AT&T Cybersecurity

AT&T Business

USM Anywhere™

AlienApps™ Guide

Updated June 19, 2024

Contents

BlueApps Overview

BlueApps extend the threat detection and security orchestration capabilities of the USM Anywhere platform to other security tools that your IT team uses, providing a consolidated approach to threat detection and response. With BlueApps, you can monitor more of your security posture directly within USM Anywhere, including your cloud services like Microsoft Office 365 and Google G Suite. BlueApps also enable you to automate and orchestrate response actions in security tools from vendors such as Cisco and Palo Alto Networks, greatly simplifying and accelerating the threat detection and incident response processes.

USM Anywhere provides hundreds of BlueApps for different data sources. In addition to translating raw log data into normalized events for analysis by USM Anywhere, some BlueApps also collect and enrich log data, perform threat analysis, and provide workflow that coordinates response actions with the infrastructure and third-party applications to provide security orchestration.

BlueApps extend the capabilities of USM Anywhere through integrations with leading security tools, most specifically in the following areas:

- Data extraction.
- Correlation of data to produce events and alarms.
- Dashboards that display data collected from your network, which help you visualize your environment and alert you to issues originating from a particular data source. These dashboards are visible if you have data for them. Sometimes it takes a few minutes for the dashboards to display. See USM Anywhere Dashboards for more information.

  Important: If there are events from the last seven days, then you can see the related dashboard. When there are no events from the previous seven days, that dashboard doesn't display.

- Orchestration ability that enables you to automate your security operations in a variety of ways. For example, if USM Anywhere finds data associated with a malicious website, orchestration rules might stipulate for this information be sent to the third-party vendor for immediate action. BlueApps with orchestration features are called Advanced BlueApps.

Edition: *All* Advanced BlueApps are available in the Standard and Premium editions of USM Anywhere.

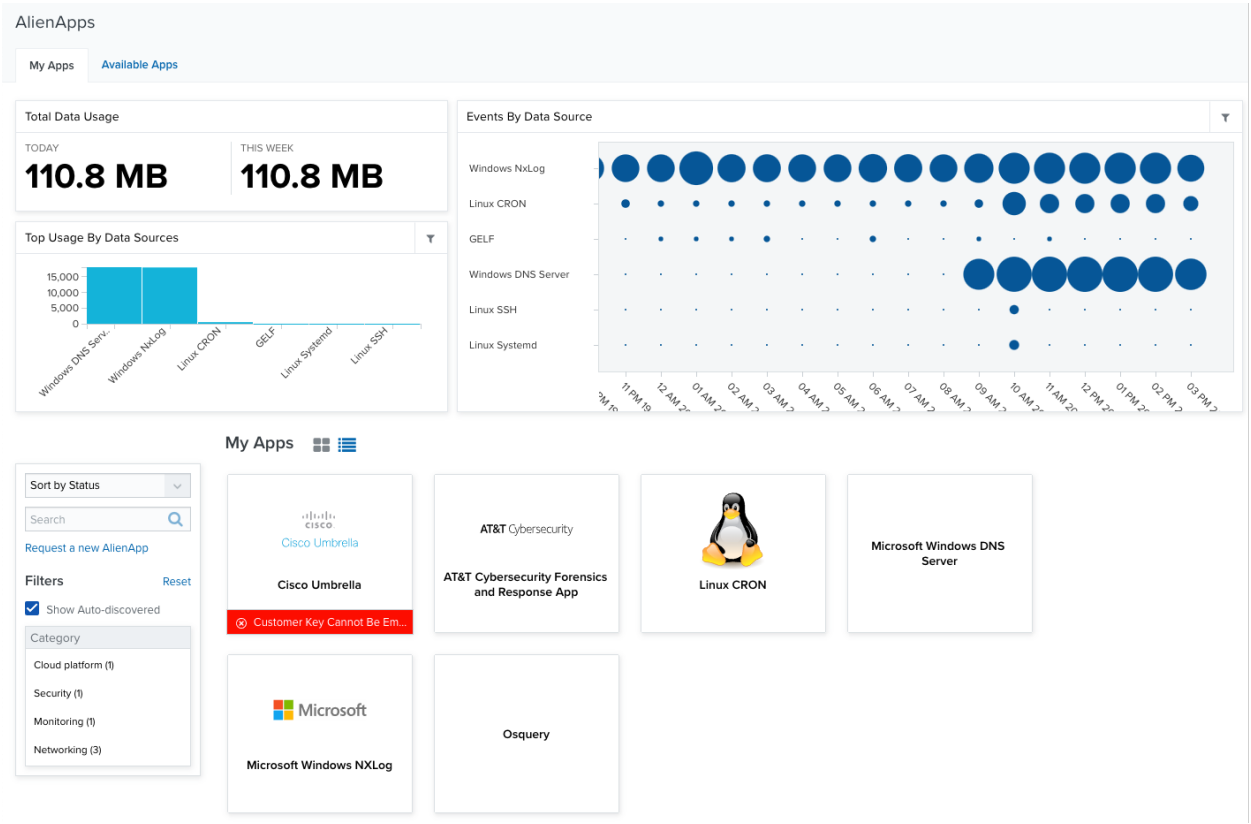
The USM Anywhere Essentials edition *only* has the following Advanced BlueApps:

- BlueApp for G Suite
- BlueApp for McAfee ePO
- BlueApp for Office 365
- BlueApp for Okta
- BlueApp for Sophos Central
- Amazon Web Services (AWS) Log Collection (with an AWS Sensor deployed)
- Google Cloud Platform (GCP) Log Collection (with a GCP Sensor deployed)
- Microsoft Azure Log Collection (with an Azure Sensor deployed)

See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

BlueApps UI

Go to **Data Sources > BlueApps** to open the BlueApps main page. Through this page, you can enable BlueApps, set up connection with third-party APIs, or create new rules for your apps. You can also assign assets to these apps.

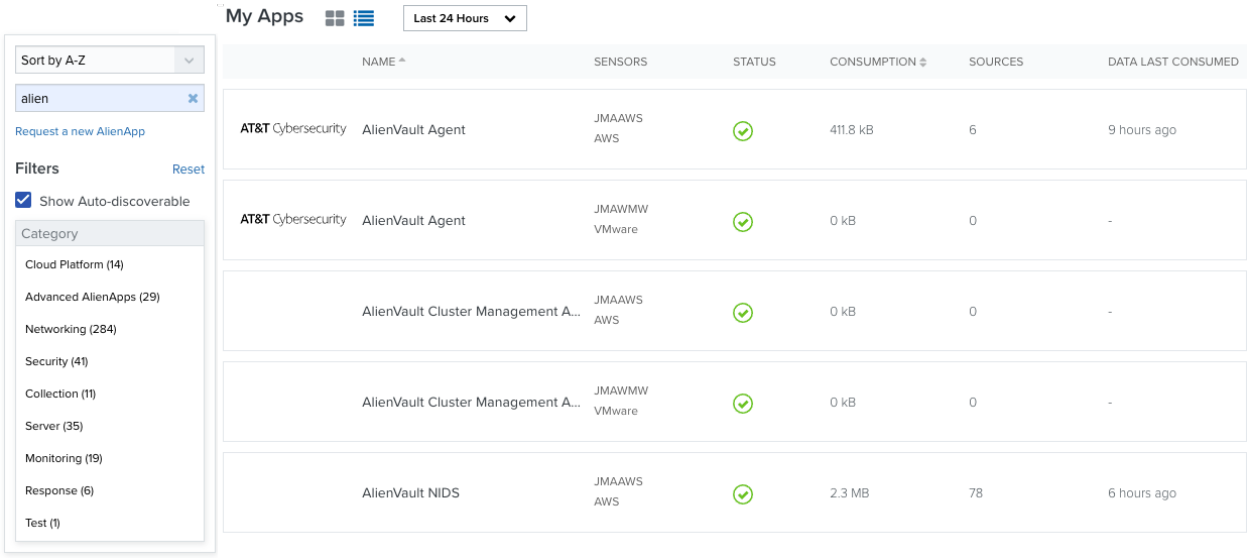


My Apps

The My Apps tab gives you information about the apps you have configured in your environment:

- **Total Data Usage**: Total data usage for the current day and for the current week.
- **Top Usage By Data Sources**: List of top data usage by BlueApps.
- **Events By Data Source**: Events correlated by BlueApps. The size of the bubbles depends on the number of issues.

You can see your apps in a list view ( ) or in a grid view ( ). When you choose the list view, you can use the time filter to limit the display of enabled apps.

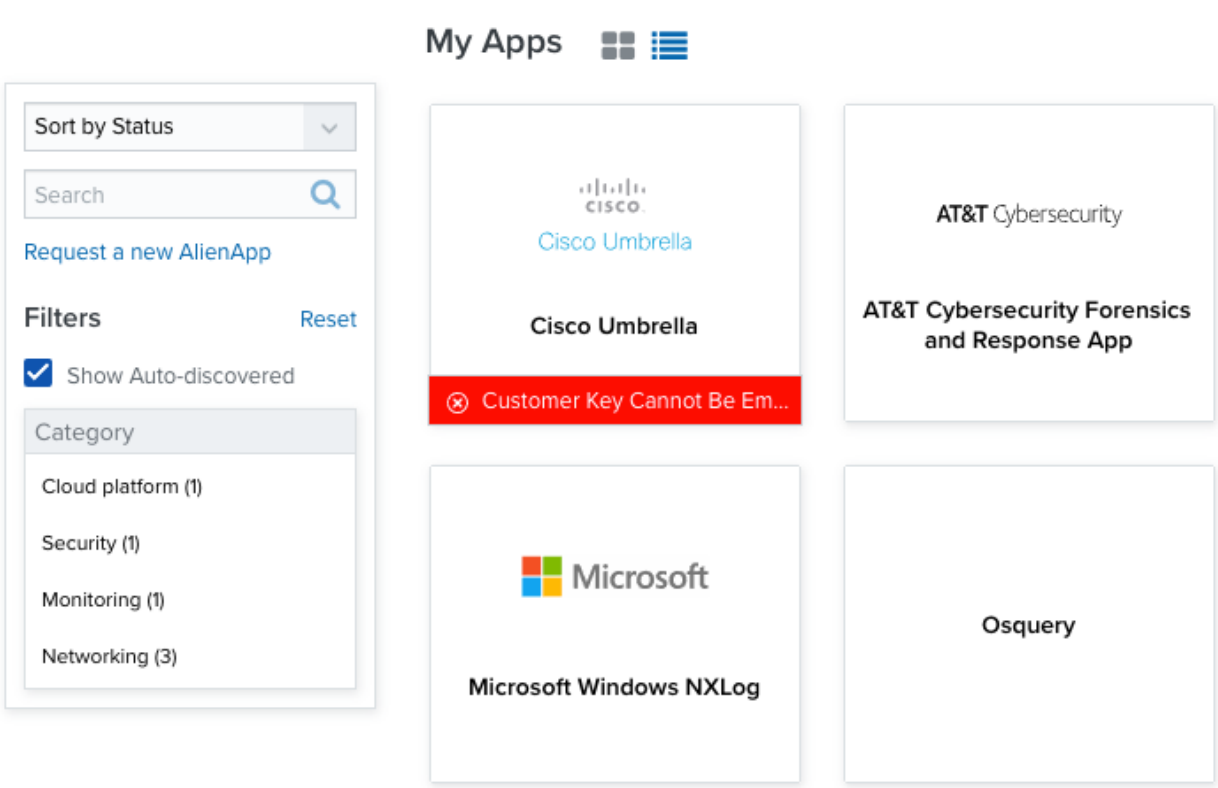


The table below summarizes the columns displayed in the list view.

Columns in the My Apps List View

Name	Description
Name	Name of the BlueApp.
Sensors	Name of the sensor where the BlueApp has been configured.
Status	Status of the BlueApp.
Consumption	Data received by the BlueApp since deployment.
Sources	Number of data sources.
Data Last Consumed	Data received by the BlueApp since last consumption.

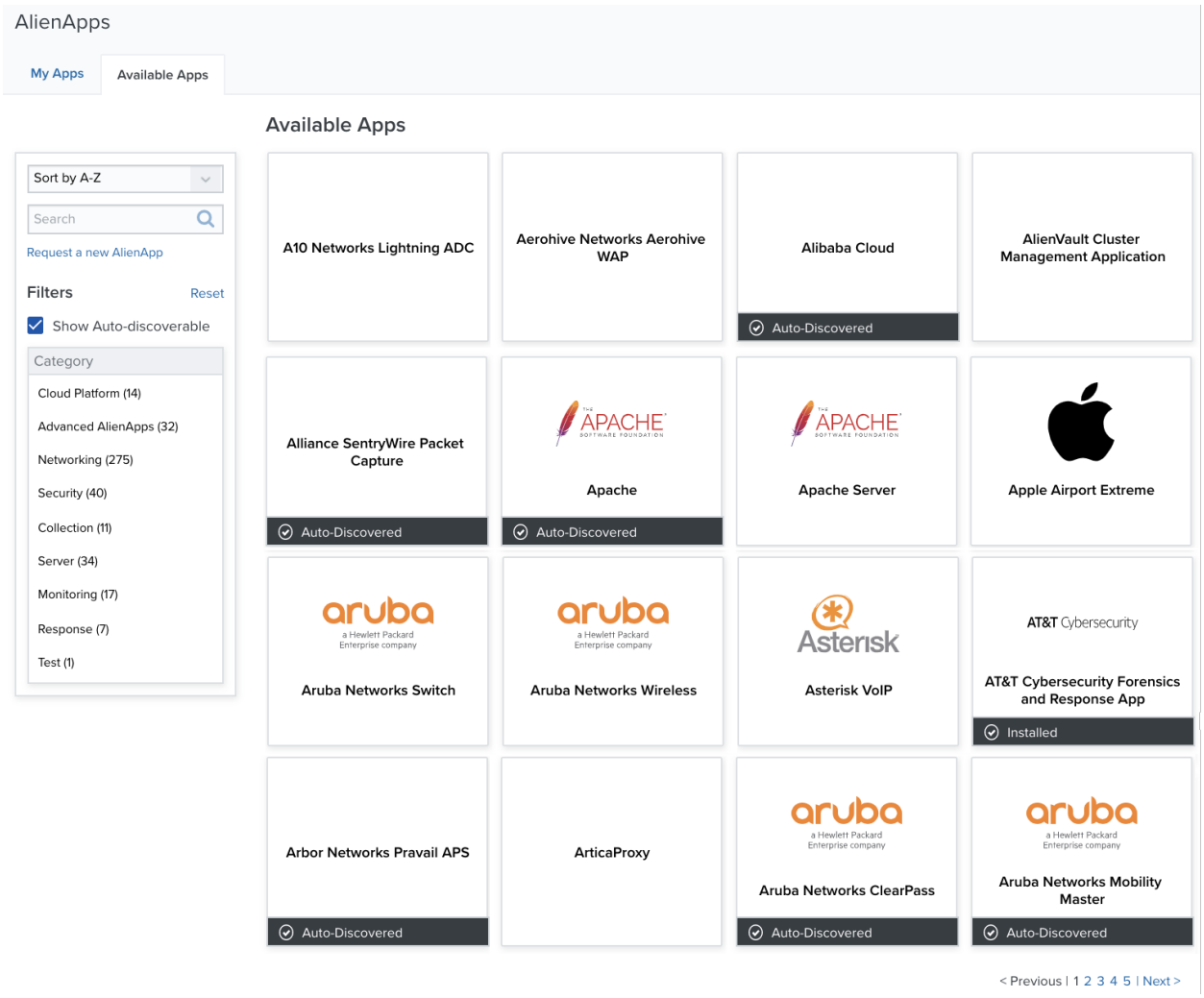
On either view, you can use the filters or search for a specific BlueApp.



You can click a tile to open the specific page for that BlueApp. Sometimes, at the bottom of the tile, you see information about the status of that BlueApp, as shown in the screenshot. You can click the tile to configure the needed data. See Advanced BlueApps for more information.

Available Apps

The Available Apps tab lists all the apps you can configure in your environment.



Through the menu on the left, you can do the following:

- Sort the BlueApps in ascending or descending order.
- Search for an BlueApp by its name.
- Choose whether or not to include auto-discovered BlueApps
- Filter the BlueApps by these categories:
  - Advanced AlienApps
  - Cloud platform
  - Collection
  - Monitoring
  - Networking

- Notification
- Response
- Security
- Server

The number between brackets displayed next to each filter indicates the number of total BlueApps available in your environment.

Click the **Reset** button to remove the selected filters. You can also remove a filter if you click the ✖ icon next to the filter.

On the bottom right corner of the page, you can navigate through the BlueApps and go to the previous or next pages.

Advanced BlueApps Best Practices

USM Anywhere provides you with the opportunity to extend your security capabilities through integrations with a wide variety of advanced BlueApps. To ensure proper functioning, it is important that the association between BlueApps and sensors is adequately handled to avoid errors and duplication of assets and events. Therefore, LevelBlue recommends the following best practice guidelines for proper configuration of your BlueApps.

Best Practice on Associating BlueApps with a Sensor

When configuring your BlueApp, it is recommended to associate it with no more than one sensor. If you connect your advanced AlienApp to multiple sensors you risk the same information being collected multiple times, which can result in the duplication of assets and events. Ensuring that each asset is associated in a one-to-one relationship will result in accurate asset and event reporting.

If this is not possible and you must associate an BlueApp with more than one sensor, apply a different set of BlueApp console credentials to each sensor.

Best Practice on Moving BlueApp Configuration Between Sensors

In the event that you need to move your BlueApp configuration from one sensor to another, you should first move all of the assets created and detected by the BlueApp from the old sensor to the new sensor before setting up your configuration on the new sensor. Once moved, these assets will then be discoverable by the new sensor.

See Editing Assets for more information on how to move assets to a new sensor.

BlueApps and Data Sources

BlueApps parse raw data and convert them into common event fields, such as user, date and time, and source or destination IP address, so that USM Anywhere can manage the information as security events. With a normalized event, USM Anywhere can display information uniformly and correlate events from various systems to generate alarms.

USM Anywhere provides hundreds of BlueApps that translate log data from common devices, operating systems, and applications. When USM Anywhere receives the raw data, it must identify a data source to use for normalization. Many data sources produce syslog messages that can be used to identify the device or application producing the message (auto-discovered), while other data sources produce log data that requires more guidance to identify a match for the data (not auto-discovered).

Data Sources: Auto Discovered or Not

In USM Anywhere, many BlueApps can analyze and match log data automatically because of hints — unique information within a syslog message that identifies the data source sending the logs. When matched, these hints enable the syslog message to be read and the data source to be determined, hence auto-discovered.

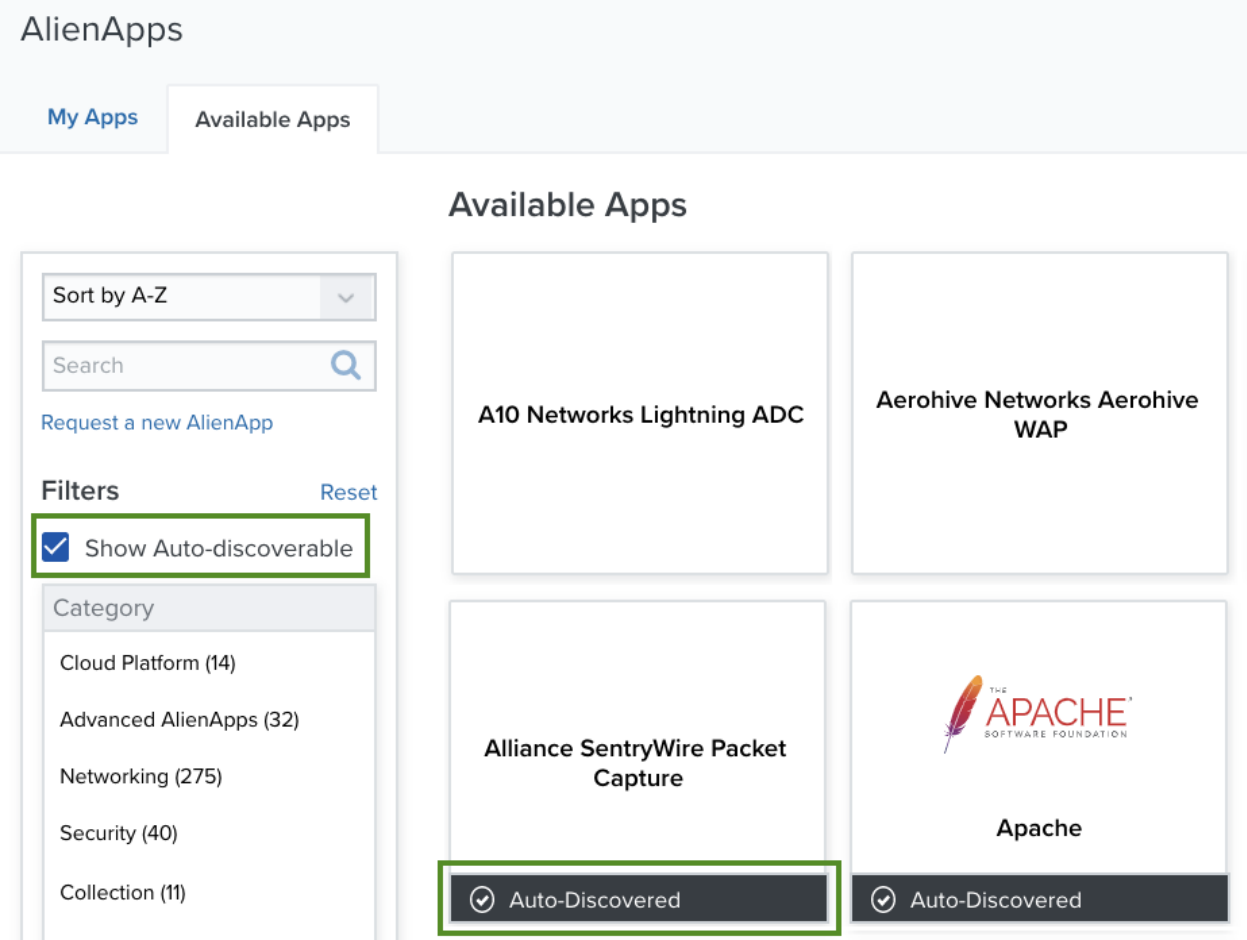
Not all BlueApps accept hints, however, because some syslog messages only contain generic data. For hints to work, syslog messages must contain unique information. When such information is missing, USM Anywhere can neither automatically identify those data sources nor read their syslog data, hence the data sources are not auto-discovered. These BlueApps require a manual association between the device sending the syslog messages and the BlueApp. See Assign Assets to BlueApps for detailed instructions.

Important: Assigning an BlueApp to an asset disables the usage of hints for the logs coming from this asset; therefore, USM Anywhere only uses the assigned BlueApps to parse and normalize those logs.

