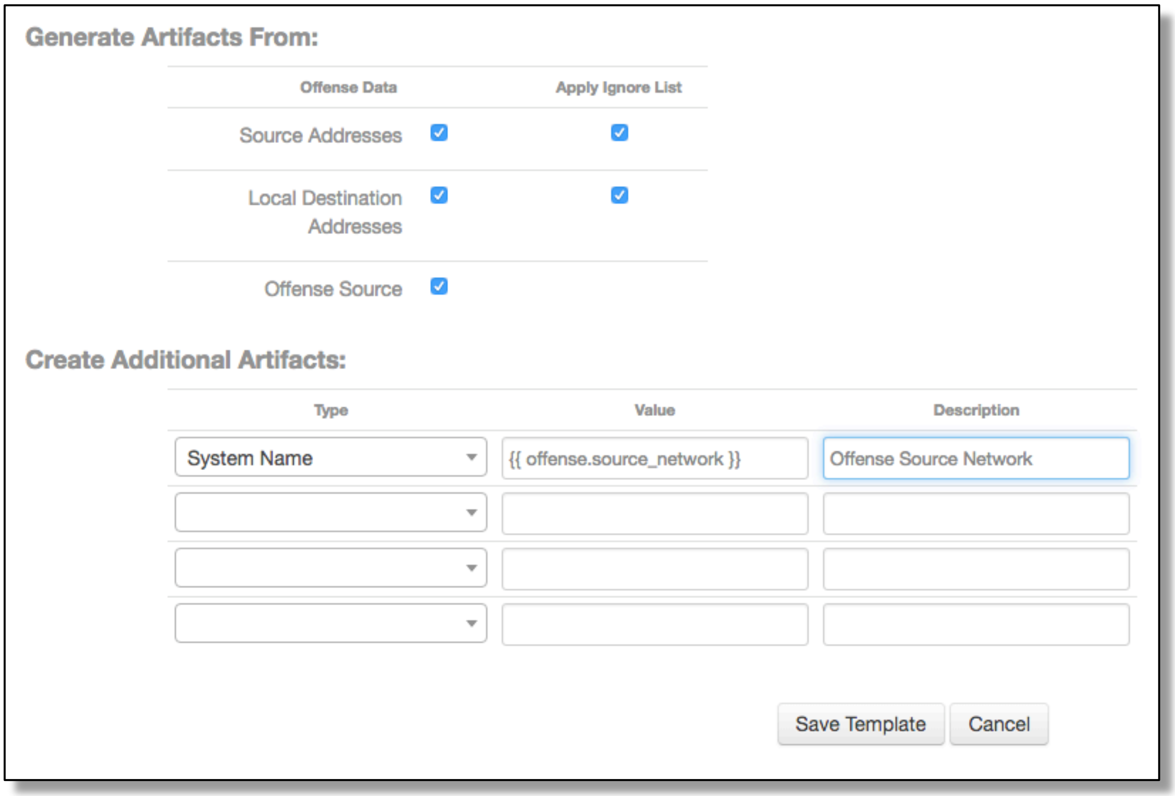
NOTE: The template language is based on JINJA2. See the JINJA2 documentation for details.

Filter Name	***Description***	***Sample Usage***
ago	Converts epoch milliseconds timestamp value to a string representation of the time in milliseconds that has elapsed since then.	`{{ offense.start_time|ago }}`
csv	Converts a list of values to a comma separated string.	`{{ offense.categories|csv }}`
res_email	Converts the user's display name to an email address, if the email address exists in the Resilient org. If not, it returns the default Resilient email address specified in app.config.	`{{ offense.assigned_to|res_email }}`
html	HTML-escaped version of value.	
Iso8601	Converts epoch milliseconds timestamp value to an ISO8601 datetime value.	`{{ offense.start_time|iso8601 }}`
js	Same as json filter but strips the surrounding quotes from the result.	`{{ offense.description|js }}`
json	JSON-friendly version of the value.	`{{ offense.description|js }}`
local_dest_ip_whitelist	Removes all entries that are on the configured Local Destination IP ignore list from a list of values.	`{{ offense.local_destination_addresses|local_dest_ip_whitelist }}`
severity	Maps a numeric QRadar severity to a Resilient severity: 8-10 = High 4-7 = Medium 1-3 = Low	`{{ offense.severity|severity }}`
src_ip_whitelist	Removes all entries that are on the configured Source IP ignore list from a list of values.	`{{ offense.source_addresses|src_ip_whitelist }}`
uniq	Removes duplicate entries from a list of values.	

Mapping Incident Artifacts

In addition to incident fields, mapping templates also allow you to specify which artifacts you want created from an offense. Artifacts are automatically created from the list of offense source addresses, offense local destination addresses, and offense source if those boxes are checked.

If you wish to create artifacts from incident fields other than those, you can do so in the **Create Additional Artifacts** section.



Generate Artifacts From:

Offense Data		Apply Ignore List
Source Addresses	☑	☑
Local Destination Addresses	☑	☑
Offense Source	☑	

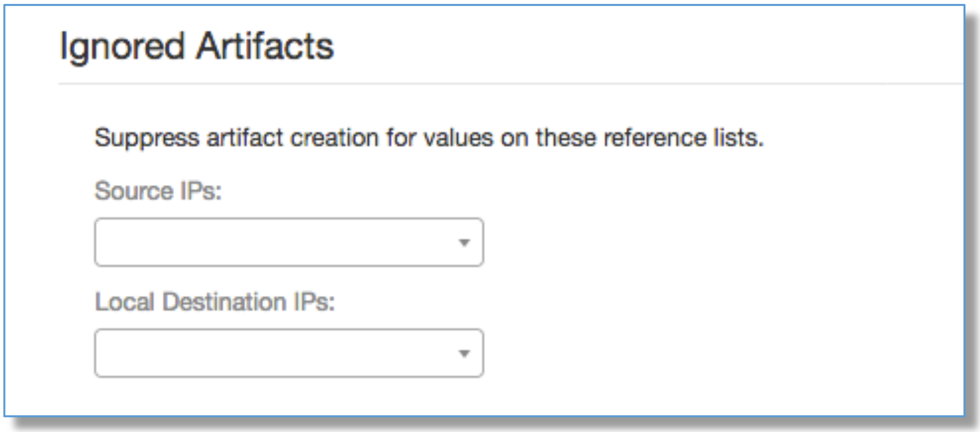
Create Additional Artifacts:

Type	Value	Description
System Name	{{ offense.source_network }}	Offense Source Network

There are likely to be source and local destination addresses on an offense that you do not want to be used to create artifacts. Often these are known addresses of internal systems. If those known addresses are stored in a QRadar Reference Set, then the integration can use that reference set as an “ignore list” for artifact creation. If **Apply Ignore List** is checked on the template, then any addresses in the offense that are in the ignore list are skipped when generating artifacts.