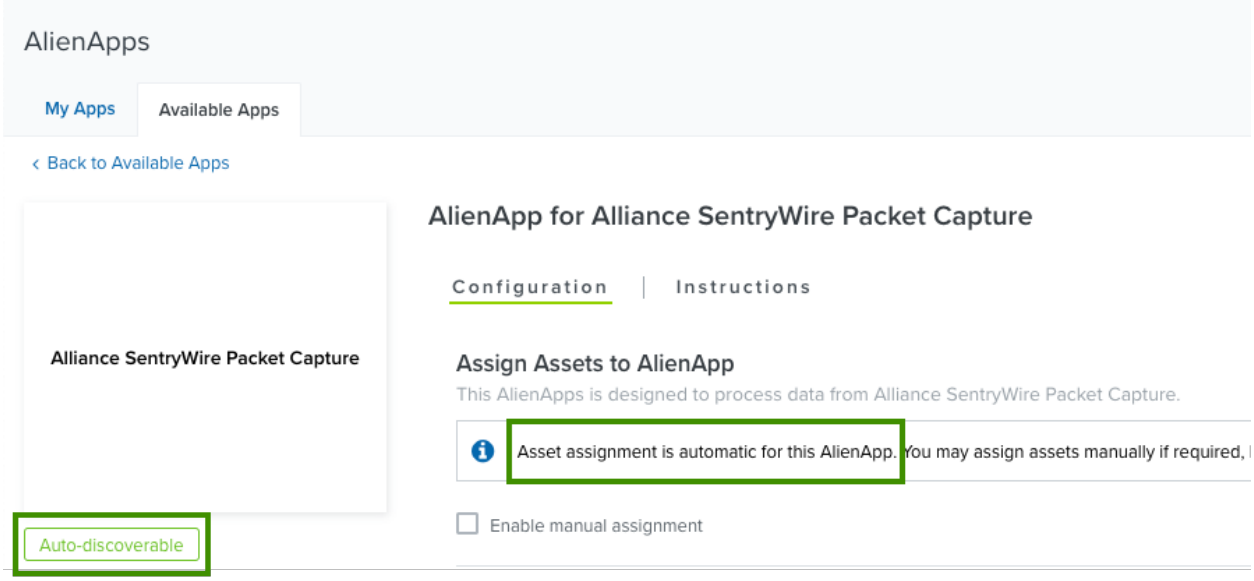
If you use a log-forwarding software (such as Splunk or Loggly) to send logs to USM Anywhere, LevelBlue recommends that you use at least two such forwarders: one forwarder for all the auto-discoverable BlueApps, and the other for the non-auto-discoverable BlueApps. In the latter case, you must create an asset in USM Anywhere to denote the forwarder and assign it to the non-auto-discoverable BlueApps. This ensures that USM Anywhere uses the correct BlueApp to parse your logs.

When multiple BlueApps are assigned to an asset, it can happen that an incorrect BlueApp is invoked to parse and normalize the log message, especially when the needed BlueApp is not included in the list of manually assigned BlueApps.

USM Anywhere clearly indicates whether an BlueApp can auto-discover its data source in the user interface (UI). On **Data Sources > AlienApps > Available Apps**, when Show Auto-discoverable is selected, auto-discovered BlueApps display a black banner at the bottom of the tile:

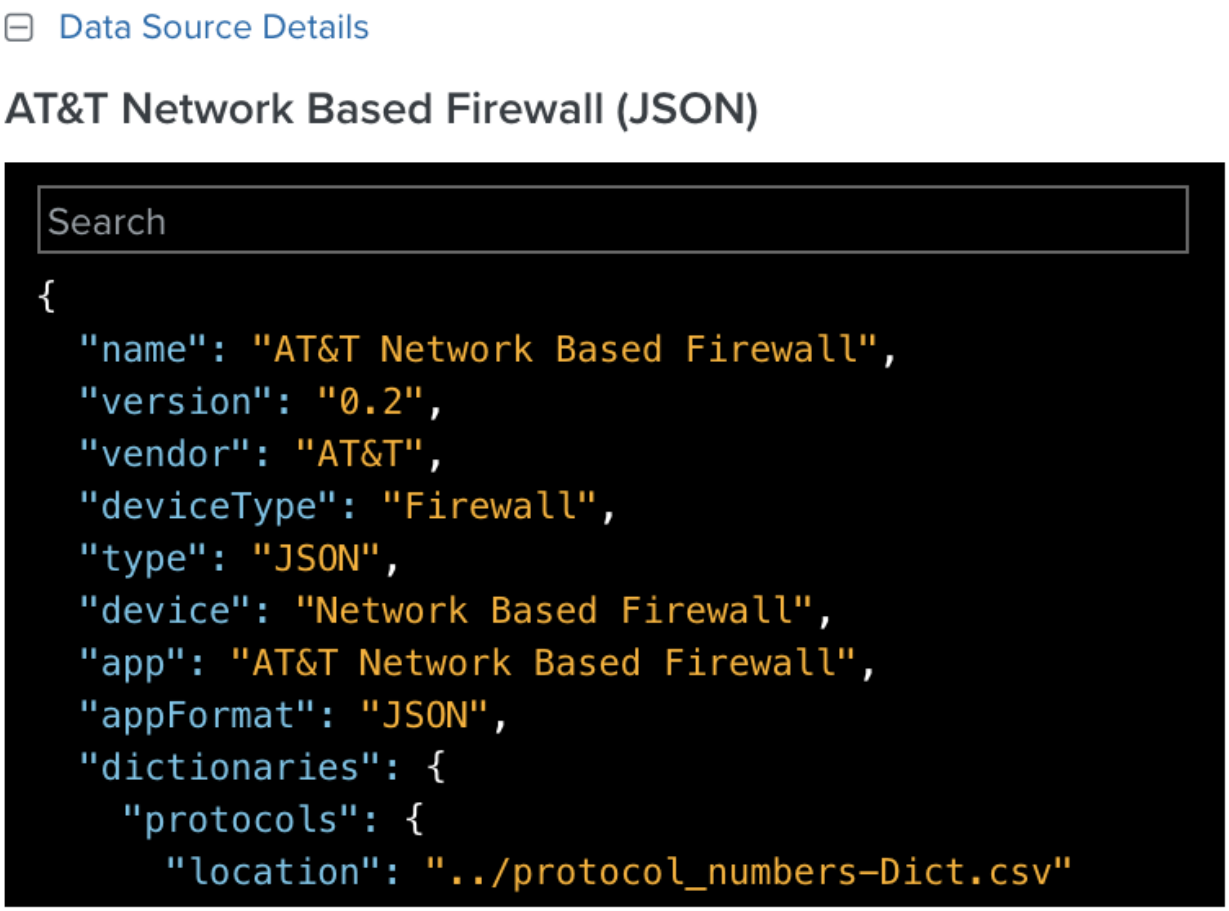


If you click a tile to open the page for a particular BlueApp, look for the following clues to indicate that the BlueApp is auto-discovered:



Data Source Details

Each of the standard BlueApps contains a section of the data source details on the Configuration page. Click ⊞ **Data Source Details** to see the data format and the full list of details for the app's data parsing.



The LevelBlue Generic Data Source

Occasionally, a log line cannot be matched by any BlueApps. This is typically caused by devices that generate non-standard syslog messages. For example, when there are non-standard date formats or other information in the syslog header, the USM Anywhere syslog parser is unable to properly extract the `tag` header. In some cases, you can modify the logging configuration on the device to produce a better result.

For cases where a matching data source is not identified, USM Anywhere parses it using a *generic* data source. This data source parses the log line using regular expressions and advanced text searches, including common log keywords. If USM Anywhere uses the LevelBlue Generic Data Source as a *best effort* to parse a log line, it adds a `Was Fuzzied = True` field to the event. You can view such events on the Activity > Events page. See LevelBlue Generic Data Source in the *USM Anywhere User Guide* for more information.

Assign Assets to BlueApps

USM Anywhere receives syslog log data from external data sources: devices, applications, or operation systems. If that data is not automatically matched with an BlueApp through hints (see Data Sources: Auto Discovered or Not), you must manually associate the BlueApp with an asset in USM Anywhere. There are two methods for creating these associations:

- By assigning one or more assets to the BlueApp (this document).
- By adding one or more BlueApps to the asset. See Adding BlueApps to an Asset for details.

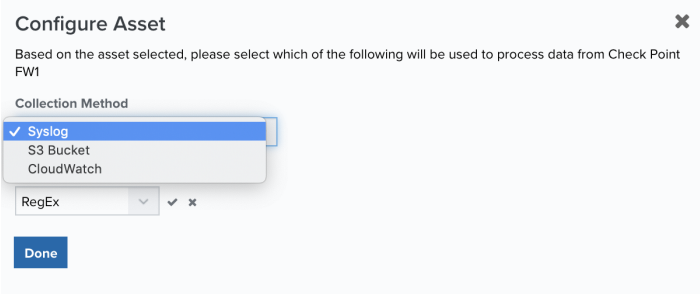
You can use a combination of these methods to ensure that USM Anywhere can identify the correct BlueApps for the log data it receives from an asset.

Important: Assigning an BlueApp to an asset disables the usage of hints for the logs coming from this asset; therefore, USM Anywhere only uses the assigned BlueApps to parse and normalize those logs.

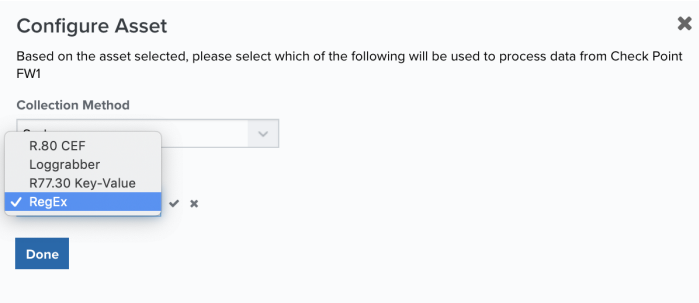
If you use a log-forwarding software (such as Splunk or Loggly) to send logs to USM Anywhere, LevelBlue recommends that you use at least two such forwarders: one forwarder for all the auto-discoverable BlueApps, and the other for the non-auto-discoverable BlueApps. In the latter case, you must create an asset in USM Anywhere to denote the forwarder and assign it to the non-auto-discoverable BlueApps. This ensures that USM Anywhere uses the correct BlueApp to parse your logs.

To assign an asset to an BlueApp

1. Go to **Data Sources > BlueApps > Available Apps**.
2. Look for the BlueApp you want to use and click the tile.
3. After the page finishes reloading, click **Assign Asset**.
4. Select the asset you want to assign. Click **Create Asset** to add an asset if it is not yet in USM Anywhere.
5. Click **Assign**.
6. When applicable, select the collection method you want to use.



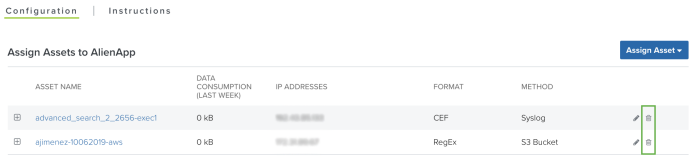
7. When applicable, select the format. See BlueApps Supported Log Formats for more information.



8. Click the ✔ icon to confirm.
9. Click **Done**.

To remove an asset from an BlueApp

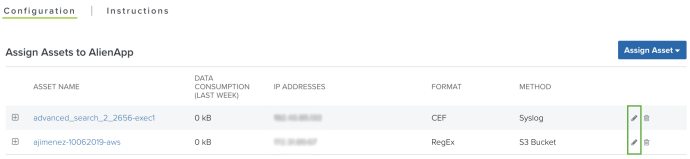
1. Go to **Data Sources > BlueApps > Available Apps**.
2. Look for the BlueApp from which you want to remove the asset and click the tile.
3. Click the 🗑 icon.



4. Click **Accept** to confirm.

To modify an assigned format

1. Go to **Data Sources > BlueApps > Available Apps**.
2. Look for the BlueApp you want to modify and click the tile.
3. Click the icon of the asset.



4. Select the new format you want to use.
5. Click the icon to confirm.
6. Click **Done**.

BlueApps Supported Log Formats

Some BlueApps in USM Anywhere support multiple formats, giving you the option to select the format suitable to your environment. The following table lists the log formats and provides a sample log line for each one.

Log Formats Supported by BlueApps

Format	Description	Sample Log
CEF	ArcSight Common Event Format	CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension] CEF:0|Security|threatmanager|1.0|100|worm successfully stopped|10| src=10.0.0.1 dst=2.1.2.2 spt=1232
CLF	NCSA Common Log Format	125.0.0.1 user - identifier sjones [10/Oct/2011:13:55:36 -0700] "GET /examp_ alt.png HTTP/1.0" 200 10801
CSV	Comma-Separated Values	2,398778306028,eni-abc,1.1.1.1,2.2.2.2,52392,443,6,11,1935,1461792267,1461792322,ACCEPT,OK

Log Formats Supported by BlueApps (Continued)

Format	Description	Sample Log
GELF	Graylog Extended Log Format	{ "version": "1.1", "host": "example.org", "short_message": "A short message", "level": 5, "_some_info": "foo" }
JSON	JavaScript Object Notation	{"DateTime":1438189080000,"UsersName":"Dev","UsersEmail":"dev@blah.com", "IPAddress":"1.1.1.1","Action":Test"}
Key-Value	A key and value pair	id=”0001” severity=”info” name=”http access” action=”pass” method=”GET” srcip=”1.1.1.1” dstip=“2.2.2.2” user=“myuser”
LEEF	Log Event Extended Format	LEEF:Version|Device Vendor|Device Product|Device Version|Event ID|Name| Severity|key=value<tab>key=value<tab>key=value<tab>key=value LEEF:0|Security|threatmanager|1.0|100|worm successfully stopped|10| src=10.0.0.1 dst=2.1.2.2 spt=1232
RegEx	Regular Expression	sshd[1097]: Failed password for invalid user ben from 1.1.1.1 port 43312 ssh2
Split	The fields are separated using a character other than comma	200|939|3934|1.1.1.1|-|1.1.1.1|'"Technology & Telecommunication”'|"test\test"|false|allowed|2.2.2.2
W3C	Extended Log File Format from W3C	#Fields: time cs-method cs-uri 00:34:23 GET /foo/bar.html
XML	Extensible Markup Language	<Root><EventID>90060</EventID><Priority>4</Priority><Message>Application - End</ Message><Category>AUDIT</Category></Root>

Events Created When BlueApps Stop Receiving Data

USM Anywhere gives you the option to set a threshold of time after which BlueApp inactivity is a concern and you should be alerted. When a BlueApp has not received data from your environment within the configured period of time, USM Anywhere generates monitoring events that display in the Events List View (Activity > Events). Since these events are not tied to any USM Anywhere Sensor that you have deployed, you will see a new sensor with the name of your USM Anywhere subdomain tied to these events. USM Anywhere will generate new monitoring events until the BlueApp starts receiving data again.

Warning: Monitoring events are generated when your BlueApp has not received data from a data source either because the data source is not sending data or because of a filtering rule. If you have a rule that filters data coming from a data source, from the perspective of USM Anywhere, that data source is not sending data.

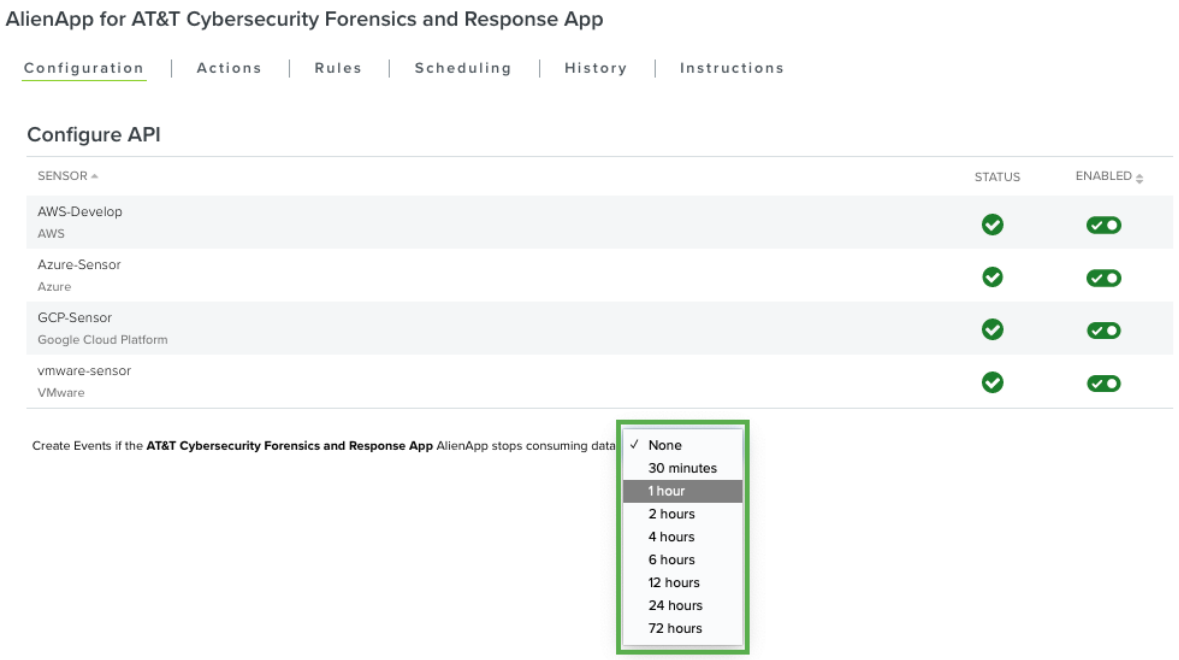
Warning: Currently, the *Event created when BlueApps stop receiving data* event is generated at the same time as the regular event and system event. Soon, this event will be generated only as a system event. See Regular Events and System Events and Orchestration Rule for the "Event from BlueApp Not Received" System Event for more information.

To configure the period of time

1. Go to **Data Sources > BlueApps**.
2. Navigate to your BlueApp and scroll to the bottom of the page.
3. On the bottom of the page, set a period of time in the Create Events If the BlueApp Stops Consuming Data field by clicking the drop-down list.

   You can select a predefined value of None, 30 minutes, 1 hour, 2 hours, 4 hours, 6 hours, 8

hours, 12 hours, 24 hours, 72 hours, 1 week, or 2 weeks.



Note: By default this field is set to None.

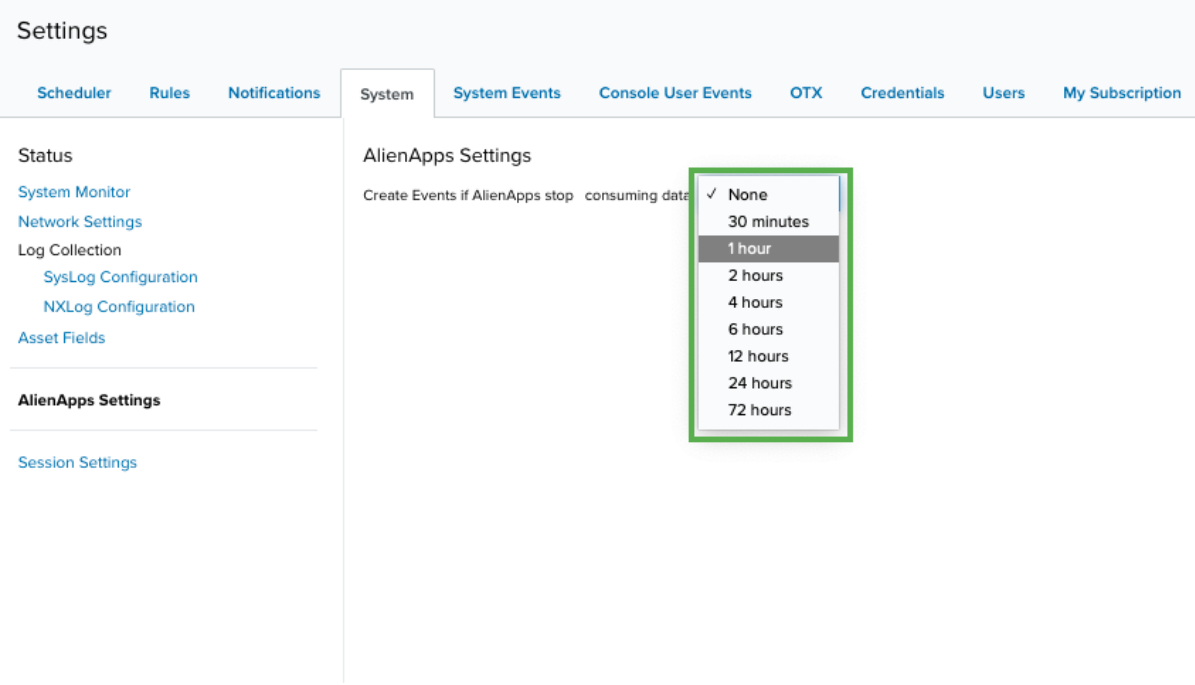
The events are displayed in the Events List View page.

To configure the period of time for all BlueApps

Important: If you configure a global time threshold events will only be generated for any BlueApp that has previously received data. No event will be generated for an app that has not yet received data.

1. Go to **Settings > System**.
2. In the left navigation pane, click **BlueApps Settings** to open the page.
3. Set a period of time in the Create Events If the BlueApps Stop Consuming Data field by

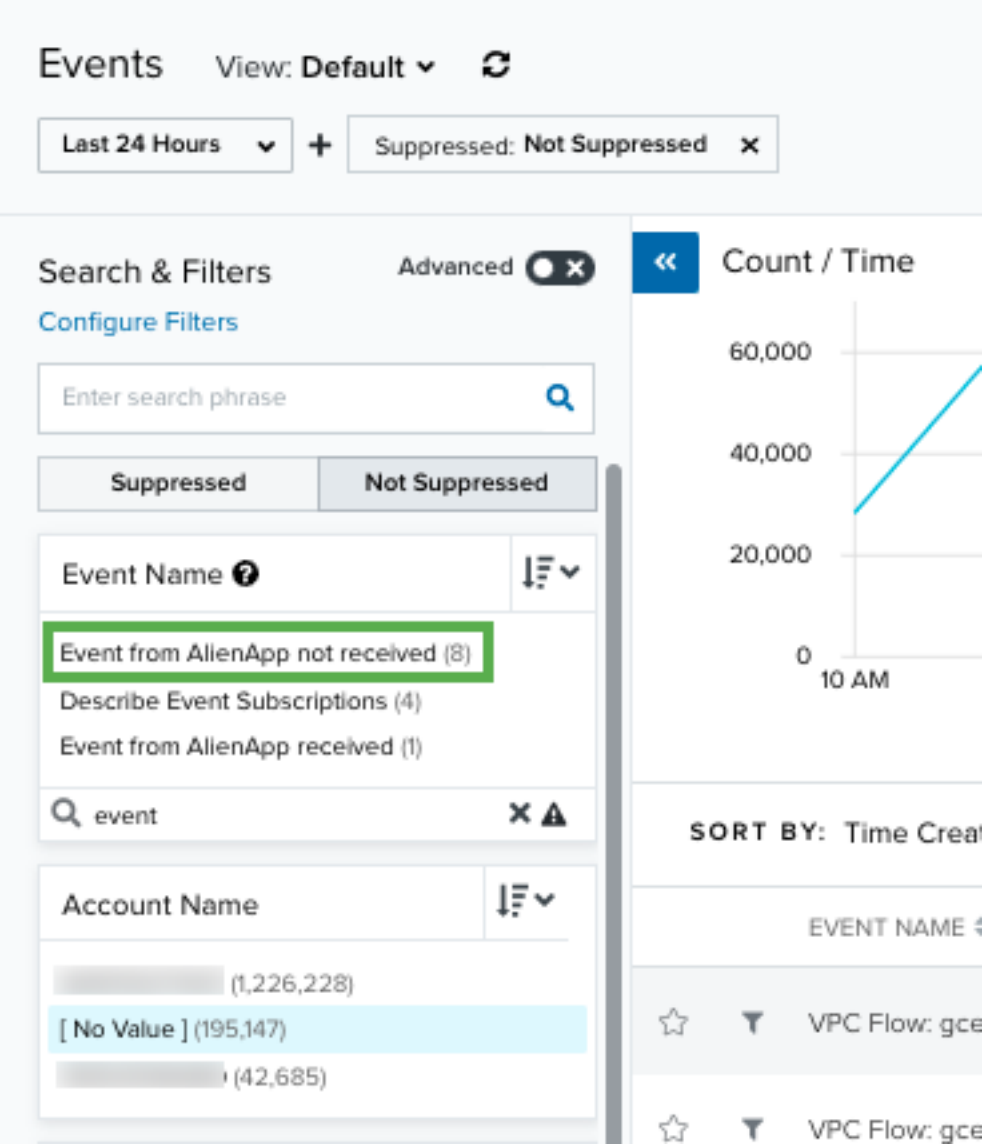
clicking the drop-down list. You can select a predefined value from the options provided.



Note: By default this field is set to None.

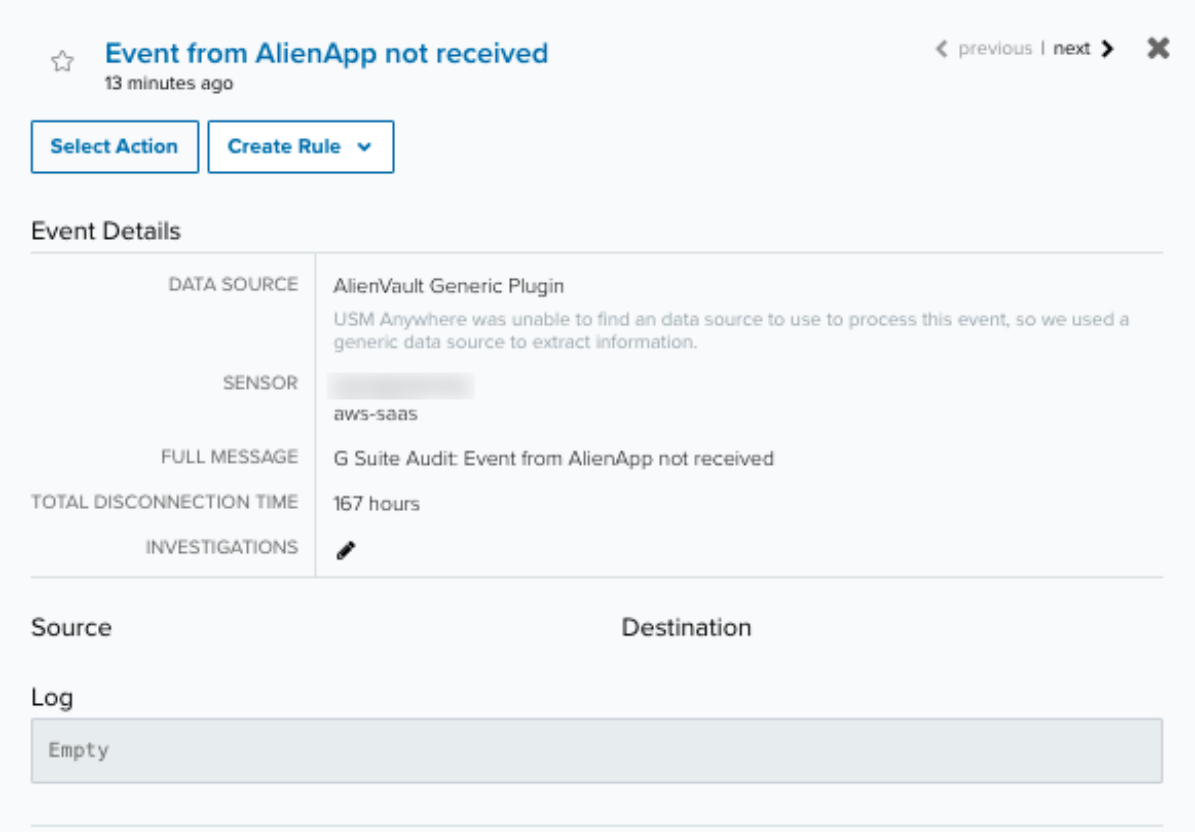
To see events created when your BlueApp stops receiving data

1. Go to **Activity > Events**.
2. In the Event Name filter, select **Event from BlueApp not received**.



The results are shown with the filtered events.

3. Click the event to see its details.



BlueApps Parser Syntax

BlueApps use parsers to extract and normalize data received from different data sources. A parser in USM Anywhere is a JavaScript Object Notation (JSON) file that defines the method of dividing input into different pieces, and then mapping those pieces to the specific fields of a normalized event. The generic parser looks like this:

```
{
	"name": "",
	"type": "",
	"version": "",
	"enrichmentScript": "",
	"device": "",
	"vendor": "",
	"deviceType": "",
	"family": "",
	"parentName": "",
	"parentVersion": "",
	"app": "",
	"hints" : [ ],
	"highlight_fields":
	"properties" : {
		"separator.pair" : "a",
		"separator.groupings" : "b"
	},
	"dictionaries": {
		"main": {
			"load": "main-dictionary-0.1.json"
		},
		"additional": {
			"contents": {
				"val1": [ 'a', 'b', 'c' ],
				"val2": [ 'a', 'b', 'c' ],
				"val3": [ 'a', 'b', 'c' ],
				"val4": [ 'a', 'b', 'c' ]
			}
		}
	},
	"tags": {
		"field1": [
			"map('key1') == '' ? map('key2') : map('key1')"
		],
		"field2": [
```

```
                        "dict('main', map('howdy'), 1)",
                        "regexp(/(d+)(.*)/, dict('additional', map('howdy'), 1), 1)"
                ],
                "field3": [
                        "split(dict('additional', tag('field2')), ',', 2)"
                ]
        }
}
```

The following table includes each field and its description that a parser uses:

Fields and Description Used by a Parser

Field	Description
name	Name of the parser.
type	Log type. The value depends on the log format for the specific data source. Some valid values are these: regex, CEF, CLF, CSV, GELF, JSON, keyvalue, LEEF, split, w3c, XML.
version	Version of the parser.
enrichmentScript	Specify the Lua script used to process a log line.
device	Data source that is sending the logs.
vendor	Data source vendor.
deviceType	Data source type (for example, firewall, router).
parentName	If a parentName is declared for the parser, a copy of the parent parser will be made and the child parser will overwrite that copy.
parentVersion	Version of the parent parser.
app	Name displayed under Data Sources > BlueApps.
hints	References to unique information within a syslog message that identify the data source sending the logs. BlueApps that contain hints will process the message when the information in the log message matches the criteria set within the parser. See BlueApps and Data Sources for more information.
highlight_fields	The most important fields shown in the principal event view.
properties	This field describes the different properties of the parser, depending on the type.

Fields and Description Used by a Parser (Continued)

Field	Description
dictionaries	For each declared dictionary, you can either call out to an external file by name (with the assumption that the path is relative to the parser file) or you can declare the contents of the dictionary inline. Every entry in the dictionary is defined as a key and a series of values.
tags	Tags define how different pieces in a log line map to the fields of a normalized event. For each tag that is defined, the USM Anywhere Sensor begins by evaluating the first code line. If the first code line returns a value, the field in event will be populated with that value. Otherwise, it evaluates the next code line until one returns a non-null value.
rules	For regular expression (regex)-type parsers, there is a set of rules with these fields: • **name**: name of the rule • **contains**: pre-match filter • **regex**: regular expression • **tags**: tags to capture

This is an example of a regex parser:

```
{
	"name": "Test Regex Parser",
	"version": "0.1",
	"type": "regex",
	"hints": [
		{
			"typeName": "tag.equals",
			"value": "test"
		}
	],
	"rules": [
		{
			"name": "Rule test 1"
			"regex": "test (\\S+)",
			"tags":
			{
				"event_name": "concat('test 1')",
				"customfield_0": "map(1)"
			}
		},
```

```
                {
                        "name": "Rule test 2"
                        "contains": ["test2"],
                        "regex": "test2 (?<src>\\S+) (?<dst>\\S+)",
                        "tags": {
                                "event_description": "concat('test 2')",
                                "source_username": "map('src')",
                                "destination_username": "map('dst')"
                        }
                }
        ]
}
```

Advanced BlueApps

Advanced BlueApps can do one or more of the following:

- Log collection
- Network inventory
- Orchestration
- Notification
- Vulnerability assessment
- Response

While regular BlueApps parse syslog forwarded from third-party devices, advanced BlueApps collect logs through the third-party Representational State Transfer (REST) API. In addition, through sensors deployed in various cloud environments, advanced BlueApps can collect logs from Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) using their native tools. See the following documentation for more information:

- AWS Log Collection
- Azure Log Collection
- GCP Log Collection

Some advanced BlueApps provide orchestration to automate your security operations. For example, if USM Anywhere finds data associated with a malicious website, orchestration rules might stipulate that such information be sent to a third-party application for immediate action. Both the BlueApp for Carbon Black EDR and the BlueApp for Cisco Umbrella provide this functionality.

For orchestration to work, you need to configure each BlueApp to connect with the third-party application. You will find configuration instructions for the different BlueApps in the left navigation menu.

Actions from some advanced BlueApps can be included as part of a playbook. Playbooks are a set of predefined actions that should always be taken in response to one or more types of alarms. You can choose app-specific actions for your playbooks that will execute through or on behalf of a specific BlueApp. Some of these app-specific actions can be automated and will execute on their own. Some are manual only and require users to run the actions. See Playbooks for more information.

Note: If there are any specific apps, app actions, or automated actions you would like to have added to playbooks that are not currently available, you can submit a request to have them considered for playbooks.

Edition: Advanced BlueApps are available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

BlueApp for Akamai Enterprise Application Access

The BlueApp for Akamai Enterprise Application Access (EAA) enables you to integrate the Akamai EAA capabilities with your USM Anywhere instance. The BlueApp for Akamai Enterprise Application Access enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from the Akamai EAA and provides orchestration actions to implement Akamai EAA incident response activities based on risk identified in USM Anywhere.

Edition: The BlueApp for Akamai Enterprise Application Access is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Akamai Enterprise Application Access

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

To configure the BlueApp for Akamai Enterprise Application Access in USM Anywhere, you need to have the Akamai Host URL, an API Access Token, Client Token, and Client Secret.

To set up your Akamai API

Follow the instructions listed in the Akamai API documentation. Here you will find the instructions on how to generate the Access Token, Client Token, and Client Secrets for USM Anywhere.

Note: You need to create the API client using an account with either READ-WRITE or ADMIN access for Akamai EAA to receive information from USM Anywhere.

Configure BlueApp for Akamai Enterprise Application Access in USM Anywhere

To enable the BlueApp for Akamai Enterprise Application Access

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Akamai Host URL, an API Access Token, Client Token, and Client Secret.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the  icon for the inactive collection job.

   The  icon turns green, and collection is enabled.
4. (Optional.) Click the  icon to customize the frequency of the event collection.

BlueApp for Akamai Enterprise Application Access Actions

The AlienApp for Akamai Enterprise Application Access (EAA) provides a set of orchestration actions that you can use to integrate the Akamai EAA capabilities with your USM Anywhere instance in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Akamai Enterprise Application Access

Action	Description
Access Log Collector	Run this action to collect logs from Akamai EAA
Scan Users	Run this action to perform Akamai EAA user scanning
Block the User	Run this action to block the user from an event or alarm
Block the User	Run this action to block the user from a response action rule to restrict their access

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms and Events

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or an event.

To launch an Akamai EAA response action for an alarm or event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Akamai EAA Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Akamai EAA Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ **Analyst** ✔ **Manager**

You can create orchestration rules in USM Anywhere that automatically trigger an Akamai Enterprise Application Access (EAA) response action when alarms or events match the criteria that you specify. After you create a rule, new vulnerabilities that match the rule conditions will trigger the Akamai EAA response action to create a new incident. The rule does *not* trigger for existing alarms or events.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

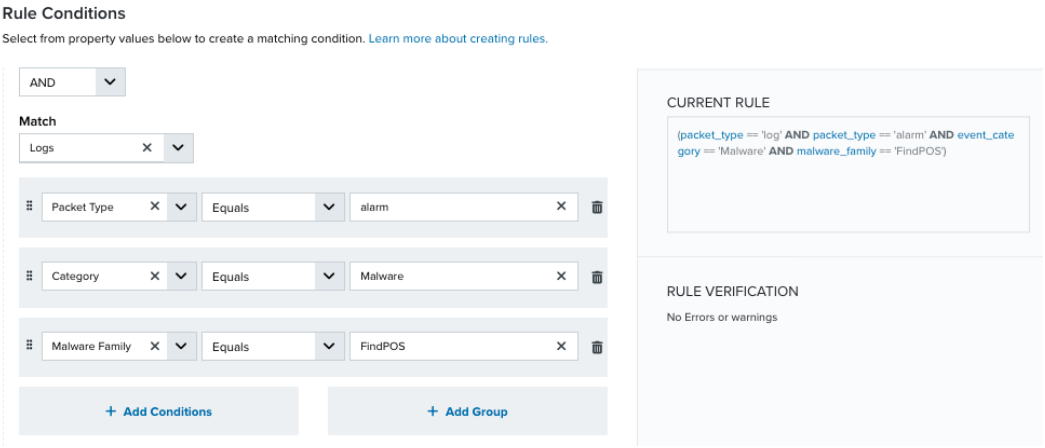
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the app**: Go to the BlueApp for Akamai Enterprise Application Access page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new Akamai EAA response action rule

1. Enter a name for the rule.
2. Select the app action for the rule and specify the information for the Akamai EAA incident.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Akamai Enterprise Threat Protector

The BlueApp for Akamai Enterprise Threat Protector (ETP) enables you to integrate the Akamai Enterprise Threat Protector capabilities with your USM Anywhere instance. The BlueApp for Akamai Enterprise Threat Protector enhances the capabilities of your threat detection management by utilizing Akamai ETP's ability to monitor threat events, Acceptable Use Policy (AUP) events, Domain Name System (DNS) events, network traffic events, and network proxy traffic. With the BlueApp for Akamai Enterprise Threat Protector, you can take the information provided from Akamai ETP and integrate it with your USM Anywhere to create orchestration actions and response actions in response to the information received.

Edition: The BlueApp for Akamai Enterprise Threat Protector is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Akamai Enterprise Threat Protector

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To configure the BlueApp for Akamai Enterprise Threat Protector in USM Anywhere, you need to have the Akamai Host URL, an API Access Token, Client Token, and Client Secret.

To set up your Akamai API

Follow the instructions listed in the Akamai API documentation. Here you will find the instructions on how to generate the Access Token, Client Token, and Client Secrets for USM Anywhere.

Note: You need to create the API client using an account with either READ-WRITE or ADMIN access for Akamai ETP to receive information from USM Anywhere.

Configure BlueApp for Akamai Enterprise Threat Protector in USM Anywhere

To enable the BlueApp for Akamai Enterprise Threat Protector

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Akamai Host URL, an API Access Token, Client Token, and Client Secret.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Akamai Enterprise Threat Protector Actions

The BlueApp for Akamai Enterprise Threat Protector (ETP) provides a set of orchestration actions that you can use to identify vulnerabilities and manage assets in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Akamai Enterprise Threat Protector

Action	Description
Add Items to Block List	Run this action to add items to a block list from an event or alarm to restrict their access
Add Items to Allowlist	Run this action to add items to an allowlist to grant authorized access
Remove Items from Block List	Run this action to remove items from the Akamai ETP block list
Remove Items from Allowlist	Run this action to remove items from an allowlist via an event or alarm
Add Items to Block List from Rule	Run this action to add items to a block list from a rule to restrict their access
Add Items to Allowlist from Rule	Run this action to add items to an allowlist from a rule to grant authorized access

Actions for the BlueApp for Akamai Enterprise Threat Protector (Continued)

Action	Description
Remove Items in Block List from Rule	Run this action to remove items from a block list based on a predefined rule to restrict their access
Remove Items in Allowlist from Rule	Run this action to remove items from an allowlist based on a predefined rule to restrict or revoke access
Create Custom List	Run this action to create a custom Akamai ETP flist

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Action from Alarms or Events

When you review the information in the Alarm Details or Event Details page, you can easily launch an action to have USM Anywhere respond to threats or suspicious activity generated from Akamai ETP.

To launch an Akamai ETP response action for an alarm or event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Akamai ETP Action**.
5. Select the app action.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Akamai ETP Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger BlueApp for Akamai Enterprise Threat Protector (ETP) response actions when events, or alarms match the criteria that you specify. This way, you can automate the way you filter IP addresses into the policies within the Akamai ETP user interface (UI).

After you create a rule, a new event, or alarm that matches the rule conditions trigger the Akamai ETP response action to create a new incident. The rule does *not* trigger for existing events or alarms.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new Akamai ETP response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the Akamai ETP incident.

   The Akamai ETP parameters that you set will depend on the action that you select.

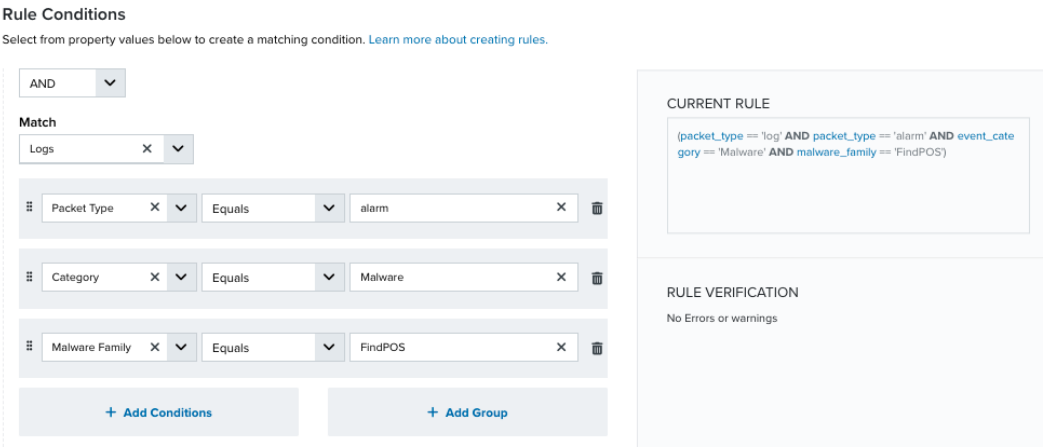
   ### Create a New Incident from an Alarm

   This is the default action if you create the rule after applying a Akamai ETP response action to an alarm. Use this action to run a new Akamai ETP rule for the addresses of a new alarm that satisfies the matching criteria.

   ### Create a New Issue from Event-Based Orchestration

   Use this action to add information to the designated Akamai ETP groups based on an incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions

for the rule.

- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not

trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for LevelBlue Forensics and Response

The BlueApp for LevelBlue Forensics and Response enables you to automate intrusion detection and response activities between USM Anywhere and your asset host systems. This BlueApp enhances the threat detection capabilities of USM Anywhere by collecting and providing Microsoft Windows and Linux system information, and provides orchestration actions to streamline incident response activities for Windows systems based on risks identified in USM Anywhere.

Edition: The BlueApp for LevelBlue Forensics and Response is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for LevelBlue Forensics and Response

To use the BlueApp for LevelBlue Forensics and Response for data collection and enforcement functions on remotes hosts, the target assets must meet the following requirements:

- The asset must be defined in the USM Anywhere asset inventory, be assigned to a sensor, and have configured credentials.
- A Windows asset must have PowerShell 3.0 or above installed.
- The Linux asset must be running Red Hat Enterprise Linux (RHEL) 5+, Fedora 14+, SUSE Desktop 10+, SUSE Enterprise Server 9+, Ubuntu 8.10+, or Debian 6.0+ with SSH enabled.

See System Settings for Authenticated Scans for information about configuring the host system to support remote management functions.

Access Rights for Credentials

USM Anywhere requires privileged access to execute system-level functions for monitored assets. Using an unprivileged account results in many "unknown" and potentially some "error" results. Make sure that you have credentials for the target assets that meet the following requirements:

- For Windows systems, USM Anywhere uses Microsoft Windows Remote Management (WinRM) framework (version 2.0 or higher) to execute the corresponding commands. Therefore, if WinRM is unavailable on a target Windows system through the account credentials, USM Anywhere will be unable to connect.

  Important: Only the members of the Remote Management Users and Administrators groups can log in through Web Services for Management (WS-Management).

- For Linux systems, USM Anywhere connects to the target host through SSH to run the supported functions. USM Anywhere supports the definition of credentials with `sudo` privilege escalation. It also supports login as a particular user followed by a `su` privilege escalation, which executes every command as a root user.

Note: USM Anywhere does not support authenticated scans on Cisco IOS.

Manage Credentials for Your Assets

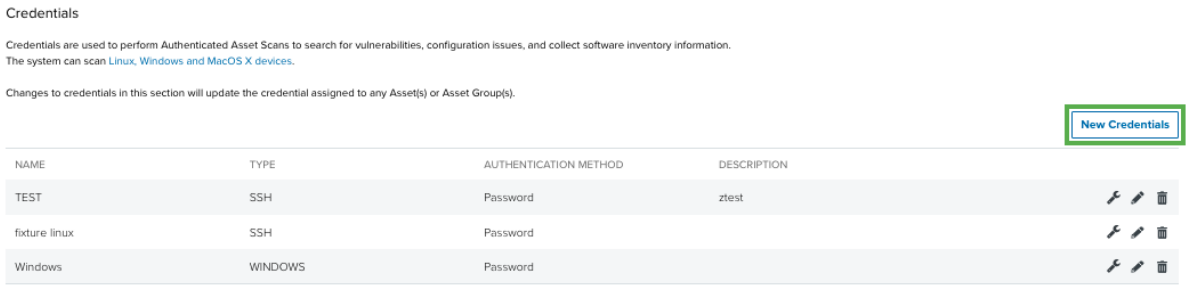
Before you use the BlueApp for LevelBlue Forensics and Response actions to perform collection and enforcement functions for your assets, you should make sure that each of the assets has assigned credentials that are able to connect to the system. In USM Anywhere, you can assign credentials for an individual asset or for an asset group.

Note: Credentials assigned directly to an asset have higher priority than those assigned to an asset group.

When USM Anywhere runs a scan or executes a system-level action, it uses the credential set assigned directly to the asset, if there is one. If those credentials don't connect or the asset doesn't have an assigned credential set, it uses the credential set assigned to the group where the asset is a member, if that asset is a member of an asset group.