NOTE: The templates do not support custom artifact types that support file attachments.

You specify the reference sets to ignore on the **Escalation** tab in the configuration screen.



Ignored Artifacts

Suppress artifact creation for values on these reference lists.

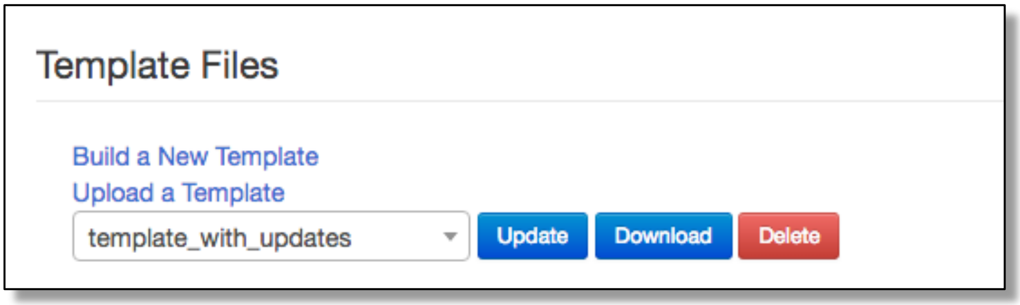
Source IPs:

Local Destination IPs:

As new source and local destination IP addresses are added to the offense, new artifacts are added to the Incident as well. In the event that an offense has a large number of IP addresses, it converts a maximum of 20 to artifacts during each polling session.

Managing Templates

You manage template files on the **Escalation** tab in the configuration screen. Clicking **Build a New Template** or **Update** for an existing template takes you to the mapping screen. Clicking **Download** allows you to retrieve an existing template for manual updates, and clicking **Delete** permanently removes a template from the app.



Template Files

Build a New Template

Upload a Template

- **IMPORTANT**: Do not use the Update feature for any templates that you have manually updated (for example, you have downloaded the template file, edited it then uploaded it). Otherwise, your changes are overwritten by the updater.

Manually Creating or Updating Templates

In most cases, the templates generated by the template creator should be sufficient. However, there are some use cases where a more advanced template is required. You can get your template close to how you want it via the mapping screen, then download it and modify it

The template language is based on JINJA2. See the JINJA2 documentation for details.

The template is rendered to a JSON document that is either posted to the Resilient platform to create a new incident or converted to a URL with key/value parameters in the Resilient Web URL format. Refer to the *Web URL Integration Guide* for complete details of this format.

The following is an example of a template. In this use case, manual updates to the template are required to support mapping the Incident Type to different values based upon the offense description.

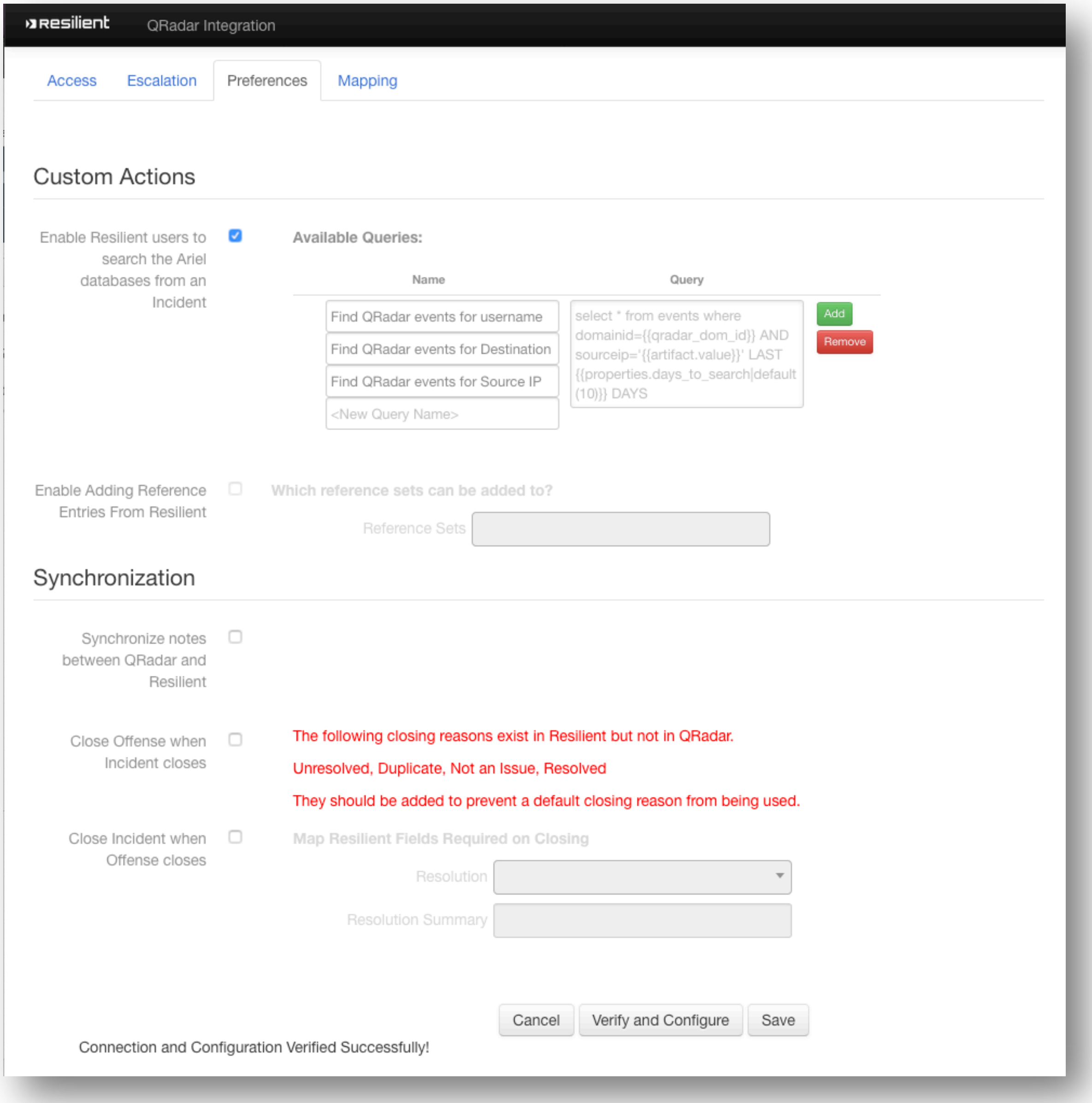
```
{
     "name": "QRadar {{offense.offense_type_name}} - {{offense.offense_source}}, ID:
{{offense.id}}",

          {# Set incident id from description #}
    {% if "malware" in offense.description %}
    "incident_type_ids": "Malware",
    {% else %}
    "incident_type_ids": "Other",
    {% endif %}
    "confirmed": 0,
    "description" : "{{offense.event_count}} events in {{offense.category_count}} categories:
{{offense.description}}",
    "discovered_date": {{offense.start_time}},
    "start_date": {{offense.start_time}},
    "severity_code" : {{offense.severity | severity}}
}
"type": "IP Address",
            "value": "{{e.sourceip|js}}",
            "description": "Source {{e.sourceip|js}}"
        } {% if not loop.last %},{% endif %}
    {% endfor %} ]
}

FROZEN="incident_type_ids","name","start_date","confirmed","discovered_date"
```