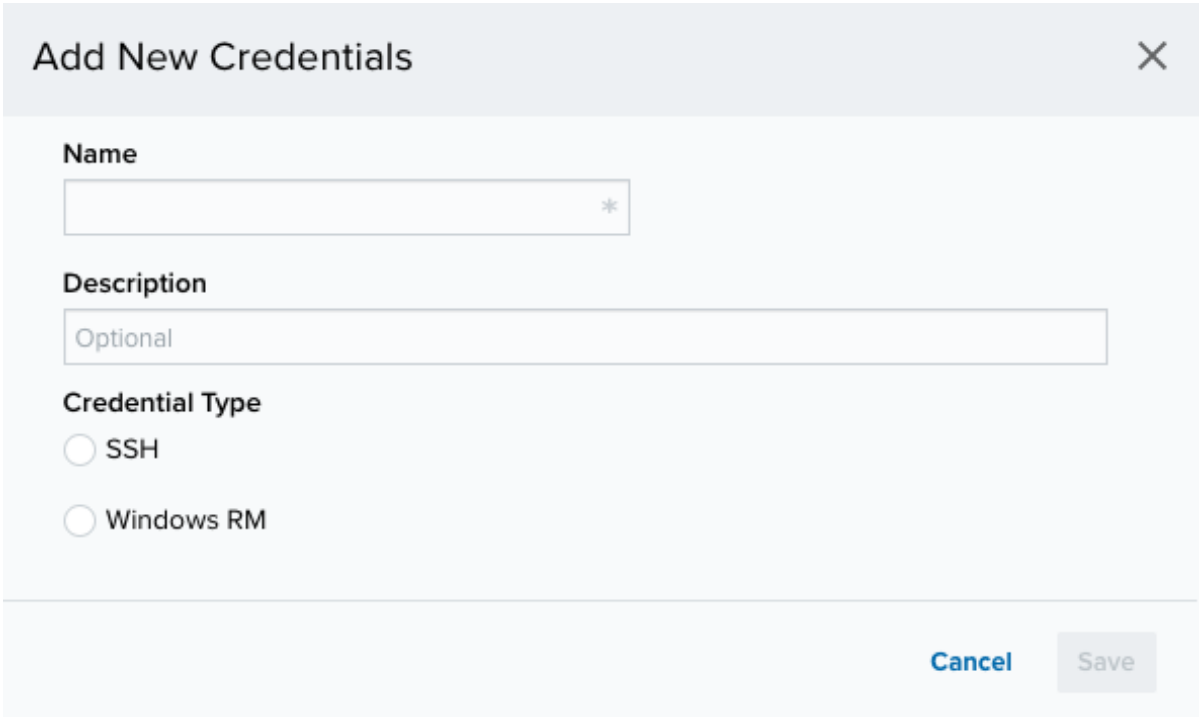
To add a new credential

1. Go to **Settings > Credentials**.



2. Click **New Credentials**.

   The Add New Credential dialog box opens.



3. Enter a name for the credential in the Name field and, if desired, a description to clarify its use in the Description field.
4. In Credential Type, select **SSH** or **Windows RM** based on the operating system of the asset.

Windows RM

Important: Only members of the Administrators or Remote Management Users groups are able to log in through WS-Management. The account used to log in to the target system must have remote and local log-on rights. See Setting Log on Locally and the Security Policy for more information.

Use the Windows RM credential for a Windows operating system. After selecting Windows RM, complete these fields:

- **Username**: Enter the username for the account with the required privileges.

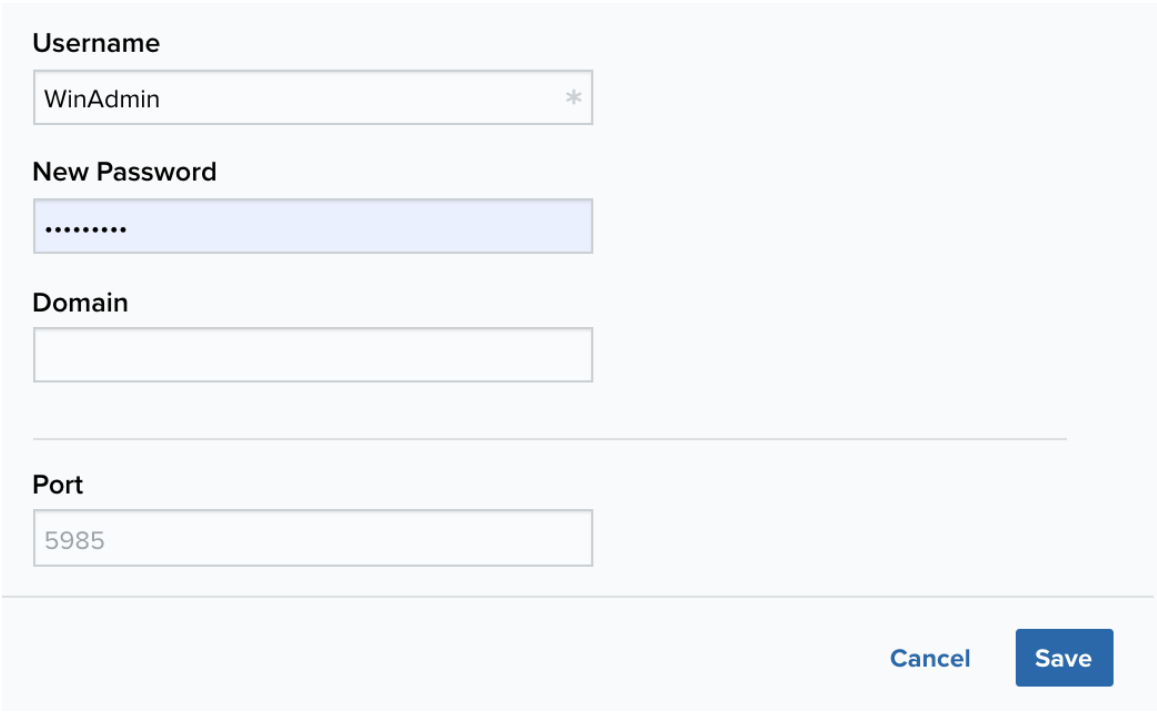
  Important: The username must have 20 characters or less.

- **Password**: Enter the password for the user account.
- **Domain**: (Optional.) Enter the domain name registered in the Domain Name System (DNS).

  Note: Use a fully qualified domain name (FQDN) instead of a Network Basic Input/Output System (NetBIOS) name. If you use a NetBIOS name, you will get an invalid SSH gateway error.

- **Port**: If an alternative port number is required, enter the port number. The default port,

5985, is standard.



SSH

Use the SSH credential for a Linux, Apple macOS, or any other device that supports an SSH connection. After selecting SSH, complete these fields:

- **Username**: Enter the username for the account with the required privileges.
- **Authentication method**: Set the SSH authentication mode and enter the password, private key, or both.
  - **Password**: Select this option to use a simple password to authenticate the user account. It is mandatory if you do not use a private key.
  - **Private key (no passphrase)**: Select this option to use a private key to authenticate the user account.
  - **Private key with passphrase**: Select this option to use a private key and password combination to authenticate the user account.

Important: A private key must start with an appropriate header, such as `"-----BEGIN RSA PRIVATE KEY-----"` and `"-----END RSA PRIVATE KEY-----"`. Always copy the certificate in the form with the header.

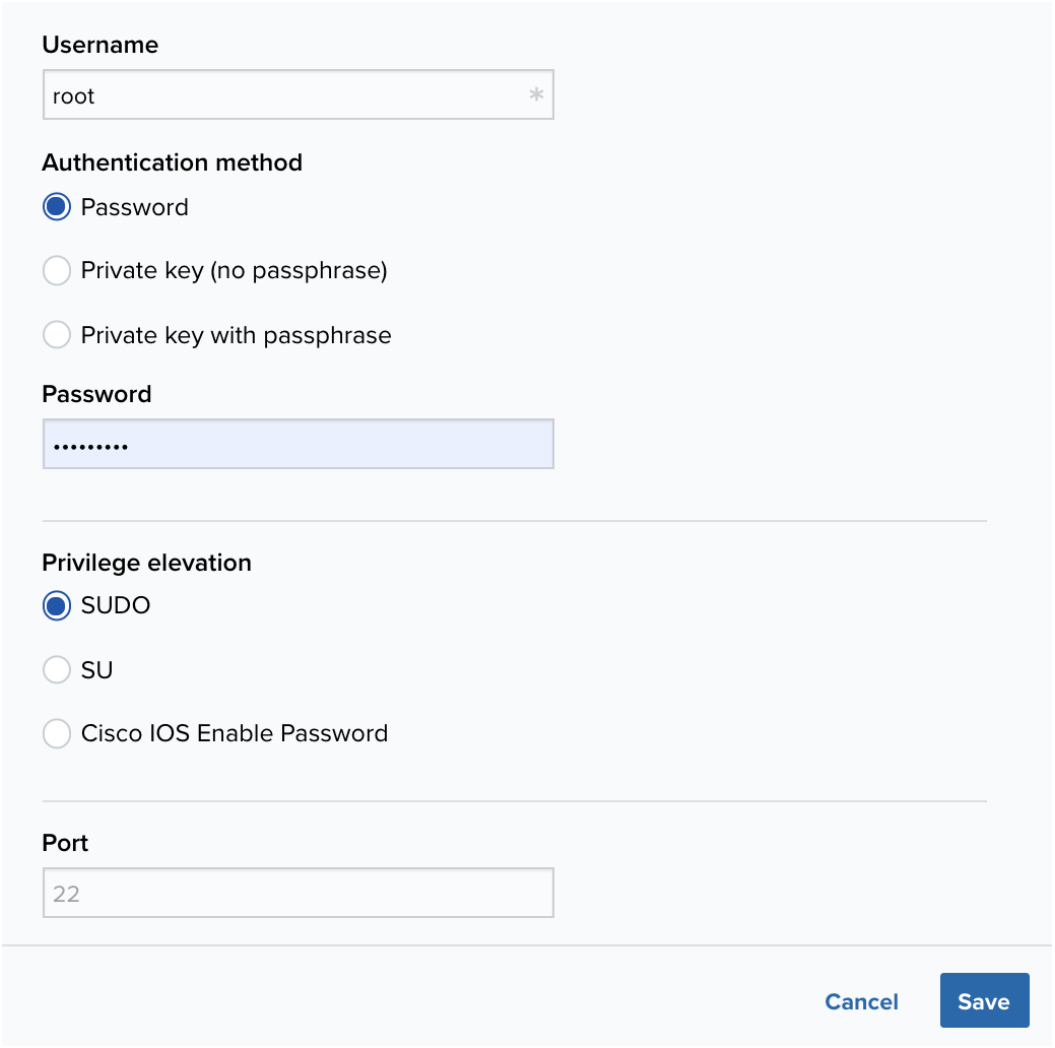
- **Password**: This field only appears if you select Password as authentication method. Enter the password that authenticates the user.
- **Privilege elevation**: Select the elevated privilege to use for the credentials.
  - **sudo**: Use this option to run single commands with root privileges. For example:

    ```
    sudo 'command1'; sudo 'command2'; sudo 'command3' ...
    ```

  - **su**: Use this option to run single commands with superuser privileges. This requires you to enter the username and password for the superuser account. For example:

    ```
    su username -c 'command1'; su username -c 'command2'; su username -c 'command3' ...
    ```

- **Port**: This is automatically set (SSH listens on port 22 by default) and cannot be changed.



5. Click **Save**.

SSH Key Manual Generation

There are a variety of ways to create an SSH key, and your company may already have predefined rules regarding an algorithm to use and what strength the key needs to be. However, if you need to create an SSH key manually and don't have a predefined company policy for the creation of the SSH key, you can use the following procedure to make a basic RSA SSH key to add to your credentials.

To create an SSH key manually

1. Open the command line for Linux or Terminal for macOS.
2. Enter `ssh-keyken` to create a 2048-bit SSH key or `ssh-keygen -b 4096` to create a 4096-bit SSH key, and then press **Enter**.

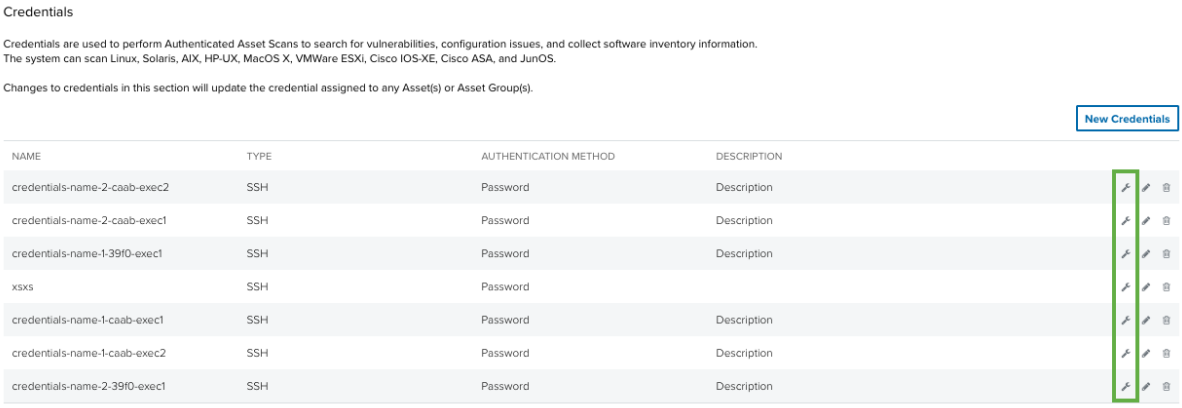
   The command line prompts you to specify a file location.
3. Press **Enter** to use the default location (`/home/<username>/.ssh/id_rsa` for Linux, or `/users/<username>/.ssh/id_rsa` for macOS), or designate another location for the file.

   The command line prompts you to specify a passphrase and enter it again to confirm it.
4. Specify a passphrase or, if you don't want to use a passphrase, leave the line blank, and then press **Enter**.
5. The SSH key is saved to either the default location or the location you specified.

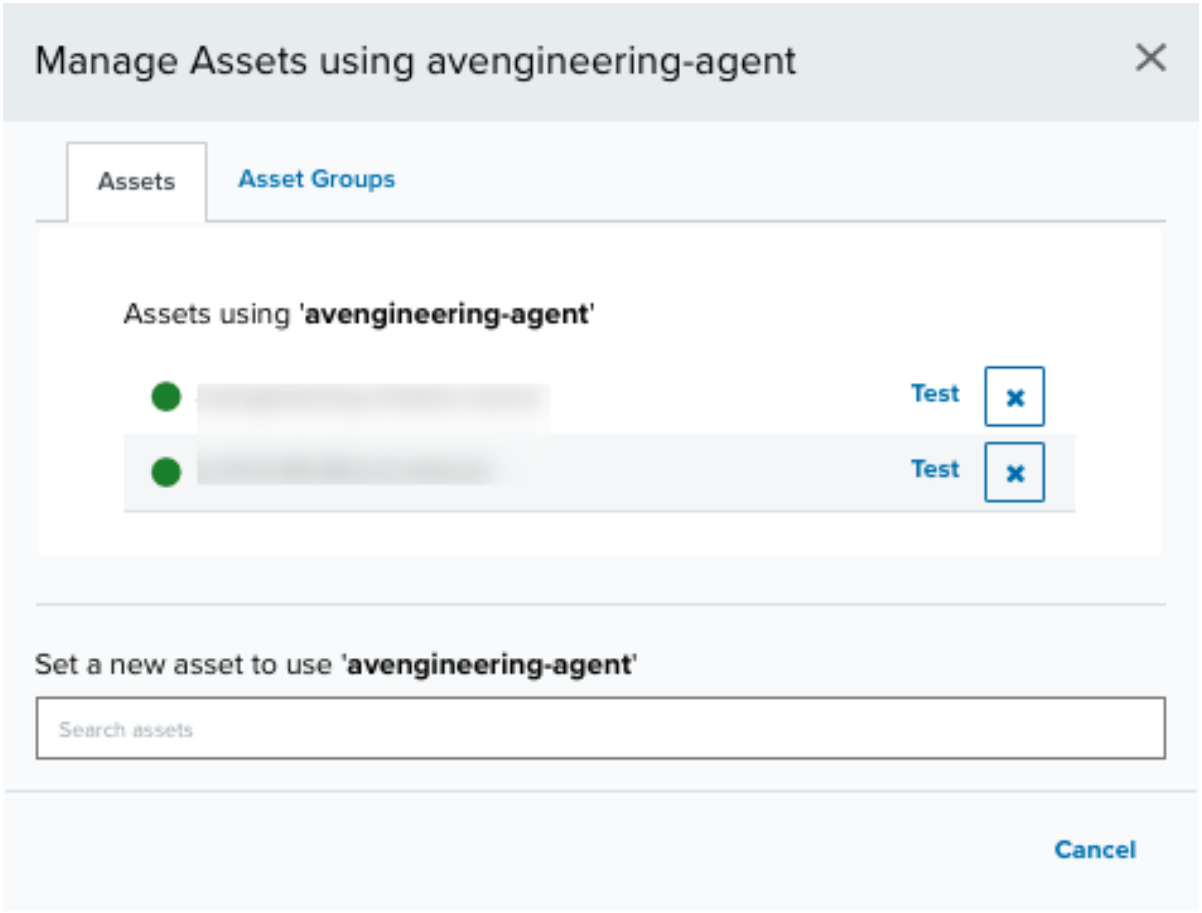
In USM Anywhere, you assign a defined credential set to an individual asset in order to use the credentials for authenticated scans, active directory (AD) scans, and BlueApp for Forensics and Response actions on the host. You can assign assets to a credential set in the Credentials page, or you can perform this task from the Assets page.

To assign a credential on the Credentials page

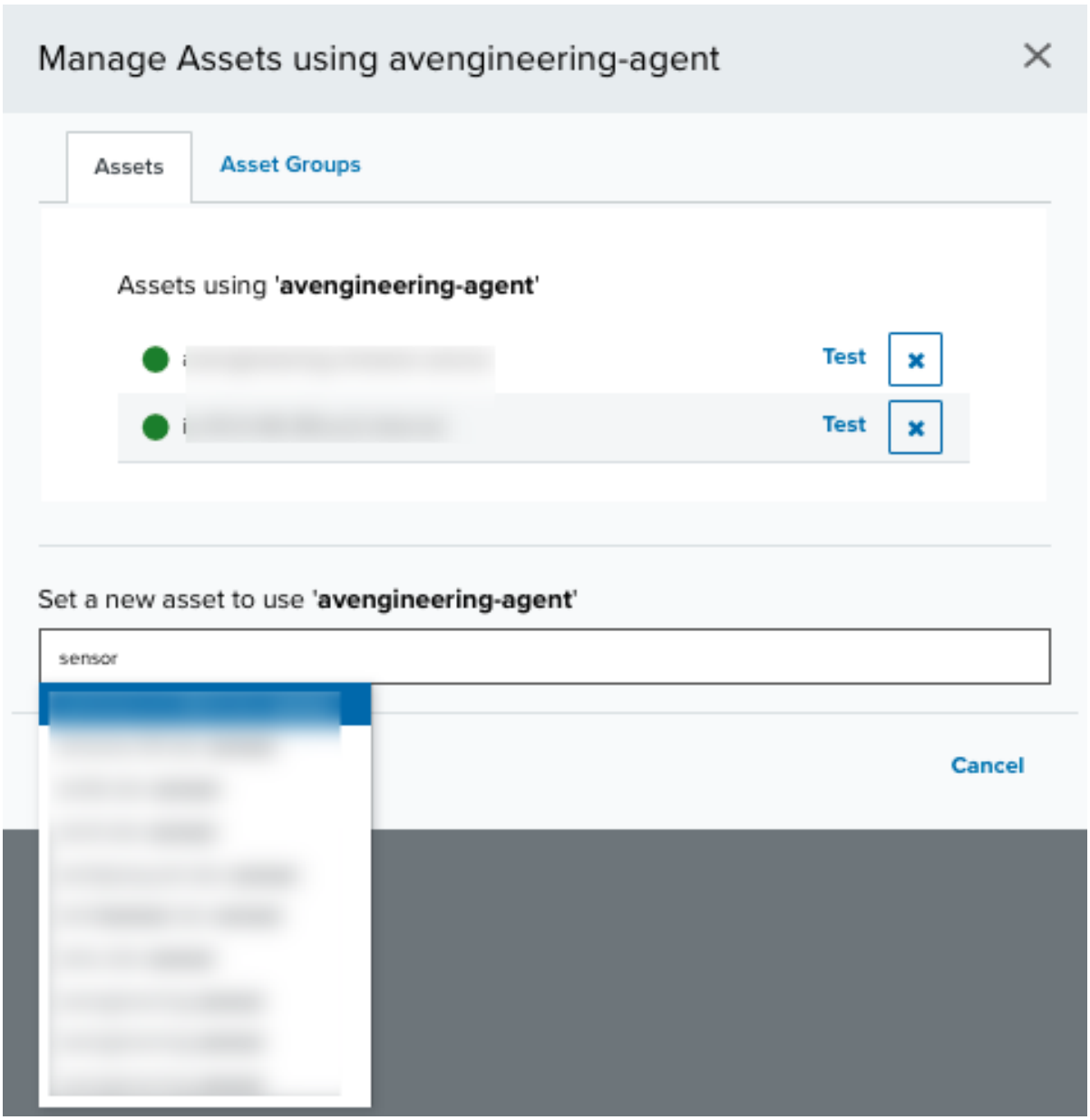
1. Go to **Settings > Credentials**.
2. In the line of the credential you want to assign, click the icon.



A dialog box opens.



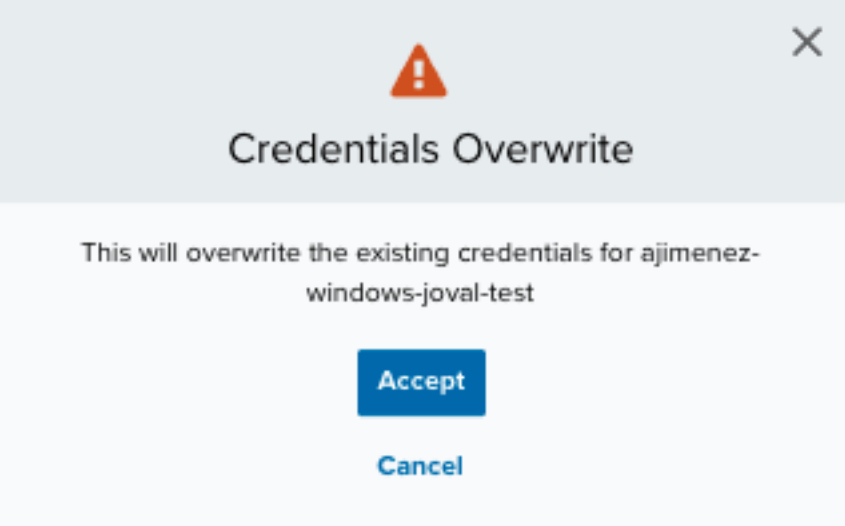
3. Enter part of the asset name in the field at the bottom of the dialog box



This displays the matching items below the field. You can enter more text to filter the list further.

4. Select the asset to assign to the credential set.

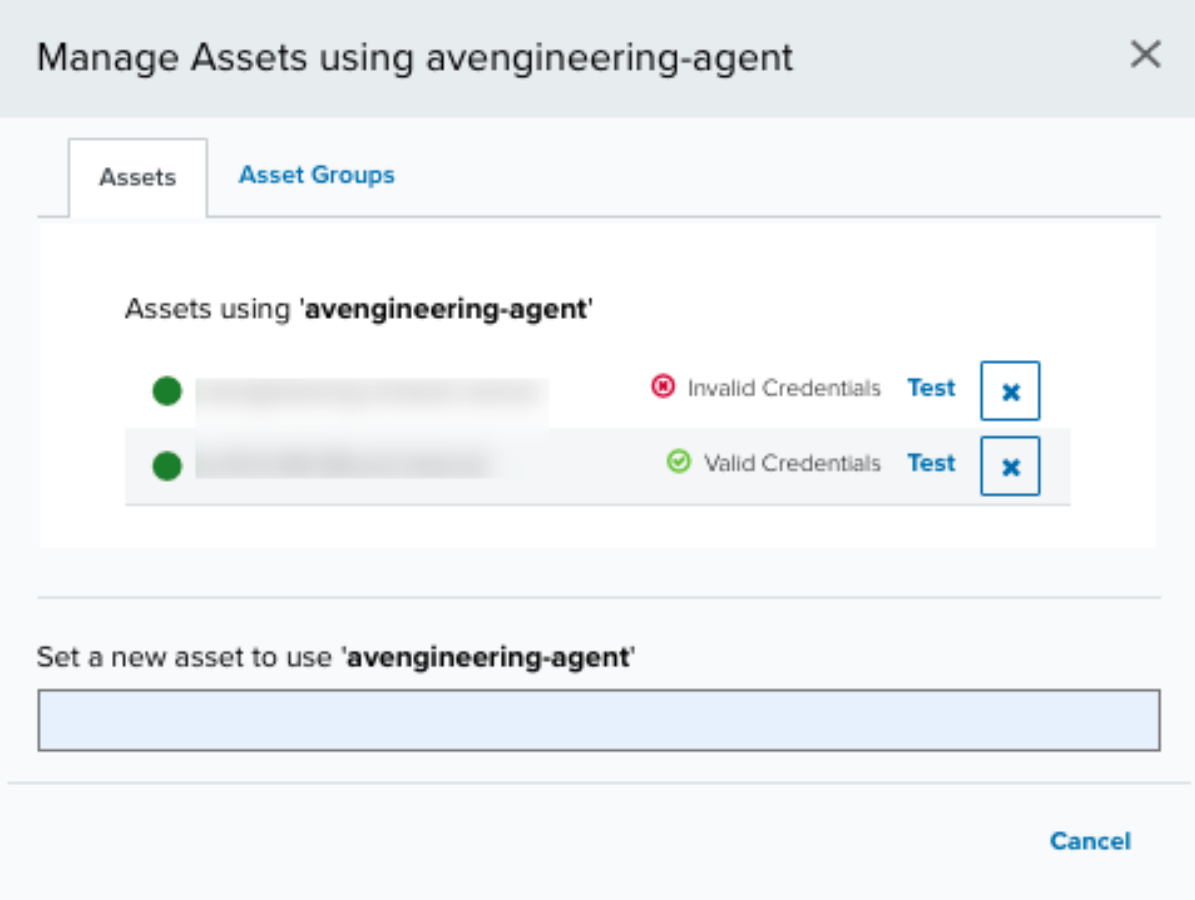
   The credentials overwrite dialog box opens.



Warning: If the asset has already assigned credentials, these credentials are going to be overwritten.

5. Next to the displayed asset name, click **Test** to execute a test connection to the asset using the credentials.

   If the test detects any warnings, a Permissions Warnings section displays. This section contains a Warning column that lists the individual warnings.



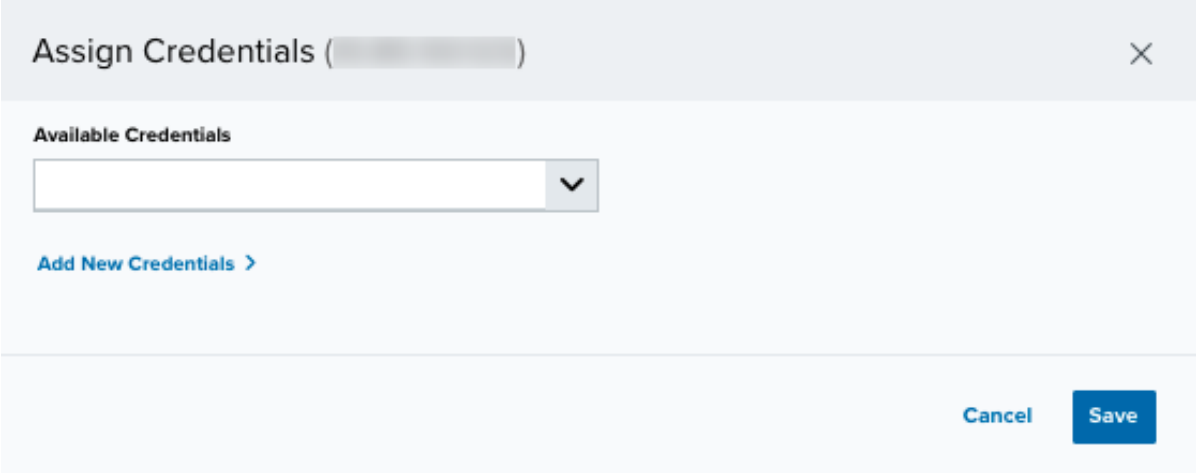
A permissions error doesn't prevent the scan from running, but it can result in the incomplete information being detailed in the scan results.

6. Click the ✕ icon to close the dialog box.

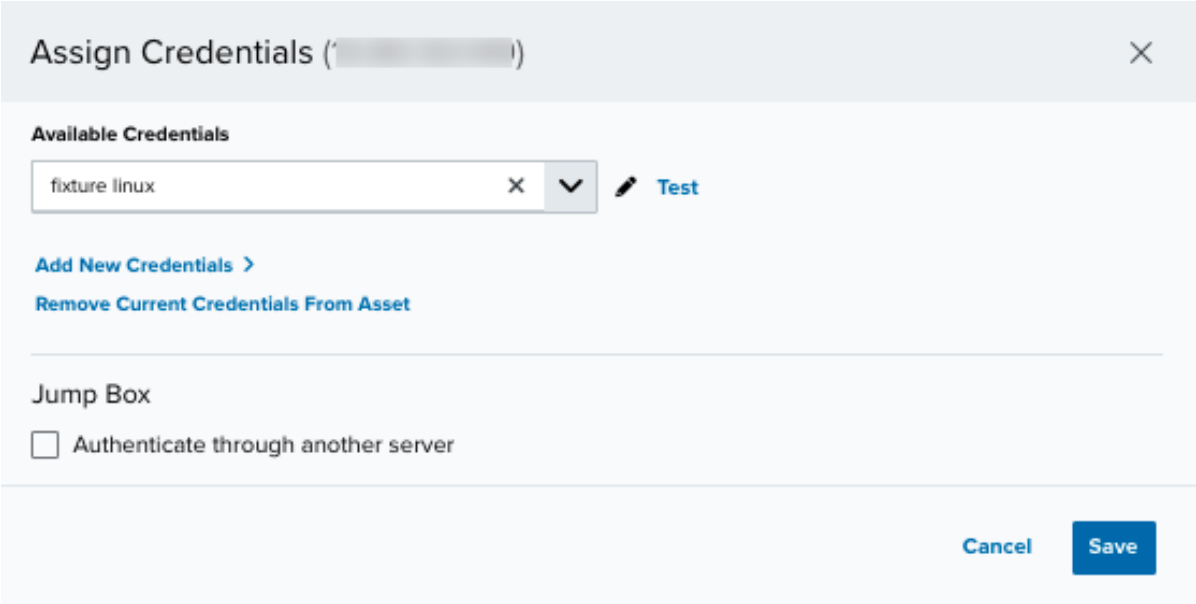
To assign a credential on the Assets page

1. Go to **Environment > Assets** and locate the asset.
2. Next to the asset name, click the ⌄ icon and select **Assign Credentials**.

   The assign credentials dialog box opens.



3. In the Available Credentials drop-down list, select the credential to use.



Note: If the needed credentials do not already exist, you can select **Add New Credentials** to define them in USM Anywhere. See Creating Credentials for more information. Use the icon to modify any information.

4. (Optional.) Select the **Jump Box** option if you want to authenticate through another asset.

   Select the checkbox and use the field to search for the asset you want to use as an authentication server.

5. Click **Test** to execute a test connection to the asset using the selected credentials.

   If the test detects any warnings, a Permissions Warnings section displays. This section contains a Warning column that lists the individual warnings and a Remediation that provides a suggested solution to resolve each warning. A permissions error doesn't prevent the scan from running, but it can result in the incomplete information being detailed in the scan results.

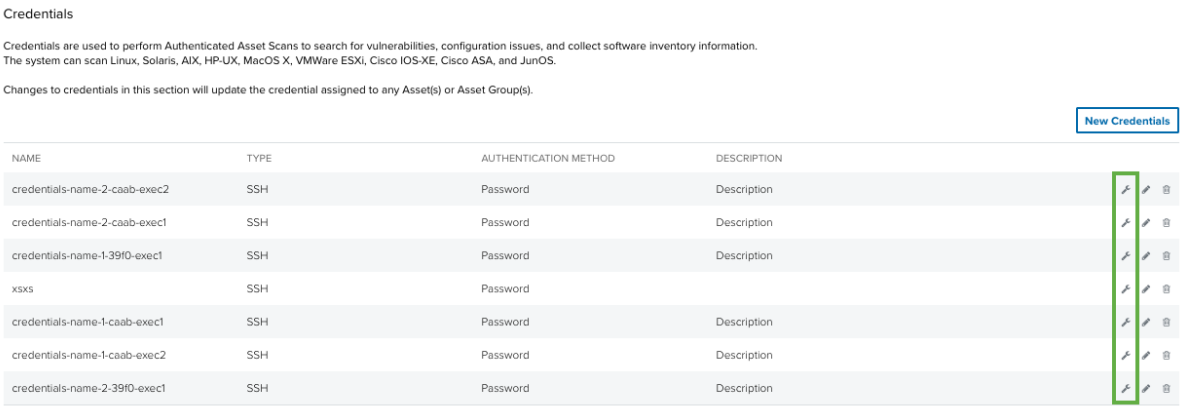
6. Click **Save**.

In USM Anywhere, you assign a defined credential set to an asset group to use the credentials for authenticated scans, AD scans, and BlueApp Forensics and Response actions on members of the group. You can assign asset groups to a credential set in the Credentials page, or you can perform this task from the Asset Groups page.

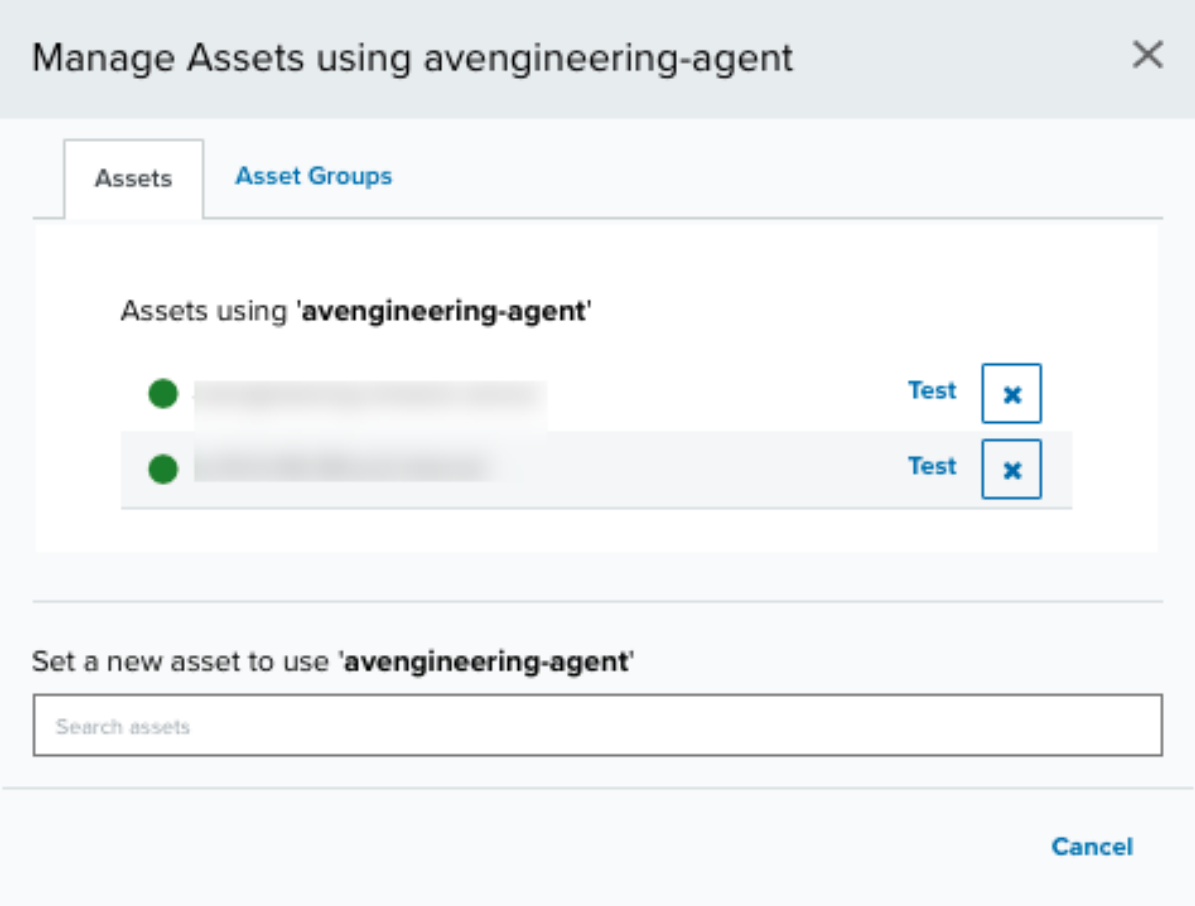
Important: When you assign a credential to an asset group, USM Anywhere assigns the credential to the asset group instead of assigning it to all of its members.

To assign a credential on the Credentials page

1. Go to **Settings > Credentials**.
2. In the line of the credential you want to assign, click the icon.

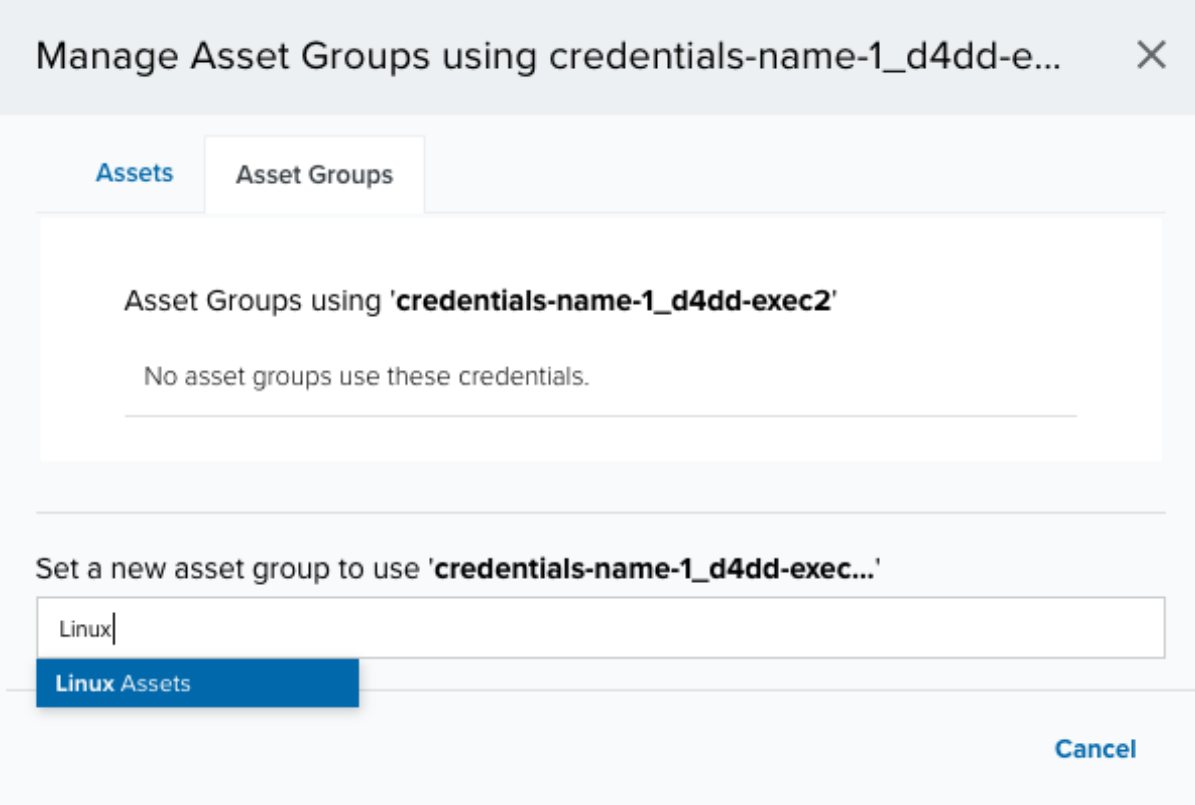


A dialog box opens.



3. Click the **Asset Groups** tab.
4. At the bottom of the dialog box, enter part of the asset group name in the field.

   This displays the matching items below the field. You can enter more text to filter the list further.
5. Select the asset group to assign to the credential set.



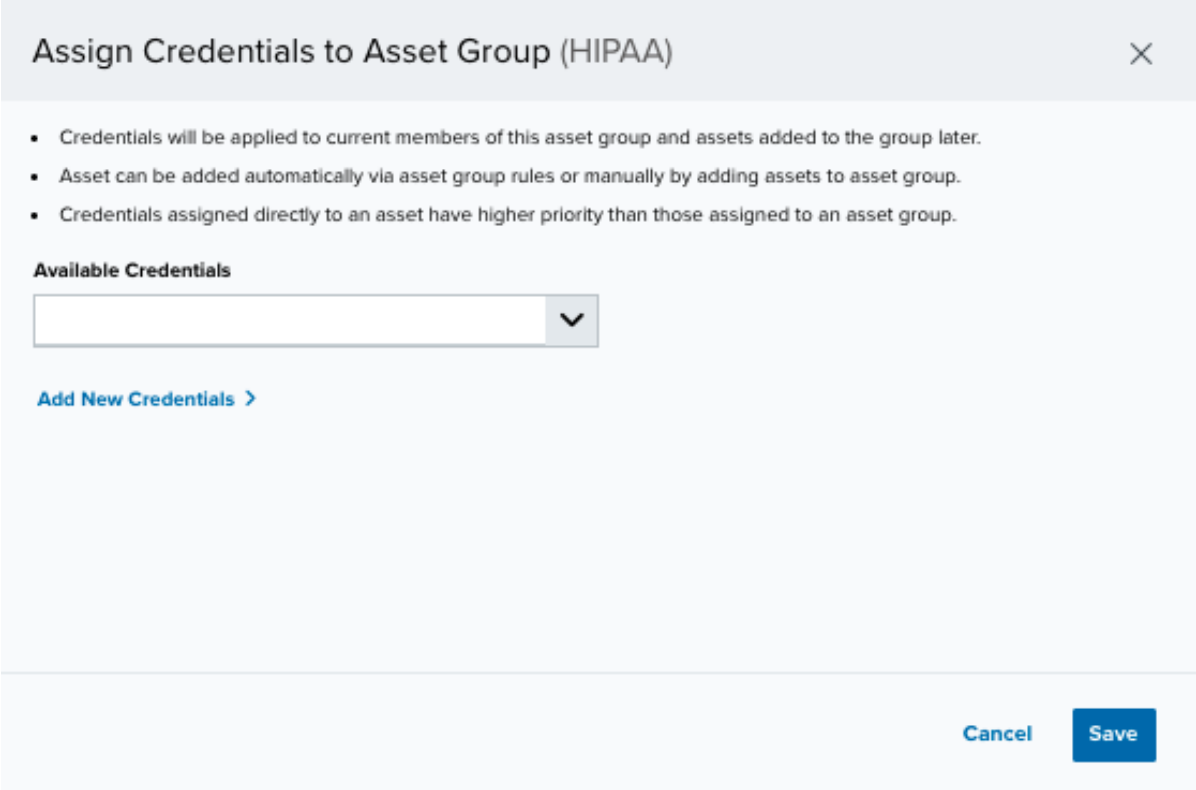
After you select the asset group, the dialog displays the item at the top. If needed, you can enter text for another asset group name and select it to assign multiple asset groups for the credential set.

6. Click the ✕ icon to close the dialog box.

To assign a credential on the Asset Groups page

1. Go to **Environment > Asset Groups**.
2. Next to the asset name, click the ⌄ icon and select **Assign Credentials**.

   The assign credentials dialog box opens.



3. In the Available Credentials drop-down list, select the credential to use.

> **Note:** If the needed credentials do not already exist, you can select **Add New Credentials** to define them in USM Anywhere. Use the icon to modify any information. Click **Remove Current Credentials From Asset Group** to remove that credential from the asset group.

4. Click **Save**.

Using the BlueApp for LevelBlue Forensics and Response Actions

With the BlueApp for LevelBlue Forensics and Response, USM Anywhere can execute system-level functions instantly — through a user-executed action or an automated rule or job — to coordinate forensics and response in a single action. Rather than manually connecting to each host and executing system-level tasks for investigation and protection purposes, you can use the BlueApp for LevelBlue Forensics and Response actions to gather forensic information or make system changes on assets monitored in USM Anywhere.

Important: Running the BlueApp for LevelBlue Forensics and Response actions requires that the target assets have assigned credentials that are suitable for administrative access to the host. See Configuring the BlueApp for LevelBlue Forensics and Response for more information.

Supported Actions

Each action that you run executes one or more functions on the host system for the target asset. Some of these functions collect system data and some perform enforcement operations. You can run an action manually from an event or alarm, or you can run an action from the BlueApp for LevelBlue Forensics and Response page for a specified asset. To automate these actions, you can schedule jobs to run an action for a specified asset, or you can create a response action rule to trigger an action from future events or alarms that meet your specified criteria.

See Data Collection Functions and Enforcement System Functions for detailed information about the functions supported by the BlueApp for LevelBlue Forensics and Response actions.

Forensic Profile Actions

The BlueApp for LevelBlue Forensics and Response provides multiple actions that you can use to perform an investigation of the target system, by running a group of data collection functions. Each of these actions is designed to provide a level of forensic profile for the target asset:

Basic Forensic Info Actions

Moderate Forensic Info Actions

Full Forensic Info Actions

USM Anywhere then generates an event for each executed function included in the forensic profile. See Viewing Forensics and Response Events and Alarms for more information about accessing these events.