Custom Actions

The Resilient integration runs a background process that connects to the Resilient Action Module, enabling several custom actions within the Resilient platform. This can be found under the Preferences tab in the Configuration Screen.



Custom Actions

Enable Resilient users to search the Ariel databases from an Incident ☑

Available Queries:

Name	Query
Find QRadar events for username Find QRadar events for Destination Find QRadar events for Source IP <New Query Name>	select * from events where domainid={{qradar_dom_id}} AND sourceip='{{artifact.value}}' LAST {{properties.days_to_search|default(10)}} DAYS

Enable Adding Reference Entries From Resilient □

Which reference sets can be added to?

Reference Sets

Synchronization

Synchronize notes between QRadar and Resilient □

Close Offense when Incident closes □

The following closing reasons exist in Resilient but not in QRadar.

Unresolved, Duplicate, Not an Issue, Resolved

They should be added to prevent a default closing reason from being used.

Close Incident when Offense closes □

Map Resilient Fields Required on Closing

Resolution

Resolution Summary

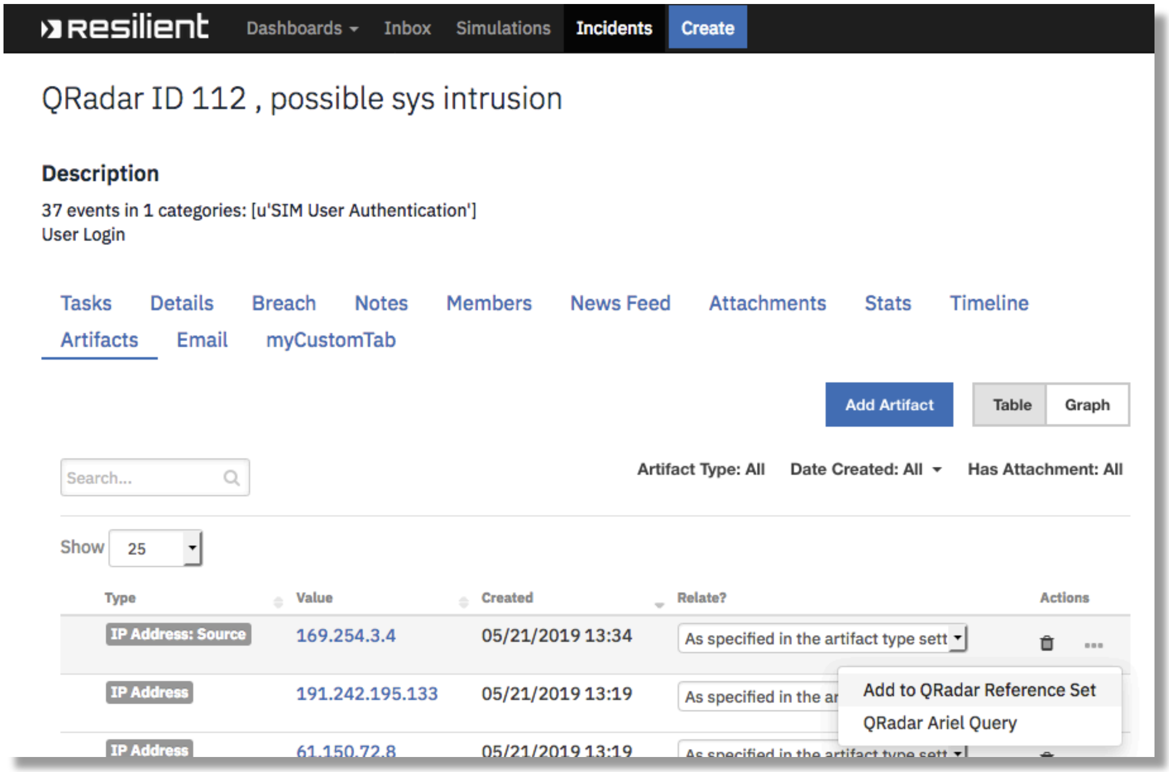
Connection and Configuration Verified Successfully!

If Multiple Organization Support is enabled, make sure that a new Ariel search query contains the following token in all proper places: `domainid={{qradar_dom_id}}`. This is to limit the ariel search with the proper domain. Also **Enable Adding Reference Entries From Resilient** is disabled, since the QRadar API does not support adding reference entries to a specific domain.

Ariel Search

This is a manual custom action that enables Resilient users to search the QRadar Ariel database for any artifact value from within the Resilient platform. This action is enabled in the Custom Actions section of the Preferences tab in the Configuration Screen. The search results are then attached to the incident in a CSV file.

In an incident's Artifact tab in the Resilient platform, click on the action menu next to the artifact you wish to query and select "QRadar Ariel Query".



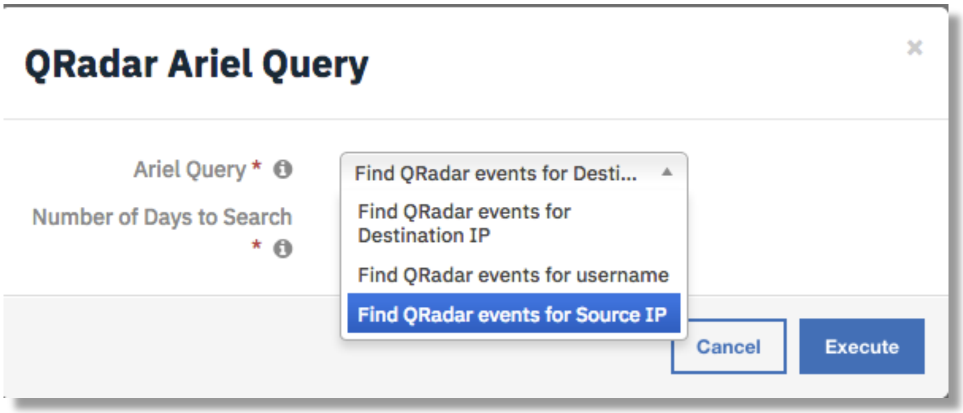
QRadar ID 112 , possible sys intrusion

Description

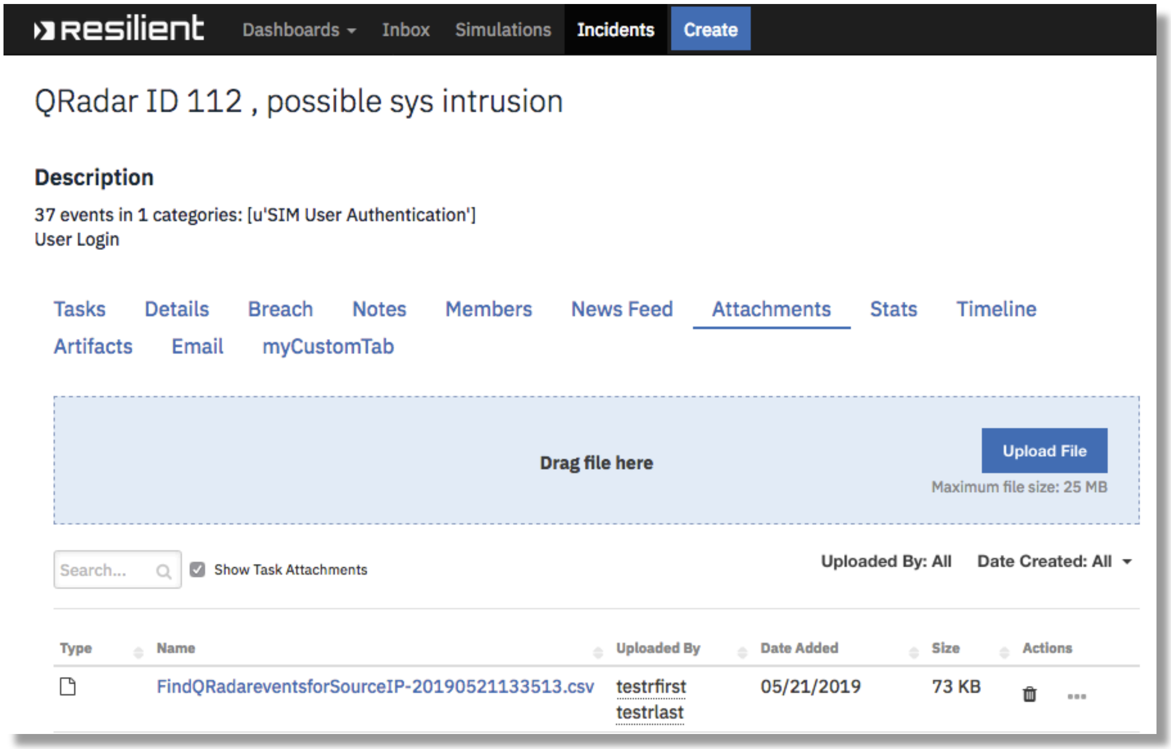
37 events in 1 categories: [u'SIM User Authentication']
User Login

Type	Value	Created	Relate?	Actions
IP Address: Source	169.254.3.4	05/21/2019 13:34	As specified in the artifact type sett	
IP Address	191.242.195.133	05/21/2019 13:19	As specified in the ar	
IP Address	61.150.72.8	05/21/2019 13:19	As specified in the artifact type sett	

Select the type of Ariel Query you wish to run from the popup modal.


QRadar Ariel Query
Ariel Query *
Number of Days to Search *
Find QRadar events for Desti...
Find QRadar events for Destination IP
Find QRadar events for username
Find QRadar events for Source IP
Cancel
Execute

The search results can be found in the .csv file under the Attachments tab.