Single Function Actions

For many of the most common functions, the BlueApp for LevelBlue Forensics and Response also provides actions to launch a simple execution of that function. The table below describes what each action does:

Action	Description	Availability
Disable Networking	Executes the Disable Networking enforcement function on the interfaces currently connected to the selected asset.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Get Active Directory Information	Executes the Get Active Directory (AD) Assets data collection function.	Scheduled Job
Get Established Connections	Executes the Get Established Connections data collection function. This displays information like the TCP State and Address Family. See the Microsoft documentation for more explanation on log fields.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule

Action	Description	Availability
Get Users	Executes the Get Users data collection function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Get Logged On Users	Executes the Get Logged On Users data collection function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Get Processes with Hashes	Executes the Get Processes with Hashes data collection function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Get Running Services	Executes the Get Running Services data collection function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Get System Info	Executes the Get System Info data collection function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule

Action	Description	Availability
Shutdown	Executes the Shutdown enforcement function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule
Set Registry Key to String	Executes the Set Registry Key to String enforcement function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Orchestration Rule
Set Registry Key to DWORD	Executes the Set Registry Key to DWORD enforcement function.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Orchestration Rule
Launch Query	Executes the specified data collection or enforcement function See Defining a Launch Query Action for more information regarding app actions.	BlueApp for LevelBlue Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule

Launch Actions from USM Anywhere

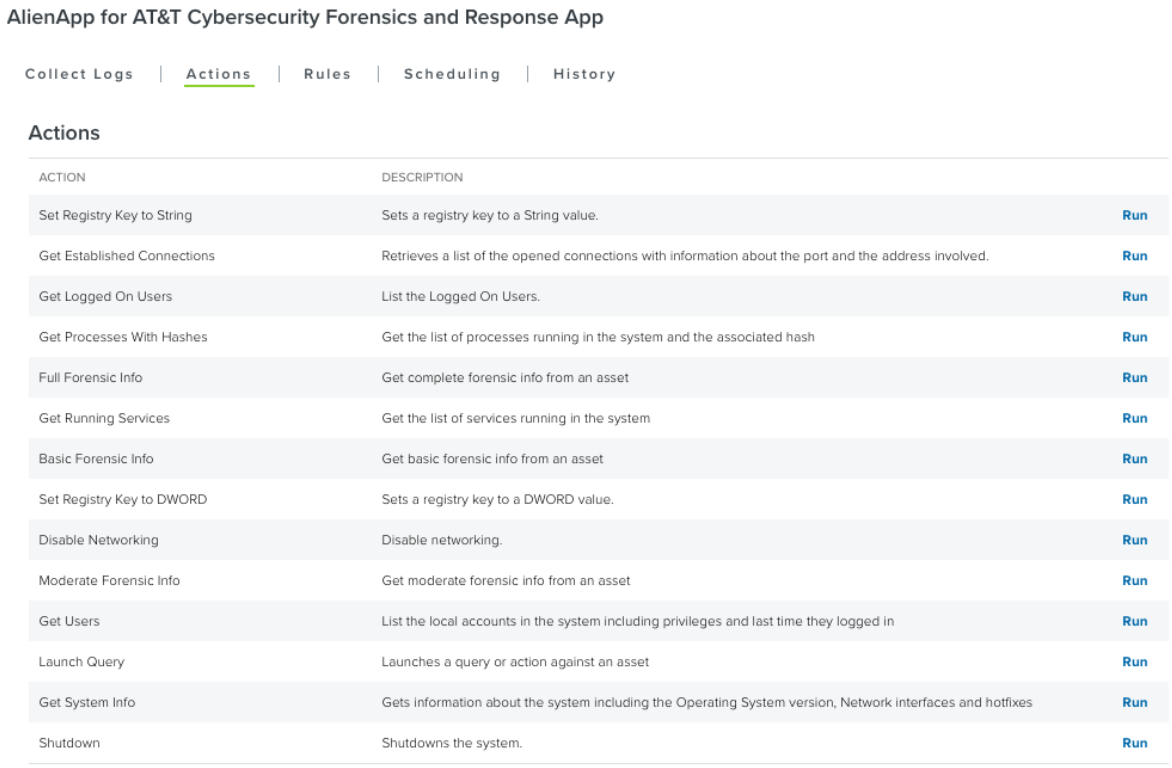
The BlueApp for LevelBlue Forensics and Response page provides an easy way to manually run a single Forensics and Response action. However, if it is an action that you want to run regularly for a specific asset, you should define a scheduled job to run the action. If you want to run the action as a response to certain events or alarms, you should define an orchestration rule.

To run an action in the BlueApp for LevelBlue Forensics and Response

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab.
5. Review the list of actions to determine which action you want to run.

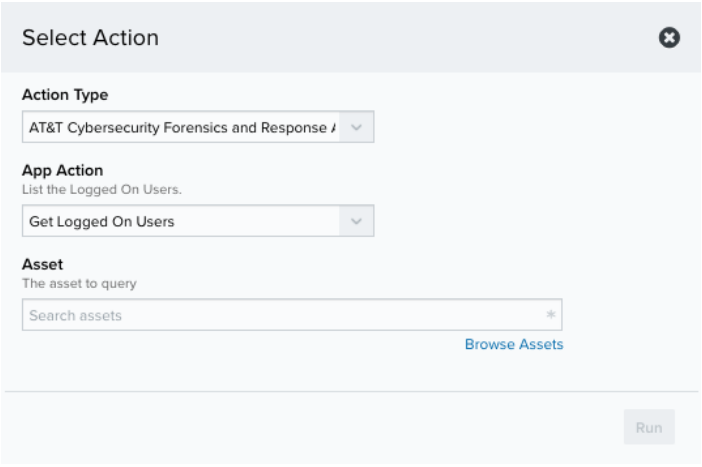
   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

   See Data Collection Functions and Enforcement System Functions topics for detailed information about each of the supported functions. If the needed function does not have a specific action, you can use the generic Launch Query action to specify the function parameters.
6. Next to the action that you want to use, click **Run**.



This opens the Select Action dialog box.

7. If needed, select the sensor on which the BlueApp is enabled to display more options.



8. Specify the asset that you want to use as a target for the action.

You can enter the name or IP address of the asset in the field to display matching items that you can select. Or you can click **Browse Assets** to open the Select Asset dialog box and browse the asset list to make your selection.

9. Click **Run**.

   USM Anywhere generates an event for each executed function. See Viewing Forensics and Response Events and Alarms for more information about accessing these events.

USM Anywhere will generate an event for each executed function included in this action's forensic profile.

Data Collection Functions

Use the data collection functions to collect forensic information from a remote Microsoft Windows or Linux machine and use it for your incident response processes. When you execute these collection functions, BlueApp for LevelBlue Forensics and Response retrieves and ingests data for analysis in USM Anywhere. It produces an event for each completed function and you can review the information on the Events page. See Viewing Forensics and Response Events and Alarms for more information about accessing these events.

Some of the most common functions are available as a singular query action. See the following table for details. For other functions, you can use the Launch Query action to specify the parameters and execute the function for an asset.

Important: These functions require that the target assets have assigned credentials that are suitable for system-level access to the host. See Configuring the BlueApp for LevelBlue Forensics and Response for more information.

System function	Collected data	Actions
Get System Info *Windows*	Information about the target system, including the operating system version, network interfaces, and hotfixes. To execute this function using the Launch Query action, specify `getSystemInfo` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info
Get Users *Windows and Linux*	A list of the local accounts in the target system, including privileges and the last login time. To execute this function using the Launch Query action, specify `getUsers` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info Get Users
Get Running Services *Windows and Linux (non-RHEL)*	A list of all currently running services on the target system. To execute this function using the Launch Query action, specify `getRunningServices` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info Get Running Services
Get Running Services RedHat *Linux (RHEL only)*	A list of all currently running services on the target system. To execute this function using the Launch Query action, specify `getRunningServices.rhel` as the Query parameter.	
Get Services *Windows*	A list of all services on the target system. To execute this function using the Launch Query action, specify `getServices` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get SMB Sessions *Windows*	Information about the Server Message Block (SMB) sessions that are currently established on the target system. To execute this function using the Launch Query action, specify `getSMBSessions` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info

System function	Collected data	Actions
Get TCP Listening Ports *Windows and Linux*	A list of the listening TCP ports on the target system. To execute this function using the Launch Query action, specify `getTCPListeningPorts` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info
Get UDP Listening Ports *Windows and Linux*	A list of the listening UDP ports on the target system. To execute this function using the Launch Query action, specify `getUDPListeningPorts` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info
Get Established Connections *Windows and Linux*	A list of the opened connections on the target system, including information about the port and the address. To execute this function using the Launch Query action, specify `getEstablishedConnections` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info Get Established Connections
Get Installed Applications *Windows*	A list of the applications installed on the target system. To execute this function using the Launch Query action, specify `getInstalledApplications` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info
Get Logged On Users *Windows*	A list of the user accounts that are currently logged in to the target system. To execute this function using the Launch Query action, specify `getLoggedOnUsers` as the Query parameter.	Basic Forensic Info Moderate Forensic Info Full Forensic Info Get Logged On Users

System function	Collected data	Actions
Get Network Configuration *Windows*	A list of the active network interfaces on the target system and their properties, including IP addresses and DHCP information. To execute this function using the Launch Query action, specify `getNetConfig` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Antivirus *Windows*	Information about antivirus tools installed on the target system, including the status. To execute this function using the Launch Query action, specify `getAntivirus` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Start Up Items *Windows*	An enumerated list of autorun artifacts on the target system that may be used by legitimate programs or malware to achieve persistence. To execute this function using the Launch Query action, specify `getStartUpItems` as the Query parameter.	Moderate Forensic Info
Get All Start Up Items *Windows*	A complete, enumerated list of autorun artifacts on the target system that may be used by legitimate programs or malware to achieve persistence. To execute this function using the Launch Query action, specify `getStartUpItemsAll` as the Query parameter.	Full Forensic Info
Get Processes *Windows and Linux*	A list of processes running on the target system. To execute this function using the Launch Query action, specify `getProcesses` as the Query parameter.	Basic Forensic Info

System function	Collected data	Actions
Get Processes With Hashes *Windows*	A list of processes running on the target system, along with the associated hash. To execute this function using the Launch Query action, specify `getProcessesWithHashes` as the Query parameter.	Moderate Forensic Info Full Forensic Info Get Processes With Hashes
Get Shares *Windows*	A list of the shared folders on the target system. To execute this function using the Launch Query action, specify `getShares` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Mapped Drives *Windows*	A list of the mapped drives on the target system. To execute this function using the Launch Query action, specify `getMappedDrives` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Scheduled Tasks *Windows and Linux*	A list of the scheduled tasks on the target system (malware often creates scheduled tasks to maintain persistence). To execute this function using the Launch Query action, specify `getScheduledTasks` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Scheduled Jobs *Windows*	A list of the scheduled jobs on the target system (malware often creates scheduled jobs to maintain persistence). To execute this function using the Launch Query action, specify `getScheduledJobs` as the Query parameter.	Moderate Forensic Info Full Forensic Info

System function	Collected data	Actions
Get Installed Hotfixes *Windows*	A list of the hotfixes installed on the target system. To execute this function using the Launch Query action, specify `getInstalledHotfixes` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Recent USB Drives *Windows*	A list of the USB devices recently used on the target system. To execute this function using the Launch Query action, specify `getRecentUSBDrives` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Shadow Copies *Windows*	A list of shadow copies on the target system. Shadow copies are used to perform manual or automatic backup copies or snapshots of computer files or volumes. To execute this function using the Launch Query action, specify `getShadowCopies` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Restore Points *Windows*	A list of the restore points available on the target system. To execute this function using the Launch Query action, specify `getRestorePoints` as the Query parameter.	Moderate Forensic Info Full Forensic Info

System function	Collected data	Actions
Get Prefetch Files *Windows*	A list of the prefetch files on the target system. Windows creates a prefetch file when an application runs from a particular location for the very first time. To execute this function using the Launch Query action, specify `getPrefetchFiles` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get DNS Cache *Windows*	A list of the contents of the DNS client cache on the target system. To execute this function using the Launch Query action, specify `getDNSCache` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Failed DNS *Windows*	A list of the 50 most recent DNS resolutions that failed on the target system. To execute this function using the Launch Query action, specify `getFailedDNS` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get EventLog Info *Windows*	A list of all the event log sources on the target system, including the size and last modification time. To execute this function using the Launch Query action, specify `getEventLogInfo` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Firewall Config *Windows*	The firewall configuration on the target system. To execute this function using the Launch Query action, specify `getFirewallConfig` as the Query parameter.	Moderate Forensic Info Full Forensic Info

System function	Collected data	Actions
Get Audit Policy *Windows*	The local audit policy information on the target system. To execute this function using the Launch Query action, specify `getAuditPolicy` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get IE History *Windows*	The history from Internet Explorer on the target system, including a list of recently visited web sites. To execute this function using the Launch Query action, specify `getIEHistory` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Typed URLs *Windows*	A list of the most recent URLs typed by the user in Internet Explorer on the target system. To execute this function using the Launch Query action, specify `getTypedURLs` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Event Tracing for Windows (ETW) Sessions *Windows*	A list of the running Microsoft Event Tracing for Windows (ETW) sessions on the target system. To execute this function using the Launch Query action, specify `getETWSessions` as the Query parameter.	Moderate Forensic Info Full Forensic Info
Get Windows Defender Information *Windows*	Information about Windows Defender on the target system. To execute this function using the Launch Query action, specify `getWindowsDefenderStatus` as the Query parameter.	Moderate Forensic Info Full Forensic Info

System function	Collected data	Actions
Get Drivers *Windows*	A list of drivers on the target system, including the location, hash, and digital signature. To execute this function using the Launch Query action, specify `getDrivers` as the Query parameter.	Full Forensic Info
Get Recently Created Files *Windows*	A list of files created on the target system within the last 24 hours. To execute this function using the Launch Query action, specify `getRecentlyCreatedFiles` as the Query parameter.	Full Forensic Info
Get Recent DLLs *Windows*	A list of DLLs created on the target system within the last 24 hours. To execute this function using the Launch Query action, specify `getRecentDLLs` as the Query parameter.	Full Forensic Info
Get Recent Links *Windows*	A list of the link files created on the target system within the last seven days. To execute this function using the Launch Query action, specify `getRecentLinks` as the Query parameter.	Full Forensic Info
Get Recent Executables *Windows*	A list of executable files created on the target system within the last 24 hours. To execute this function using the Launch Query action, specify `getRecentExecutables` as the Query parameter.	Full Forensic Info

System function	Collected data	Actions
Get Compressed Files *Windows*	A list of the compressed files created on the target system within the last seven days. To execute this function using the Launch Query action, specify `getCompressedFiles` as the Query parameter.	Full Forensic Info
Get Encrypted Files *Windows*	A list of the encrypted files created on the target system within the last seven days. To execute this function using the Launch Query action, specify `getEncryptedFiles` as the Query parameter.	Full Forensic Info
Get Downloads *Windows*	A list of the downloaded files created on the target system. To execute this function using the Launch Query action, specify `getDownloads` as the Query parameter.	Full Forensic Info
Get Windows Defender Detections *Windows*	Information about malware threats on the target system detected by Windows Defender. To execute this function using the Launch Query action, specify `getWindowsDefenderDetections` as the Query parameter.	Full Forensic Info

Enforcement System Functions

Use the enforcement functions to mitigate an incident or contain a threat, such as malware, on a remote Microsoft Windows system. You can trigger actions that execute these functions directly from an event or alarm, and easily create a rule to execute the function for similar events or alarms that occur in the future. You can also create a scheduled job to execute one or more functions for a specific asset, such as performing a system restart at the same time each day.

Important: These functions are supported only for Windows hosts in your USM Anywhere asset inventory.

Target assets must have assigned credentials that are suitable for system-level access to the host. See Configuring the BlueApp for LevelBlue Forensics and Response for more information.

Set Registry Key to String

Use this function to set or update a registry key to a standard string (REG_SZ) value on a Windows target system.

You can run this function using the Set Registry Key to String action from the BlueApp for LevelBlue Forensics and Response page or as an action from an orchestration rule. Set the parameters according to the registry key and value.

Path: Enter the path for the registry key. For example, `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion`.

Name: Enter the name of the registry key. For example, `MyKey`.

Value: Enter the new value for the key as a standard string format. For example, `New-Key-Value`.

Set Registry Key to DWORD

Use this function to set or update a registry key to a 32-bit integer string (REG_DWORD) value on a Windows target system.

You can run this function using the Set Registry Key to DWORD action from the BlueApp for LevelBlue Forensics and Response page or as an action from an orchestration rule. Set the parameters according to the registry key and value.

Path: Enter the path for the registry key. For example, `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion`.

Name: Enter the name of the registry key. For example, `MyVersionKey`.

Value: Enter the new value for the key as a standard string format. For example, `108`.

Disable Networking

Use this function to disable all the network interfaces on a Windows target system. This is typically executed to isolate a system that has been compromised or is infected with malware.

You can run this function using the Disable Networking action from the BlueApp for LevelBlue Forensics and Response page, from the Alarm or Event details, or as an action from an orchestration rule or scheduled job. You specify the asset for the function and no parameters are required.

Shutdown

Use this function to shut down a Windows target system. This is a typical response action in situations where a system is compromised and must be shut down in order to stop further damage.

You can run this function using the Shutdown action from the BlueApp for LevelBlue Forensics and Response page, from the Alarm or Event details, or as an action from an orchestration rule or scheduled job. You specify the asset for the function and no parameters are required.

Stop Process

Use this function to stop a process on a Windows target system using the process identification (ID). This function returns information about the terminated process and USM Anywhere displays this as an event.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `stopProcess` as the value.

First Optional Parameter: Enter the name for the process to be stopped. For example, `TermService`. If needed, you can determine this value by executing a Get Processes function.

Disable Local User

Use this function to disable a local user account on a Windows target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `disableLocalUser` as the value.

First Optional Parameter: Enter the name of the user account to be disabled. For example, `TempUser`. If needed, you can determine this value by executing a Get Users function.

Disable AD User

Use this function to disable an Active Directory user account on a Windows target system that is configured as an AD domain controller.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `disableADUser` as the value.

First Optional Parameter: Enter the name of the AD user account to be disabled. For example, `TempUser`. If needed, you can determine this value by executing a Get AD Users function.

Stop Service

Use this function to stop a service on the target system using the service name and retrieve information about stopped service.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `stopService` as the value.

First Optional Parameter: Enter the name of the service to be stopped. If needed, you can determine this value by executing a Get Running Services data collection function.

Restart Service

Use this function to restart a service on the target system using the service name.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `restartService` as the value.

First Optional Parameter: Enter the name of the service to be stopped. If needed, you can determine this value by executing a Get Running Services data collection function.

Send Message

Use this function to send messages to a user connected to the target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `sendMessage` as the value.

First Optional Parameter: Enter the username account. A value of * sends a message to all connected users.

Second Optional Parameter: Enter the message text.

Block Remote Address Outbound

Use this function to create a new rule in the Windows firewall to block outbound connections to a specified address. This is useful to block a command and control when a system has been compromised.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `blockRemoteAddressOutbound` as the value.

First Optional Parameter: Enter the remote IP address to be blocked.

Block Remote Address Inbound

Use this function to create a new rule in the Windows firewall to block inbound connections from a specified address. This is useful to block the source of an attacker that is launching a brute force, denial of service (DoS), or other attack.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `blockRemoteAddressInbound` as the value.

First Optional Parameter: Enter the remote IP address to be blocked.

Block Inbound Port

Use this function to create a new rule in the Windows firewall to block inbound connections to a specific port.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `blockInboundPort` as the value.

First Optional Parameter: Enter the port number to be blocked.

Restart

Use this function to restart the target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `restart` as the value.

Shutdown

Use this function to shut down the target system.

You can run this function using the Shutdown action from the BlueApp for LevelBlue Forensics and Response page, from the Alarm or Event details, or as an action from an orchestration rule or scheduled job. You specify the asset for the function and no parameters are required.

Restore

Use this function to restore the target system to the specified restore point.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `restore` as the value.

First Optional Parameter: Enter the ID for the restore point. If needed, you can determine this value by executing a Get Restore Points data collection function.

Enable Windows EventLog Channel

Use this function to enable a Windows EventLog channel on the target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `enableLogChannel` as the value.

Disable Windows EventLog Channel

Use this function to disable a Windows EventLog channel on the target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `disableLogChannel` as the value.

Launch a Windows Defender Scan

Use this function to launch a Windows Defender scan on the target system.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `launchWindowsDefenderScan` as the value.

First Optional Parameter: Enter the scan type. This value can be `QuickScan`, `FullScan`, or `CustomScan`.

Second Optional Parameter: If you specify the CustomScan type, enter the path to scan (for example, `C:\Directory`).

Update Windows Defender Signatures

Use this function to update the Windows Defender signatures on the target system from the Microsoft update server.

You can run this function through the Launch Query action. Set these parameters for the Launch Query app action:

Query: Enter `updateWindowsDefenderSignatures` as the value.

Defining a Launch Query Action

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

The BlueApp for LevelBlue Forensics and Response supports an extensive list of system-level functions that you can execute on a host system. Many of the most common data collection functions are included in the forensic profile actions or as standalone actions. You can also use the Launch Query action to specify any of the supported functions and any needed parameters for the function.

You can use the Launch Query action when you need to perform one of the following tasks:

- Create a scheduled Forensics and Response job
- Launch a Forensics and Response action from an alarm or event
- Create a Forensics and Response orchestration rule
- Run an action from the BlueApp for LevelBlue Forensics and Response page

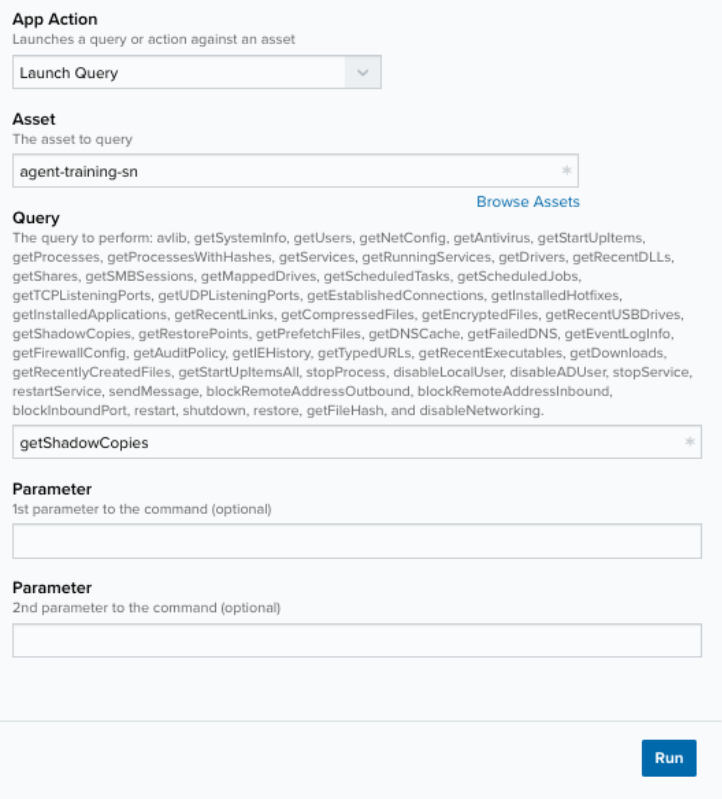
See the information in Data Collection Functions and Enforcement System Functions to determine the query syntax and parameters for the function you want to run using the Launch Query action.