QRadar ID 112 , possible sys intrusion

Description

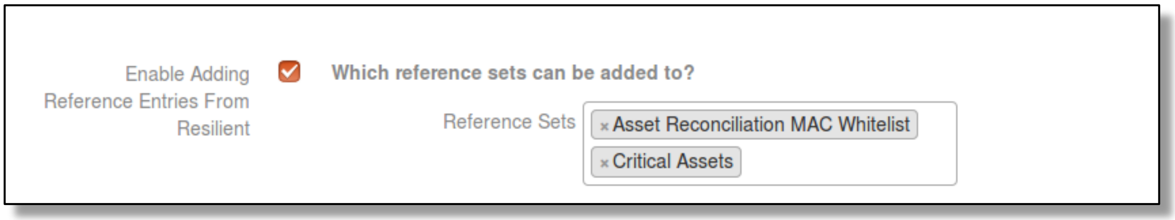
37 events in 1 categories: [u'SIM User Authentication']
User Login

Type	Name	Uploaded By	Date Added	Size	Actions
🗋	FindQRadareventsforSourceIP-20190521133513.csv	testrfirst testrlast	05/21/2019	73 KB	🗑 •••

Add to Reference Set

This manual action enables a user to add an artifact value to a QRadar Reference set. When enabled, the list of selected reference sets from QRadar automatically populates into the Rule drop-down list in the Resilient platform. This feature can be used in conjunction with the "ignored artifacts" reference sets. If an artifact is created automatically from a template but it is determined that it is not valuable data (such as an IP Address of internal system), you can use the Add to Reference Set action to add the value to the ignore list. That prevents future incidents from having the unwanted artifact added.

This is disabled if Multiple Organization Support is enabled.

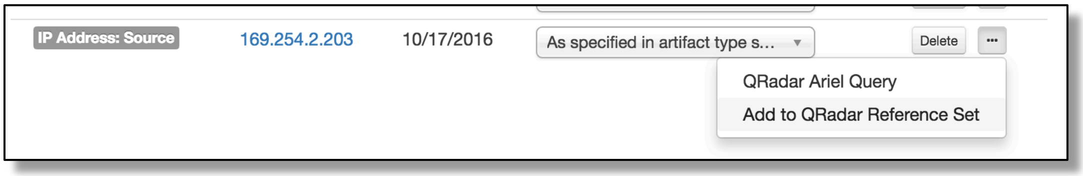


Enable Adding Reference Entries From Resilient ☑

Which reference sets can be added to?

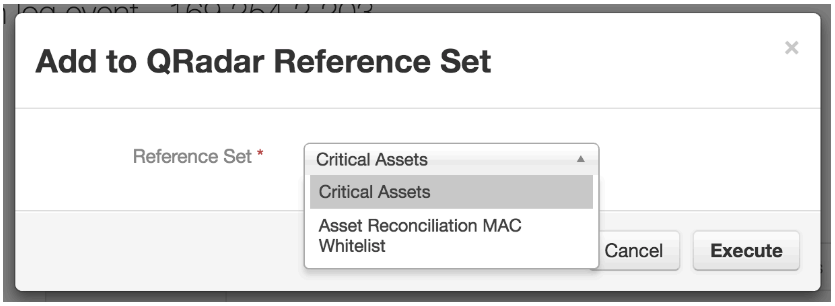
Reference Sets: × Asset Reconciliation MAC Whitelist, × Critical Assets

App Configuration Option



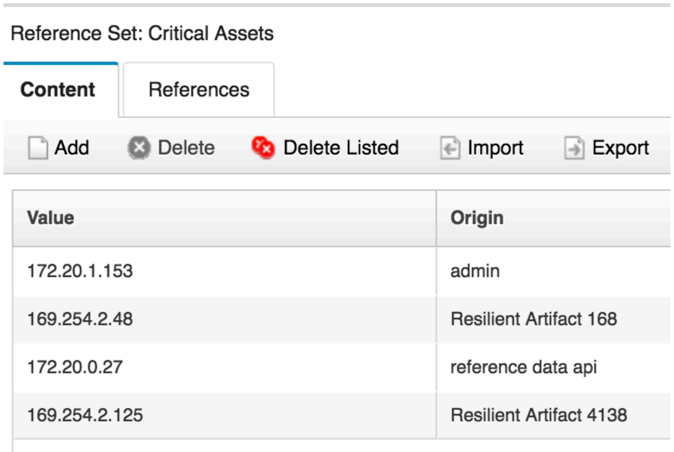
IP Address: Source	169.254.2.203	10/17/2016	As specified in artifact type s... ▾	Delete	···

Resilient Artifact Action Menu



Add to QRadar Reference Set

Reference Set *: Critical Assets



Reference Set: Critical Assets

Value	Origin
172.20.1.153	admin
169.254.2.48	Resilient Artifact 168
172.20.0.27	reference data api
169.254.2.125	Resilient Artifact 4138

Reference Set

Updating Incidents

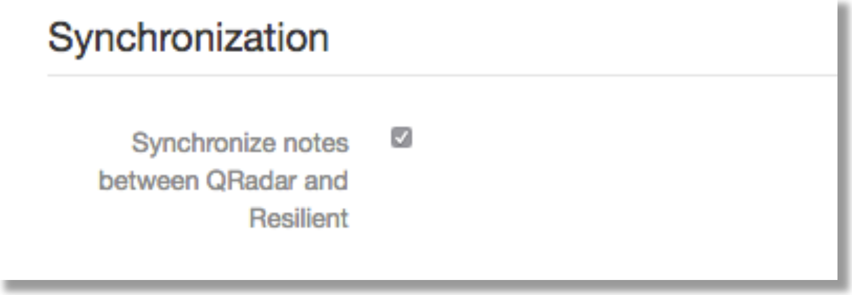
An offense in QRadar continues to evolve after it is created. New events and addresses become associated with it. These updates are automatically pushed to the corresponding incident so long as both the incident and the offense remain open. Because the same template that was used to create an incident is used to update it, any changes to that template after an incident is created affects how it is updated. Similarly, deleting a template results in no further updates to the incidents that were created with it. Any fields that contain a mapping using the {{ }} jinja syntax is updated any time the offense changes, unless the template has marked the field as locked. See Mapping Incident Fields for more details.

Offense updates also trigger new artifacts to be created in the Resilient platform if the template was configured for artifact generation.

Synchronized Notes

The integration polls QRadar for new offense notes to copy over to the Resilient platform. An automatic custom action in the Resilient platform alerts the integration any time a new note is added to an Incident, which is then copied to the corresponding offense. This bi-directional sync is enabled with the **Synchronize Notes** option in the Synchronization section of the Preferences tab in the Configuration screen.

NOTE: This feature applies only to notes added to incidents, not the notes added to tasks.