To define a query for the BlueApp for LevelBlue Forensics and Response

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab.
5. Locate the Launch Query action and click **Run**.

   This opens the Select Action dialog box.
6. If needed, select the sensor on which the BlueApp is enabled to display more options.
7. Specify the asset that you want to use as a target for the action.

   You can enter the name or IP address of the asset in the field to display matching items that you can select. Or you can click **Browse Assets** to open the Select Asset dialog box and browse the asset list to make your selection.
8. In the Query field, enter the function to perform.



9. (Optional.) If the function requires parameters, use the Parameter fields to enter the values in order.

Scheduling a Forensics and Response Job

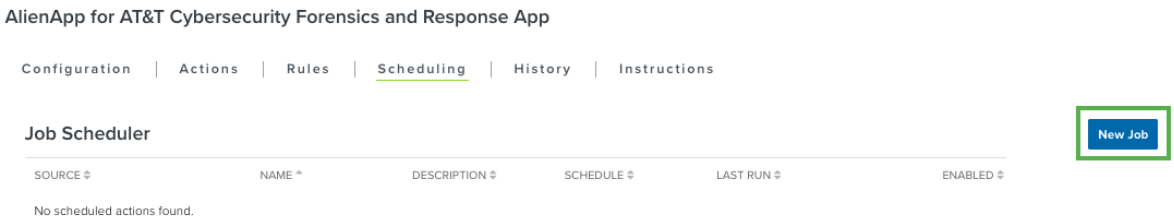
Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

The BlueApp for LevelBlue Forensics and Response provides easy access to define a scheduler job to retrieve your Microsoft Windows or Linux system data. You can also create a scheduler job to execute system-level enforcement functions on Windows hosts, such as Shutdown, Restart, and Stop Process. Review the information in Supported Actions to determine the action that you want to use for your scheduled job.

After you create the new job, you can make changes to the parameters for the scheduled job or review its history in the Scheduler page. See USM Anywhere Scheduler in the *USM Anywhere User Guide* for more information about working with scheduled jobs.

To schedule a Forensics and Response job

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Scheduling** tab.
5. On the right side of the page, click **New Job**.

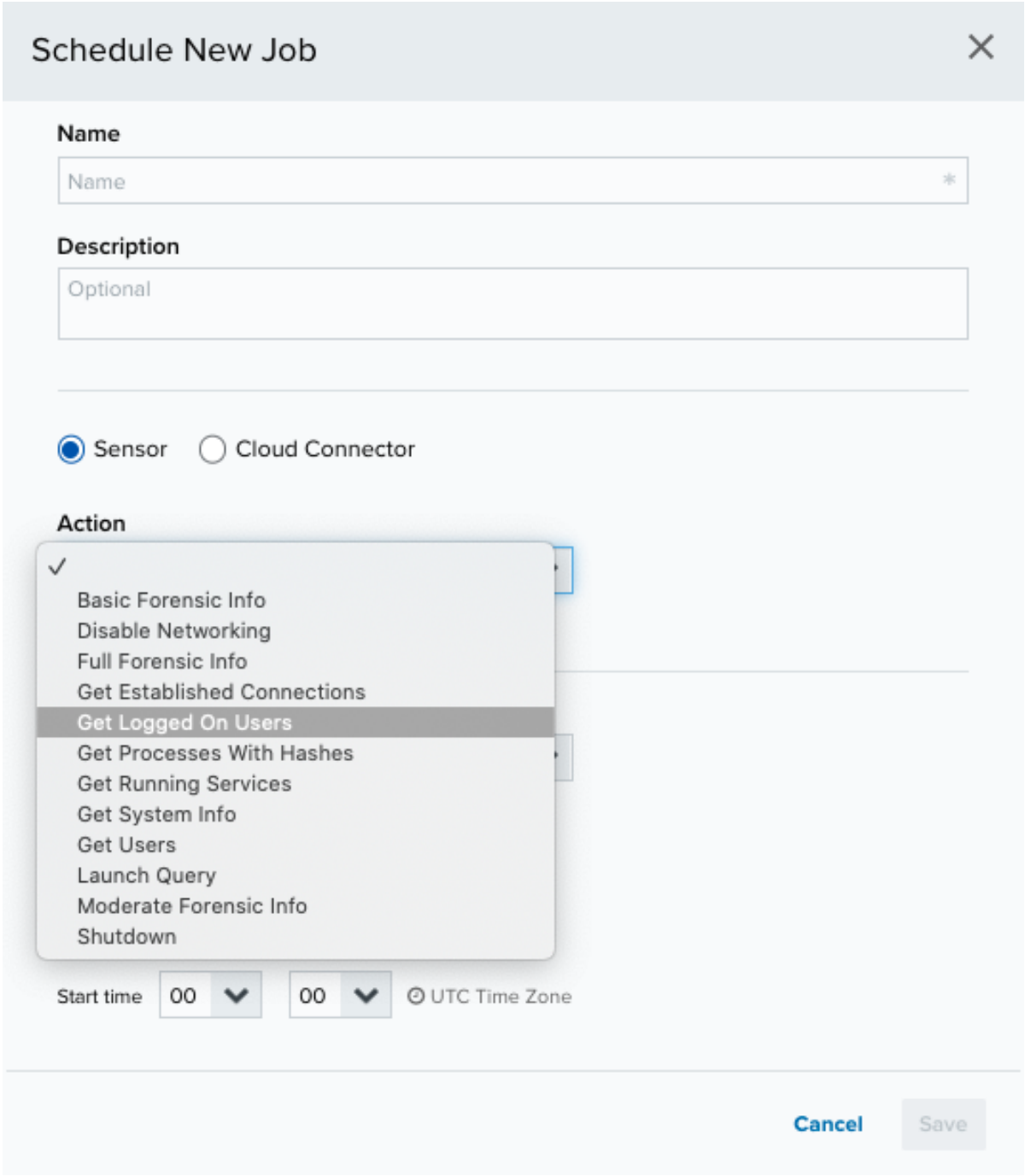


   This opens the Schedule New Job dialog box.

6. Enter the name and description for the job.

   The description is optional, but it is a best practice to provide this information so that others can easily understand what it does.

7. Select **Sensor** as the source for your new job.
8. Click the **Action** drop-down and select the command you want to run.



9. Specify the asset that you want to use as a target for the action.

   You can enter the name or IP address of the asset in the field to display matching items that you can select. Or you can click **Browse Assets** to open the Select Asset dialog box and browse the asset list to make your selection.

10. (Optional.) Set the required parameters.

    Some enforcement actions take one or more parameters in order to execute to system function on the target system. See Enforcement System Functions if you need more information about these parameters for a specific function.

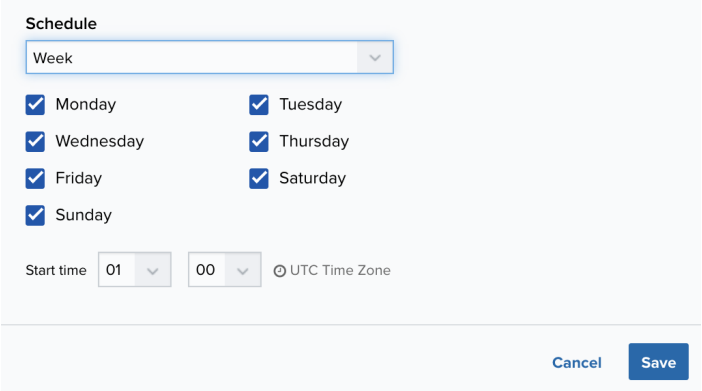
11. In the Schedule section, specify when USM Anywhere runs the job:

    a. Select the increment as **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

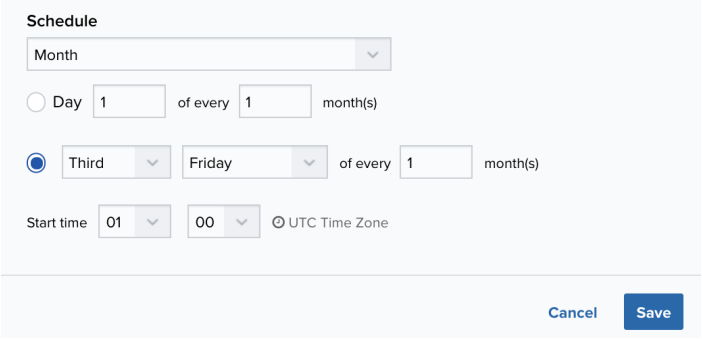
    > **Warning:** After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See USM Anywhere System Monitor for more information.

    b. Set the interval options for the increment.

    The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.



Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.



> **Important:** USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

c. Set the start time.

   This is the time that the job starts at the specified interval. It uses the time zone configured for your USM Anywhere instance (the default is Coordinated Universal Time [UTC]).

12. Click **Save**.

Launching a Forensics and Response Action from an Event or Alarm

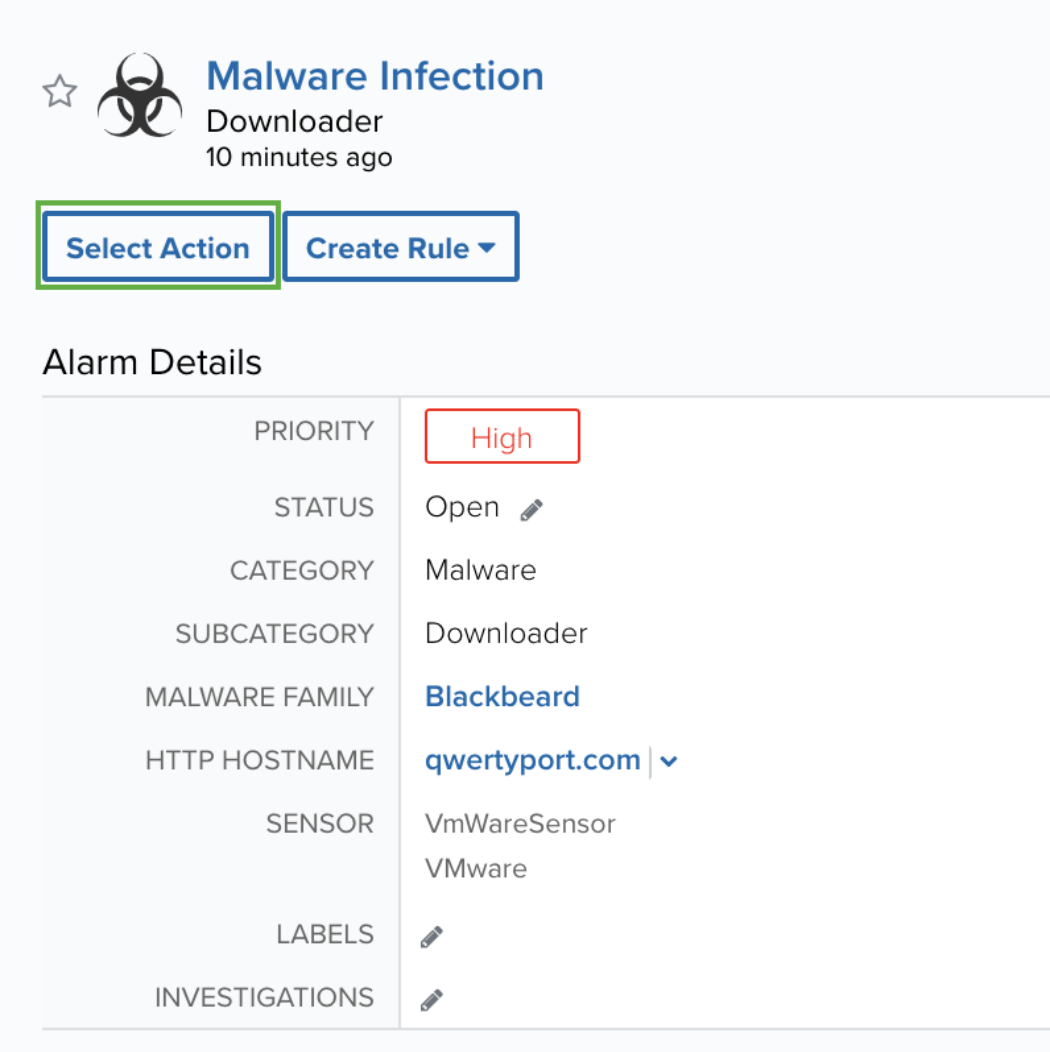
Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

When you review the information in the Alarm Details or Event Details, you can easily launch a Forensics and Response action. If you want to apply the action to similar items that occur in the future, you can also create an orchestration rule directly from the executed action.

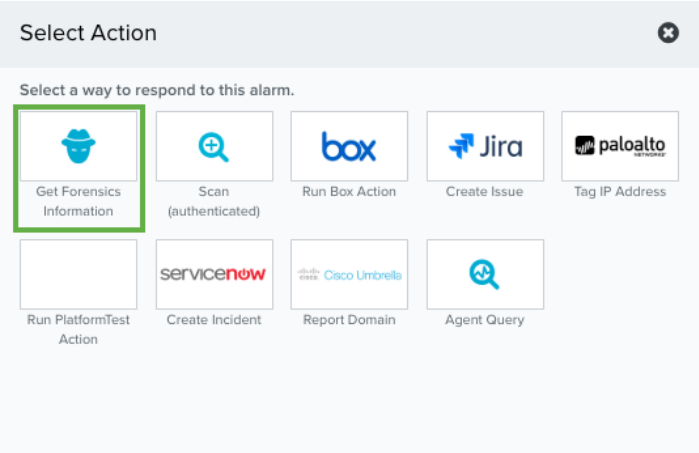
Review the information in Supported Actions to determine the action that you want to launch.

To launch a Forensics and Response action from an alarm or event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.

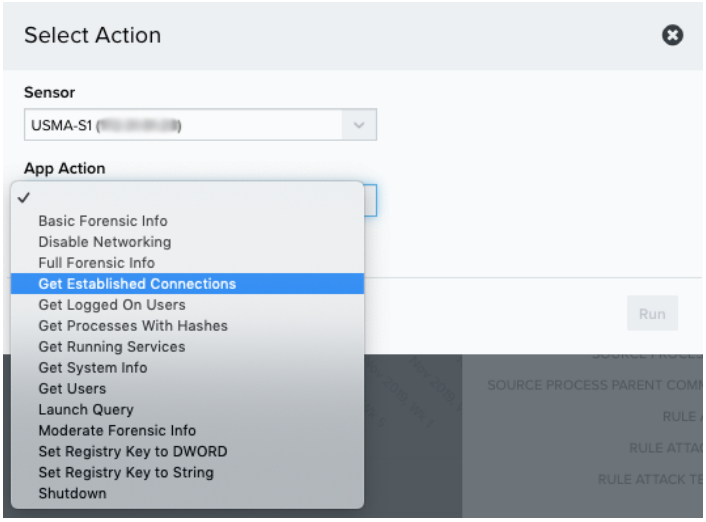


4. In the Select Action dialog box, select the **Get Forensics Information** tile.



This displays the options for the selected action type.

5. If you have more than one deployed USM Anywhere Sensor, select the sensor associated with the asset that you want to use as the target for the action.
6. Click the App Action list and select the action you want to run for the asset.

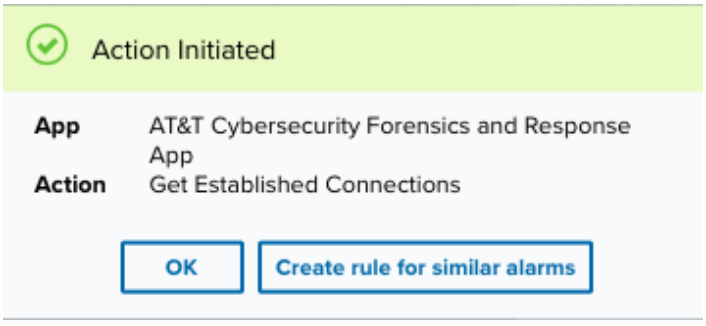


7. Specify the asset that you want to use as a target for the action.

   You can enter the name or IP address of the asset in the field to display matching items that you can select. Or you can click **Browse Assets** to open the Select Asset dialog box and browse the asset list to make your selection.

8. Click **Run**.

   After USM Anywhere initiates the action, it displays a confirmation dialog box.



   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating a Forensics and Response Rule

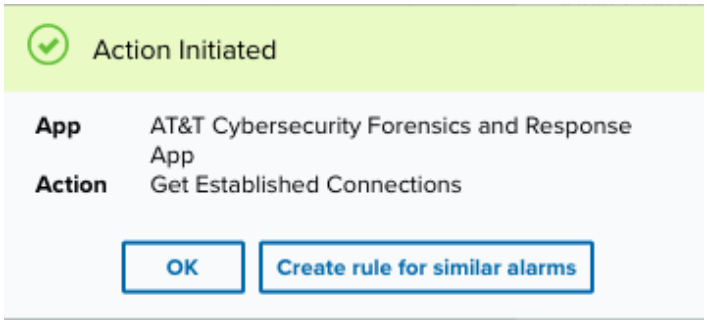
Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

The BlueApp for LevelBlue Forensics and Response enables you to create orchestration rules that automatically run a data collection or enforcement action in response to future events or alarms that meet your criteria. You can define the rule to run the action on the associated source asset, associated destination asset, or any asset you specify.

All rules include a rule name and conditional expression. They can also include optional multiple occurrence and window length parameters. There are two methods for creating a new BlueApp for LevelBlue Forensics and Response orchestration rule in USM Anywhere.

- **From an Applied Action**: You can automatically create a rule using the action that you apply from an existing alarm or event. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

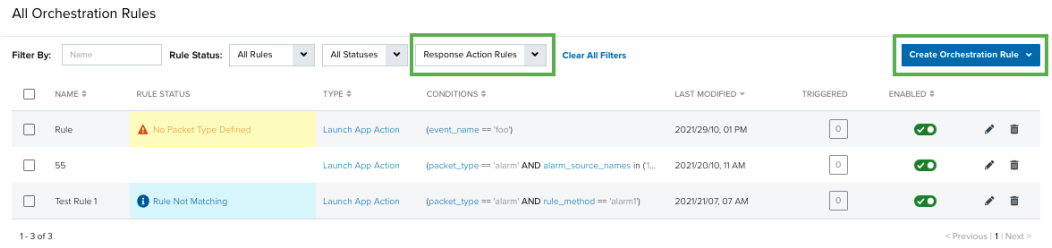
  In the confirmation dialog box, click **Create rule for similar alarms** or **Create rule for similar events**.



- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click

Create Orchestration Rule > Response Action Rule to define the new rule.



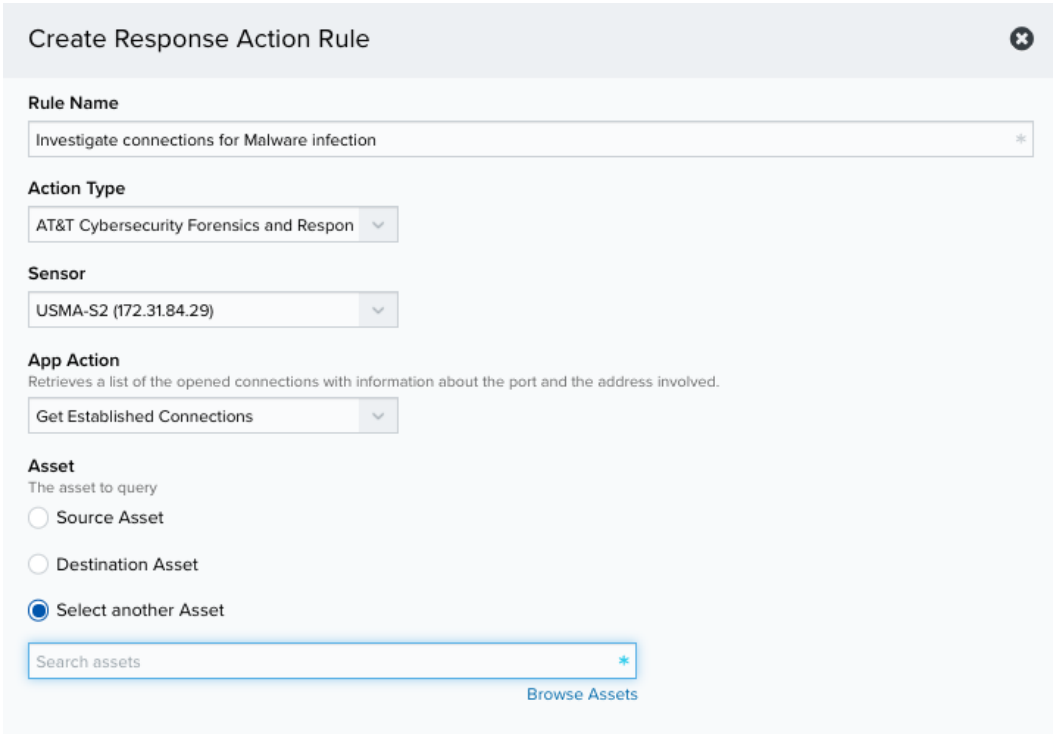
Both of these methods display the Create Response Action Rule dialog box. Use this to specify the new rule, including the Forensics and Response action to run and the criteria for a future event or alarm that triggers the rule.

To define a Forensics and Response rule

1. Enter a unique name for the rule.
2. Select the Action for the rule.

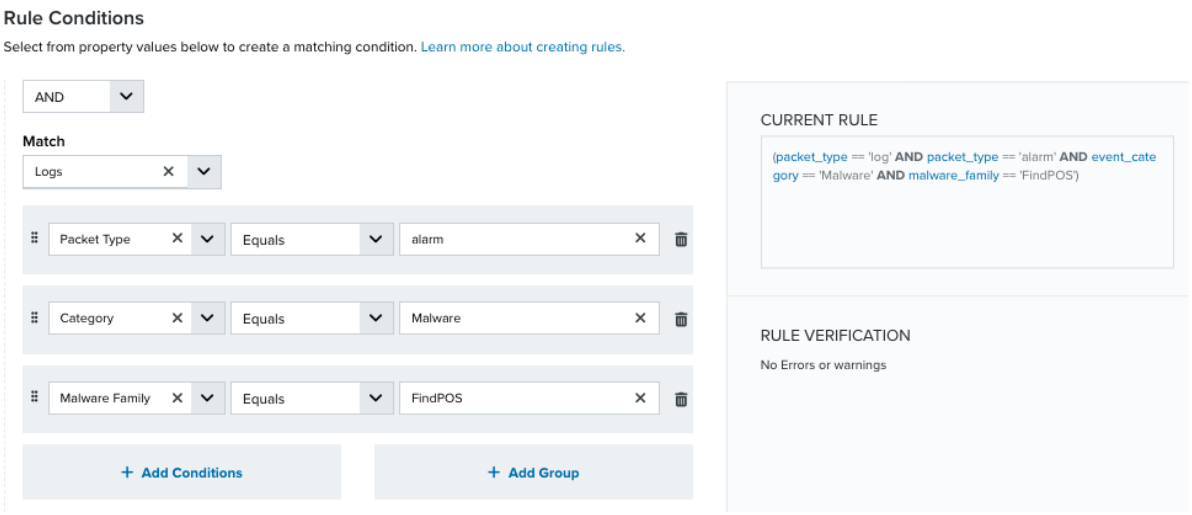
   Review the information in Supported Actions to determine the action that you want to use for the rule.