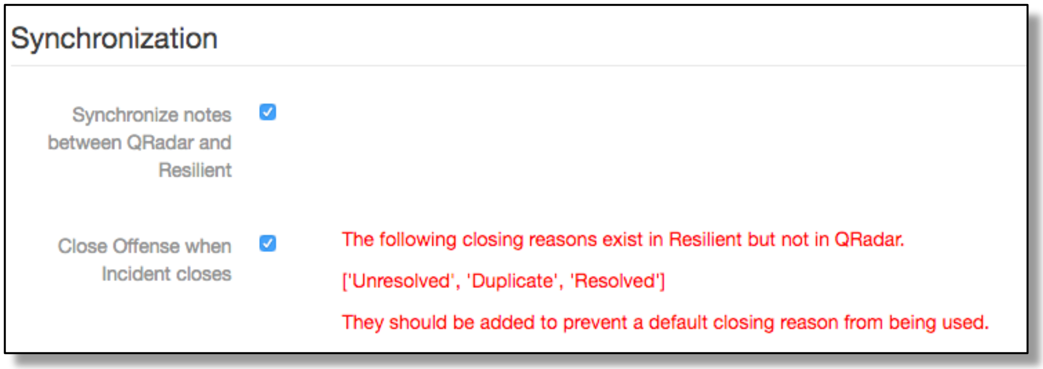
Synchronization

Synchronize notes between QRadar and Resilient ☑

Automatically Closing Offenses

An automatic action notifies the integration whenever an incident is closed. If desired, this can trigger the corresponding offense to close as well.

Under Synchronization of the Preferences tab in the Configuration Screen, check **Close Offense when Incident closes**. When the offense is closed, a closing reason is provided. If the Resolution on the Incident matches a closing Reason in QRadar, then that reason is used. If the Incident Resolution does not exist as a closing Reason in QRadar, then a default of "Policy Violation" is used. For this reason, it is advised that you configure the Custom Offense Closing Reasons in QRadar and Resolution Values in the Resilient platform to match. As shown in the following image, the integration warns you of any Resolution values in the Resilient platform that do not have a corresponding closing Reason in QRadar.



Synchronization

Synchronize notes between QRadar and Resilient ☑

Close Offense when Incident closes ☑

The following closing reasons exist in Resilient but not in QRadar.

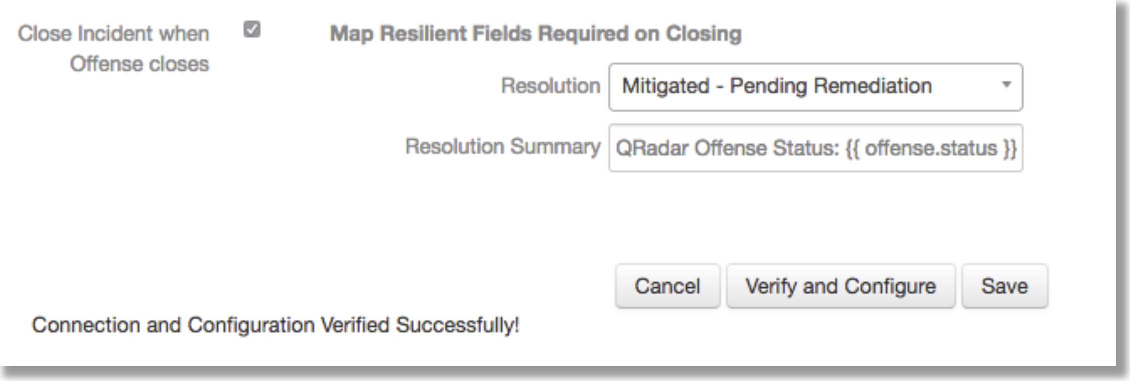
['Unresolved', 'Duplicate', 'Resolved']

They should be added to prevent a default closing reason from being used.

When the offense is closed, a note is added to indicate the Resilient user who closed the Incident, the Resolution ID, and the Resolution Summary.

Automatically Closing Incidents

You can set the integration to close an incident automatically in the Resilient platform whenever it detects that the corresponding Offense has been closed. This happens as part of the background update task, which runs every 2 minutes. The Resilient platform has a set of fields that are required to be populated in order for an incident to be closed. That set of required closing fields is configurable.



Close Incident when Offense closes ☑

Map Resilient Fields Required on Closing

Resolution: Mitigated - Pending Remediation

Resolution Summary: QRadar Offense Status: {{ offense.status }}

Connection and Configuration Verified Successfully!

Under the Synchronization section of the Preferences tab in the Configuration Screen, check **Close Incident when Offense closes**. This prompts you to map a value for each of the Incident fields that have been set as "required on close". The syntax is the same as described in Mapping Incident Fields section.

Database Backup and Rollback

The QRadar plugin contains a database, which needs to be kept in sync with the Resilient platform database. Whenever you perform a backup or rollback of the Resilient database, you need to do the same for the QRadar local database. The steps to do both are defined below.

QRadar plugin database backup

Before backing up the database, you must stop the QRadar plugin. This is best done using the API, as described in the QRadar API documentation. The following example shows a curl command using the version 10.0 API:

```
curl -s -X POST -u <USER> -H 'Version: 10.0' -H 'Accept: application/json'
'https://<QRADAR_IP_ADDRESS/api/gui_app_framework/applications/<QRADAR_PLUGIN_APPLICATION_ID>?st
atus=STOPPED'
```

1. Navigate to the ``/store/docker/volumes/qapp-<your app-id>` directory.
2. Make a copy of the `resilient.db` file.
3. Restart the QRadar Plugin. This is best done using the API, as described in the QRadar API documentation. The following is an example curl command using the version 10.0 API:

```
curl -s -X POST -u <USER> -H 'Version: 10.0' -H 'Accept: application/json'
'https://<QRADAR_IP_ADDRESS/api/gui_app_framework/applications/<QRADAR_PLUGIN_APPLICATION_ID>?st
atus=RUNNING'
```

QRadar plugin database rollback

Before rolling back the database, you must stop the QRadar plugin. This is best done using the API, as described in the QRadar API documentation. The following example shows a curl command using the version 10.0 API:

```
curl -s -X POST -u <USER> -H 'Version: 10.0' -H 'Accept: application/json'
'https://<QRADAR_IP_ADDRESS/api/gui_app_framework/applications/<QRADAR_PLUGIN_APPLICATION_ID>?st
atus=STOPPED'
```

1. Enter the Docker image for the Resilient QRadar App.
2. Navigate to the `/store` directory.
3. Replace the `resilient.db` file with the backup file.
4. Restart the QRadar Plugin. This is best done using the API, as described in the QRadar API documentation. The following is an example curl command using the version 10.0 API:

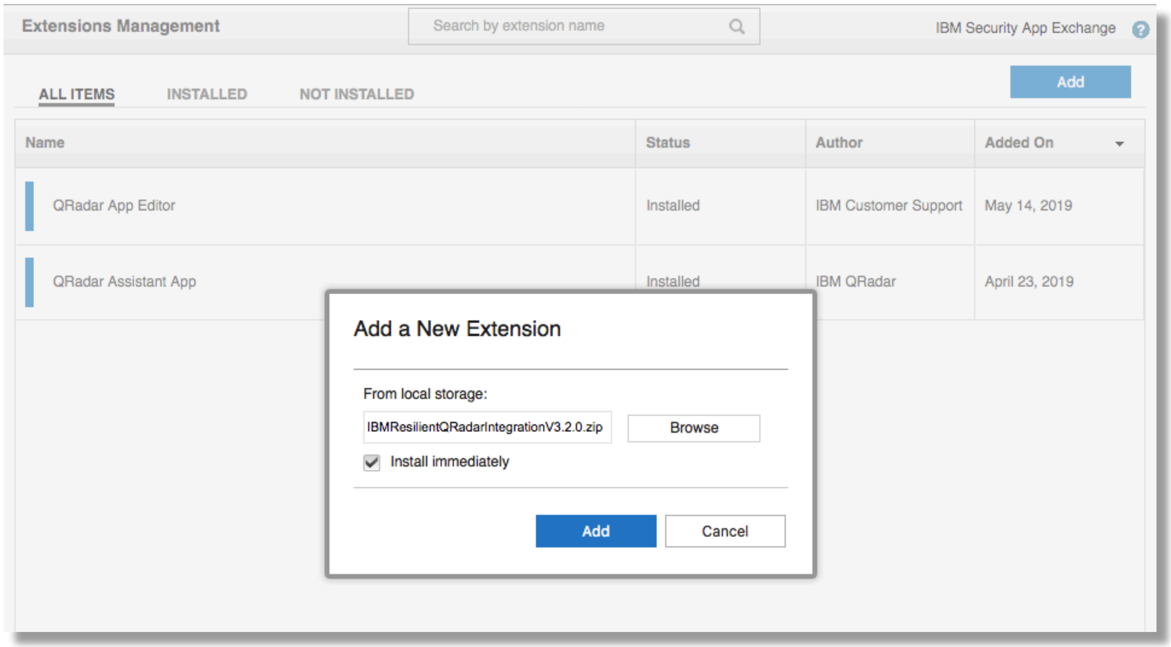
```
curl -s -X POST -u <USER> -H 'Version: 10.0' -H 'Accept: application/json'
'https://<QRADAR_IP_ADDRESS/api/gui_app_framework/applications/<QRADAR_PLUGIN_APPLICATION_ID>?st
atus=RUNNING'
```

Upgrade

You can upgrade your IBM Resilient QRadar Integration from version 3.1.x to 3.3.x. You perform the upgrade from the Extension Management tool located in the administrator console. You must have administrator privileges in QRadar to upgrade the plugin.

Perform the following steps to upgrade QRadar integration:

1. In the administrator console in QRadar, select the Extensions Management tool icon.
2. In the Extensions Management window, click the **Add** button.
3. Click **Browse** then select the QRadar integration zip file.
4. Check the **Install immediately** option to begin installation once the application is uploaded to the QRadar repository.
5. Click the **Add** button to start the installation.



Name	Status	Author	Added On
QRadar App Editor	Installed	IBM Customer Support	May 14, 2019
QRadar Assistant App	Installed	IBM QRadar	April 23, 2019

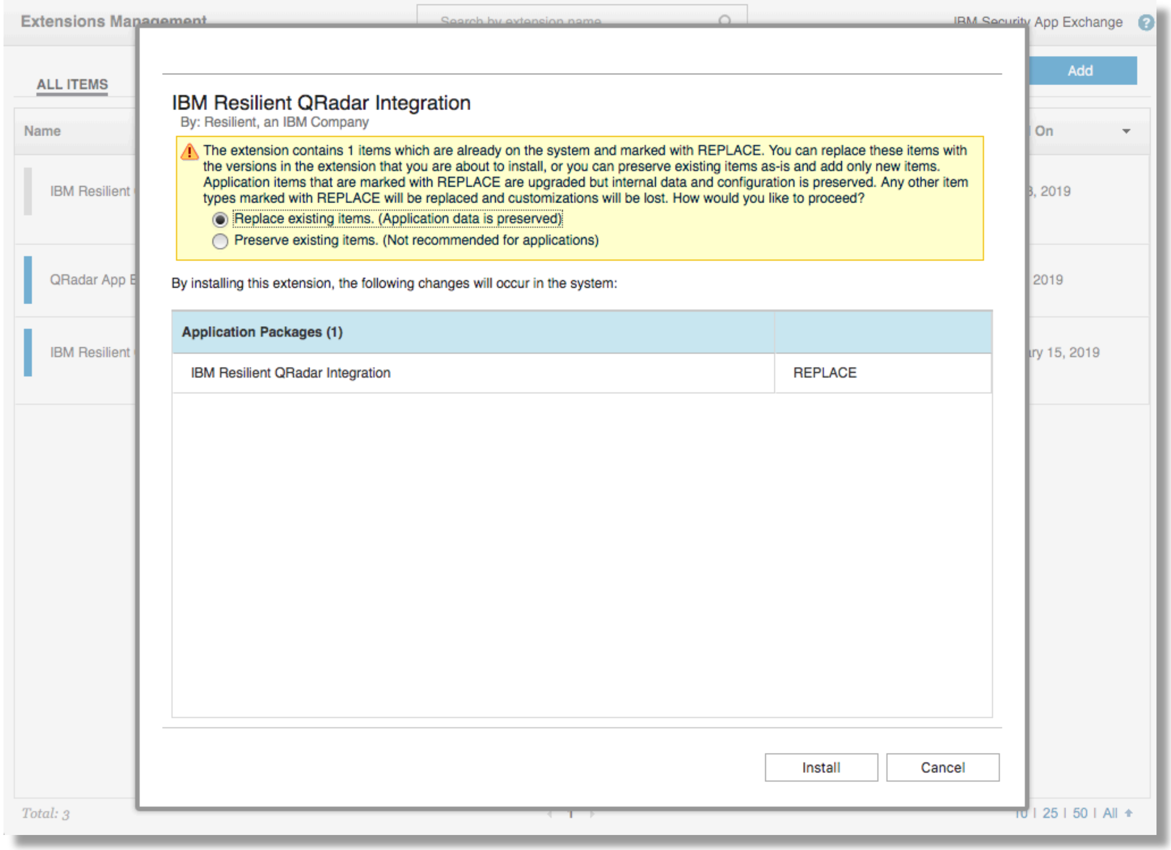
Add a New Extension

From local storage: IBMResilientQRadarIntegrationV3.2.0.zip

☑ Install immediately

6. When prompted, choose **Overwrite** to overwrite your existing data then click **Install**.

   This option should save the templates in /store directory and keep your access configuration.



IBM Resilient QRadar Integration

By: Resilient, an IBM Company

The extension contains 1 items which are already on the system and marked with REPLACE. You can replace these items with the versions in the extension that you are about to install, or you can preserve existing items as-is and add only new items. Application items that are marked with REPLACE are upgraded but internal data and configuration is preserved. Any other item types marked with REPLACE will be replaced and customizations will be lost. How would you like to proceed?

● Replace existing items. (Application data is preserved)

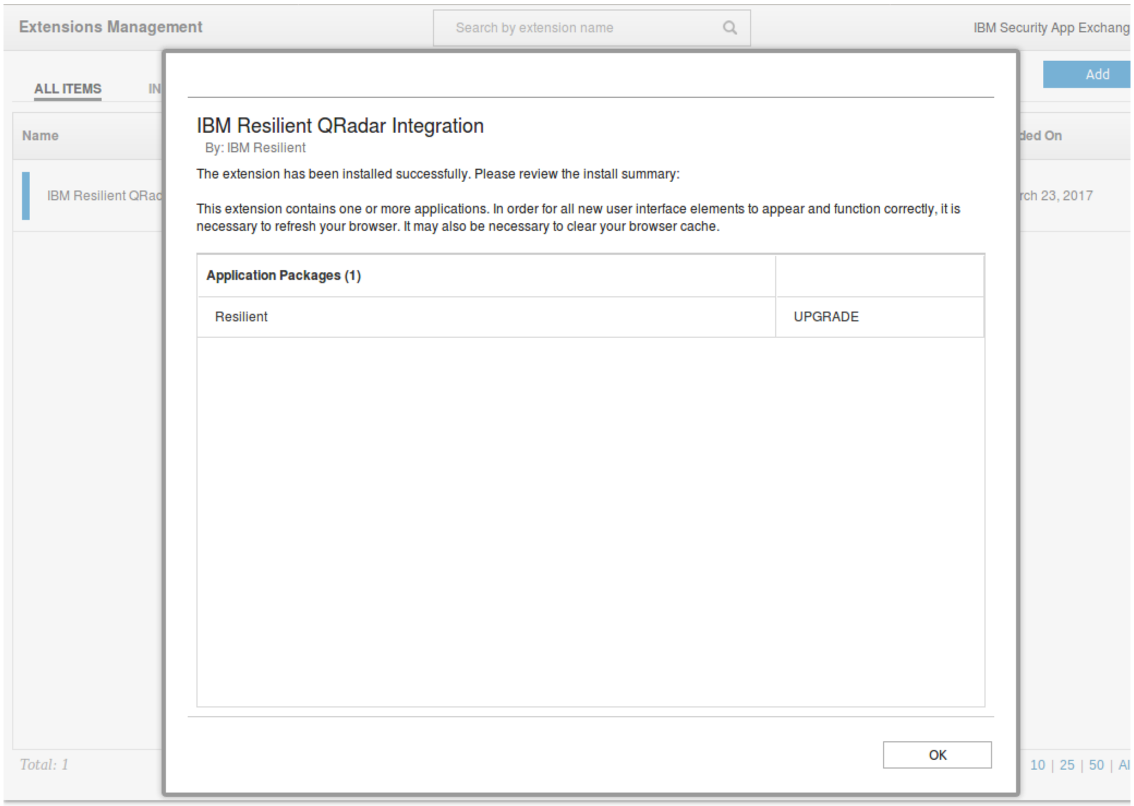
○ Preserve existing items. (Not recommended for applications)

By installing this extension, the following changes will occur in the system:

Application Packages (1)	
IBM Resilient QRadar Integration	REPLACE

Install Cancel

7. Click **OK** to finish the installation when you see the status of UPGRADE.



IBM Resilient QRadar Integration

By: IBM Resilient

The extension has been installed successfully. Please review the install summary:

This extension contains one or more applications. In order for all new user interface elements to appear and function correctly, it is necessary to refresh your browser. It may also be necessary to clear your browser cache.

Application Packages (1)	
Resilient	UPGRADE

When done, make sure to clear your web browser’s cache after installation, as advised by IBM QRadar. The application is upgraded and available for use.

License

IBM Resilient is willing to license software or access to software to the company or entity that will be using or accessing the software and documentation and that you represent, as an employee or authorized agent ("you" or "your"), that you will use or access this software and documentation only on the condition that you accept all of the terms of this license agreement.

The software and documentation within IBM Resilient's Development Kit are copyrighted by and contain confidential information of IBM Resilient. By accessing and/or using this software and documentation, you agree that while you may make derivative works of them, you:

1) will not use the software and documentation or any derivative works for anything but your internal business purposes in conjunction with your licensed used of IBM Resilient's software, nor will you;

2) provide or disclose the software and documentation or any derivative works to any third party.

THIS SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL IBM RESILIENT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.