3. Select the target Asset for the action.



- **Source Asset**: Use this option to use the source endpoint of the alarm or event as the target asset.
- **Destination Asset**: Use this option to use the destination endpoint of the alarm or event as the target asset.
- **Select another Asset**: Use this option to specify the asset that is always the target for the action when the rule is triggered. Use the search text box or click **Browse Assets** to locate and select the asset.

4. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

5. Click **Save Rule**.
6. Click **OK** in the confirmation dialog box.

Viewing Forensics and Response Events and Alarms

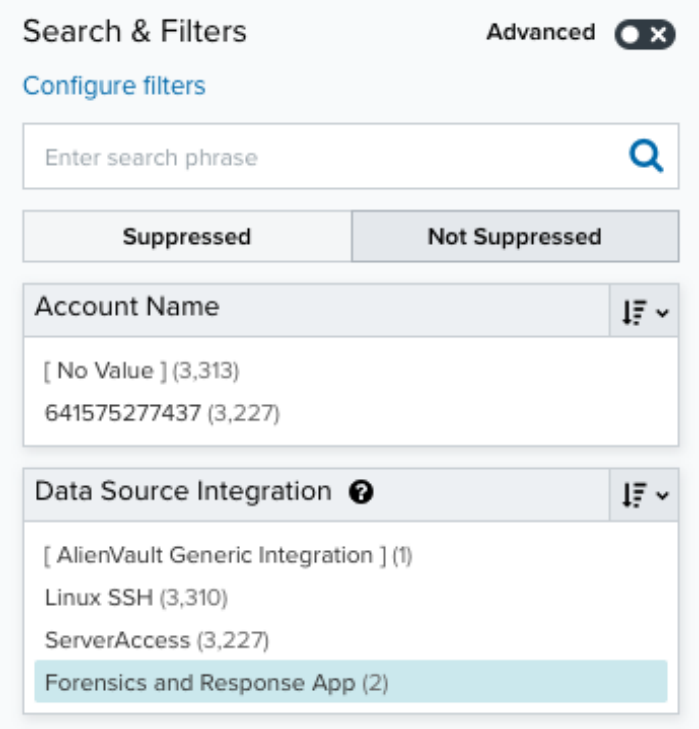
Role Availability	Read-Only	Investigator	Analyst	Manager

The BlueApp for LevelBlue Forensics and Response translates the data it retrieves into normalized events for analysis. After you enable this BlueApp, events are displayed in the Events page, where you can view information about the collected forensic information. These events can trigger alarms to alert your team about a system compromise.

To view BlueApp for LevelBlue Forensics and Response events

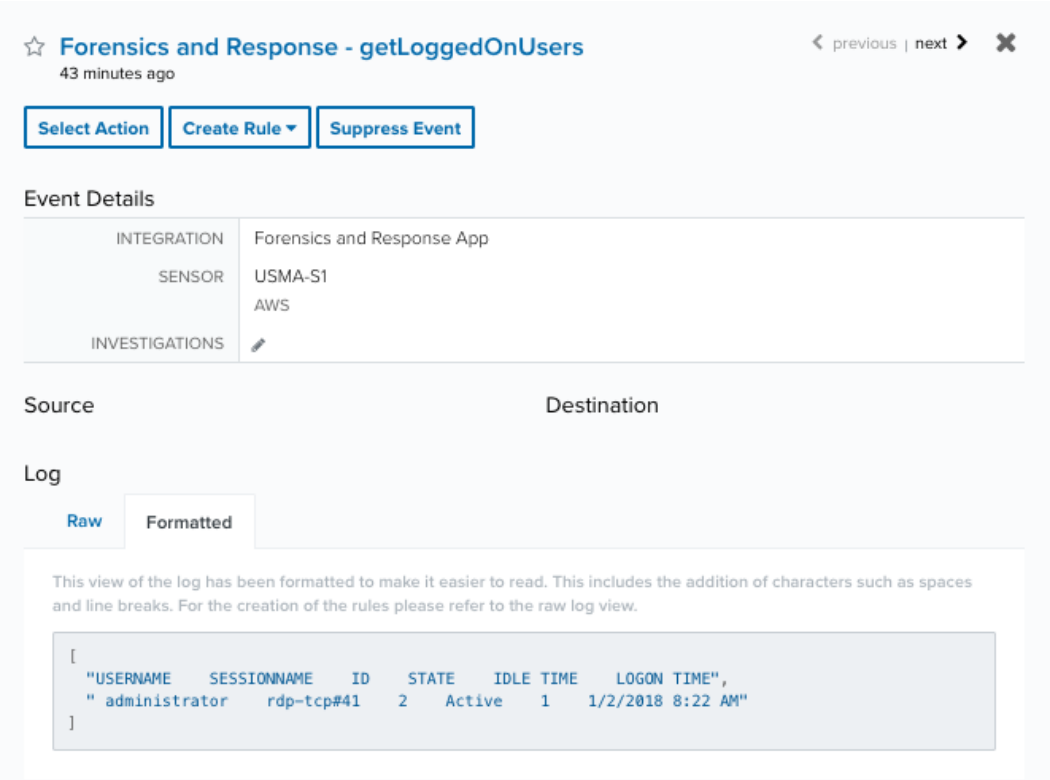
1. Select **Activity > Events** to open the events page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

   USM Anywhere includes several filters displayed by default.
3. Scroll down to the Data Source filter and select **LevelBlue Forensics and Response App** to display only those events on the page.

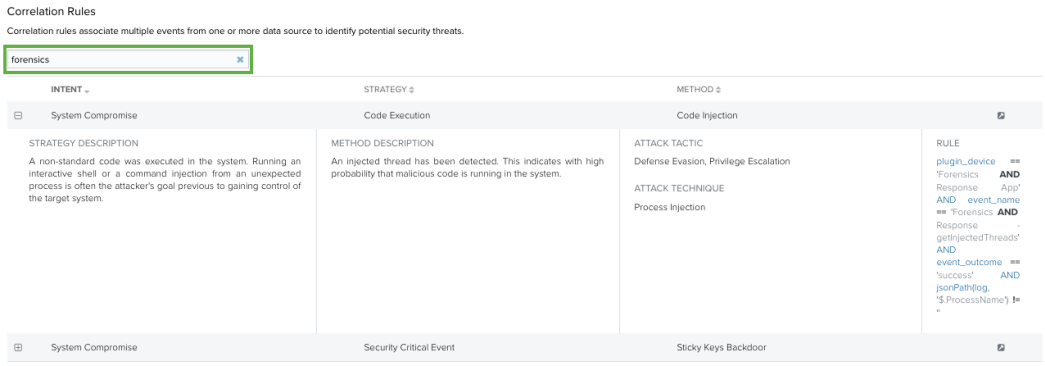


If this filter is not displayed, click the **Configure filters** link, which is in the upper left corner of the page, to configure filters for the page. See Managing Filters in the *USM Anywhere User Guide* for more information about configuring filters for pages.

4. Select an event in the list to view detailed information.



USM Anywhere includes built-in correlation rules that generate an alarm from one or more of these events. These rules analyze the events for patterns that indicate a code injection or Sticky Keys compromise for an asset. You can view the specifics of these rules on the Correlation Rules page by entering `forensics` in the Search field.



If you want to generate an alarm for other types of Forensics and Response events, you can create your own custom alarm rules and define the matching conditions to fit your criteria.

BlueApp for LevelBlue Secure Remote Gateway

The BlueApp for LevelBlue Secure Remote Gateway, powered by Zscaler, enables you to use Zscaler's Internet gateway tools to block IPs and URLs in response to threats detected in USM Anywhere. When an alarm, event, or rule is triggered, the BlueApp for LevelBlue Secure Remote Gateway can add the source or destination address to your denylist.

Edition: The BlueApp for LevelBlue Secure Remote Gateway is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for LevelBlue Secure Remote Gateway

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

Before BlueApp for LevelBlue Secure Remote Gateway, powered by Zscaler, can connect to USM Anywhere, you need to submit a Move, Add, Change, Delete (MACD) Request through the BusinessDirect Web Portal.

To acquire LevelBlue Secure Remote Gateway details

1. Log in to the AT&T BusinessDirect Web Portal using your BusinessDirect ID and password.
2. Request an admin account with the Client-BlueApp role.

   Specify the account name and email address you want to associate with the role.
3. Once the MACD request is approved, you can view your login and password in the AT&T

BusinessDirect Web Portal.

Use the details provided to access the Zscaler portal and obtain the base URI and API key to finish configuration in USM Anywhere.

To acquire Zscaler configuration details

1. Log in to the Zscaler admin page using your Zscaler credentials.
2. Go to **Administration > API Key Management**.

   The page displays the base Uniform Resource Identifier (URI) and API key.
3. Copy the base URI and key value to your clipboard or a secure location. You will need to enter them in USM Anywhere to configure the AlienApp.

To connect the LevelBlue Secure Remote Gateway API to USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the information you collected previously:
   - Base URI
   - Username
   - Password (provided from the BusinessDirect Web Portal MACD request)
   - Zscaler API Key
7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Zscaler APIs, a  icon displays in the Health column.

If the ⊗ icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Zscaler connection.

BlueApp for LevelBlue Secure Remote Gateway Actions

The BlueApp for LevelBlue Secure Remote Gateway, powered by Zscaler, provides a set of orchestration actions that you can use to identify and categorize items to block as a response to threats identified by USM Anywhere

As USM Anywhere surfaces events, vulnerabilities, and alarms, your team determines which items require a response action. Rather than manually tagging threats, you can use the BlueApp for LevelBlue Secure Remote Gateway orchestration actions to enforce protection based on the information associated with the event or alarm.

Actions for the BlueApp for LevelBlue Secure Remote Gateway

Action	Description
Add to Blocked List	Add a source or destination to the Zscaler blocked list.
Add to Allowed List	Add a source or destination to the Zscaler allowed list.
Remove from Allowed List	Remove a source or destination from the Zscaler blocked list.
Add to Custom Category	Add a source or destination to a Zscaler category. Typing a category will bring up autocomplete suggestions of existing categories. When selecting this action, the Select Action window will also display two additional links at the bottom on the window. Click the **Search for existing categories** link to see if the IP address is currently associated with any categories. Click the **URL Lookup** link to obtain further information about the IP address such as the type of address and whether or not Zscaler has any registered security alerts associated with it.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

To launch an LevelBlue Secure Remote Gateway orchestration action for an alarm

1. Go to **Activity > Alarms** or **Acitvity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **LevelBlue Secure Remote Gateway** tile.
5. For the App Action, select the action you want to launch.

   You can launch an action to add or remove an IP address to the allowed list, add an IP address to the blocked list, or add the IP address to a custom category.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Enter the name of the category you want the IP added to, if applicable.
7. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating AT&T Secure Web Gateway Response Action Rules

Role Availability	Read-Only	Investigator	Analyst	Manager

The BlueApp for LevelBlue Secure Remote Gateway, powered by Zscaler, has unique response actions which enable you to quickly respond to threats identified by USM Anywhere. You can create response action rules in USM Anywhere that automatically trigger when alarms or events match the criteria that you specify.

After you create a rule, new events or alarms that match the rule will trigger the AT&T Secure Web Gateway action to tag to the associated source or the destination host. The rule does **not** trigger for your existing alarms or events.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

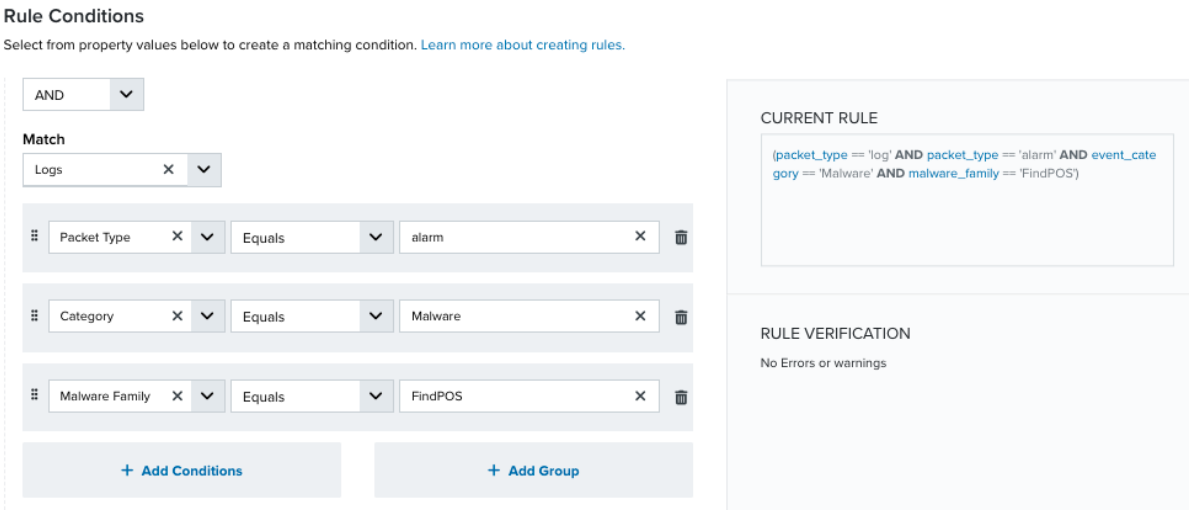
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new AT&T Secure Web Gateway response action rule

1. Enter a name for the rule.
2. Select the action you want to launch from the **Action** dropdown menu.

   You can launch an action to tag the destination host or source for an alarm or an event.

3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. Click **OK** in the confirmation dialog box.

BlueApp for Box

The BlueApp for Box provides deep security monitoring for your Box activities, helping you safeguard content management and file sharing through early threat detection and rapid response. It enhances the threat detection capabilities of USM Anywhere by collecting and analyzing data from your Box Enterprise account. After successfully configured, the BlueApp for Box does the following:

- The BlueApp for Box queries the Box API every 20 minutes for information, such as authentication events, user account updates, malware and ransomware infections, application and file activities, and Box platform changes. USM Anywhere then parses the data and displays them as events in the user interface (UI).
- The out-of-the-box correlation rules for Box events, provided by the BlueApp for Box, enable USM Anywhere to automatically create alarms, notifying you about suspicious activity in your Box environment.
- USM Anywhere includes a predefined dashboard that provides an overview of Box activity so that you have quick visibility to streamline your investigation and incident response processes.
- The BlueApp for Box also provides advanced security orchestration to launch or automate user-initiated actions against threats detected in your Box environment.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Box

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

Connected through the Box application programming interface (API), the BlueApp for Box uses a predefined scheduler job to collect information from Box every 20 minutes, such as authentication events, user profile updates, user state changes, application and group assignment, and Box platform changes. After USM Anywhere collects and analyzes the first of these events, you can view them in **Activity > Events** and the Box dashboard.

Important: You must have access to your Box Enterprise account for configuring the integration with the BlueApp for Box. The USM Anywhere Sensor you want to use for the BlueApp for Box must have outbound connectivity to api.box.com on port 443.

To enable the BlueApp to connect to the Box API

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. Click the **Instructions** tab.
5. Follow the instructions on the page to obtain the Enterprise ID from Box. This step is better conducted in a different browser.
6. Click the **Configuration** tab.
7. Click **Configure API**.
8. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
9. In the Box Enterprise ID field, paste the value obtained from Box.
10. Click **Save**.
11. Verify the connection.

    After USM Anywhere completes a successful connection to the Box APIs, a icon displays in the Health column.

    If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Box connection.
12. In the USM Anywhere main menu, go to **Settings > Scheduler** and search for the collection job for Box.
13. Enable the job if it is not already enabled.

    Important: The BlueApp will not work if the scheduler job is not enabled.

    When this job runs for the first time after the connection, it collects Box events from the previous 24 hours. On subsequent runs (every 20 minutes), it only collects new events since the last check.

BlueApp for Box Orchestration

With the collection of your Box Enterprise account activities through the configured BlueApp for Box, USM Anywhere collects, enriches, and analyzes data from your Box environment. It detects any suspicious activity, such as anomalous user behavior, credential abuse, or brute-force authentications. When USM Anywhere detects a threat, it generates an alarm. See the following table for examples of alarms that the BlueApp may produce.

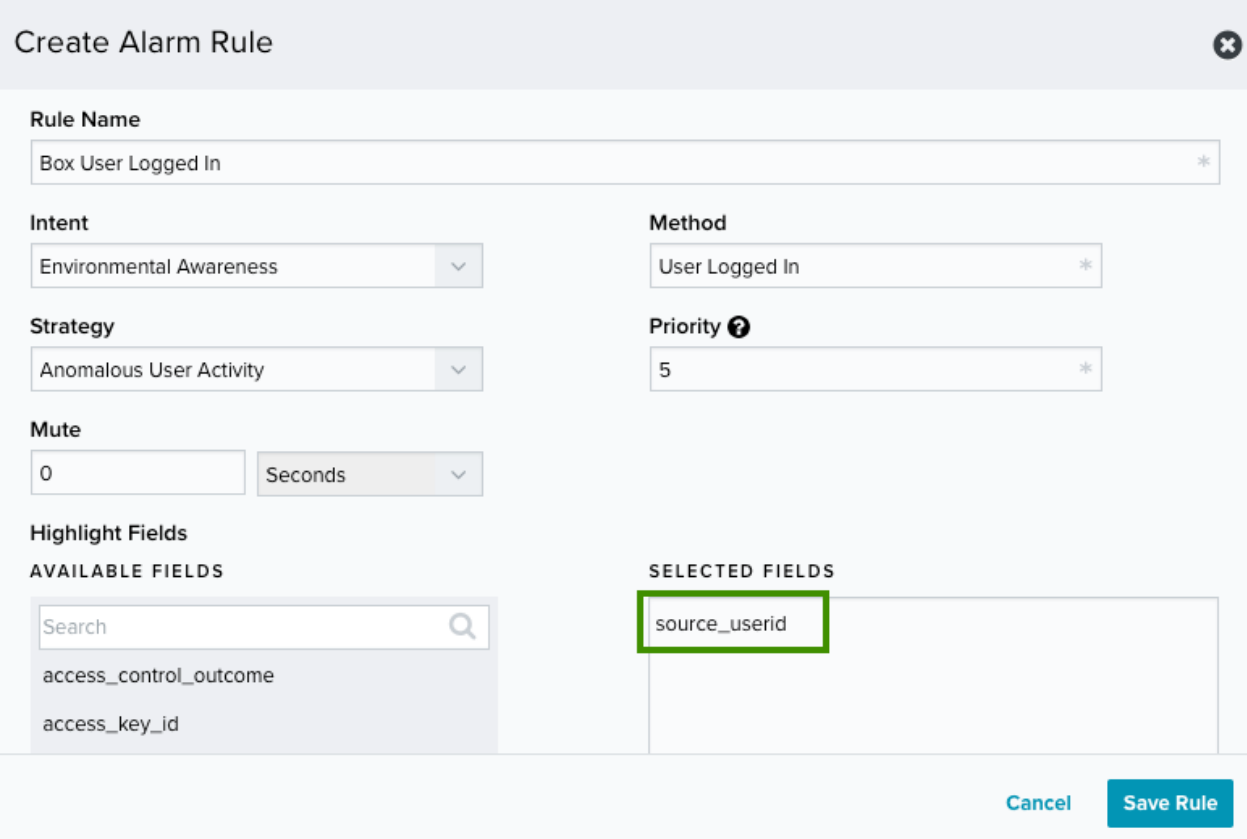
Examples of Alarms Generated from Box Data

Intent	Strategy	Method
System Compromise	Credential Abuse	Authentication to Box from a known malicious host
	Ransomware Infection	Multiple uploads with known ransomware extension
		Ransomware decryption instructions file upload
Exploitation & Installation	Malware Infection	Executable downloaded from Box followed by malware activity
Delivery & Attack	Brute Force Authentication	Successful login after a brute-force attack
		Password spraying against Box
	Data Exfiltration	File sent to a known malicious host
	Known Malicious Infrastructure	Box application created from a known malicious host
		File shared from a known malicious host
Reconnaissance & Probing	Brute Force Authentication	Multiple login failures
Environmental Awareness	Access Control Modification	Two-factor authentication disabled
	Account Manipulation	Multiple user accounts deleted
	Anomalous User Behavior	Admin login from an unknown device
	Credential Abuse	User login from two different countries in a short period
	Defense Evasion - Cover Tracks	User account created and deleted in short period

Examples of Alarms Generated from Box Data (Continued)

Intent	Strategy	Method
	Defense Evasion - Disabling Security Tools	Box security policy deleted
	Malware Infection	Box detected a malicious file upload
	Sensitive Data Disclosure	Box support access granted

You can create more rules to generate alarms for the Box events that are important to you. See Creating Alarm Rules from the Events page for detailed instructions. If you want to use the Disable Box User action from the resulting alarm, you must select **source_userid** as one of the fields when creating such a rule. For example:



Similarly, if you want to use the Create Box Task action from the resulting alarm, you must select **file_id** and **file_owner** as highlight fields when creating the alarm rule.

Launching a Box Response Action

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

After USM Anywhere identifies Box events and alarms, you determine which Box activities are suspicious and should be investigated, and use the Box workflow to notify the investigator. For example, if you see a file upload event and think it should be investigated, rather than manually notifying the investigator, you can use the BlueApp for Box response action, Create Box Task, to create a task in Box and send an email to the owner, thus simplifying your workflow.

The BlueApp for Box provides two actions: Disable Box User and Create Box Task. Both actions are available when you launch a response action directly from an alarm (described in the table below) or launch a response action in an orchestration rule.

Action	Description
Disable Box User	Run this action to inactivate the user account in Box.
Create Box Task	Run this action to create a task on a file in Box.

Note: Before launching a Box response action, you must have enabled and connected the BlueApp for Box to your Box Enterprise account. See Configuring the BlueApp for Box for more information.

When reviewing an alarm originated from a Box event, should you conclude that the Box user account has been compromised, you can launch an action to inactivate the Box user account associated with that alarm. If you want to apply the action to similar alarms that occur in the future, you can create an orchestration rule after you apply the action.

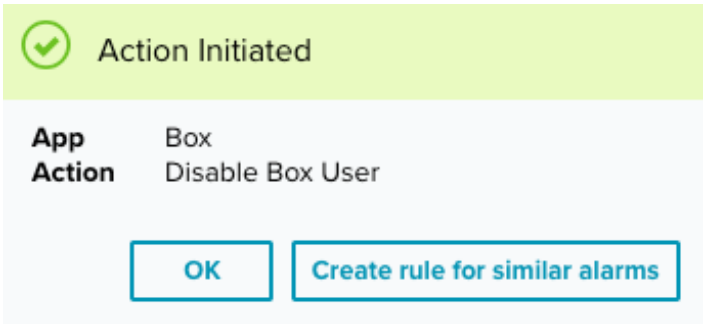
To launch the Disable Box User action for an alarm

1. Go to **Activity > Alarms**.
2. Review the alarms generated on the Box events, and then click the alarm to open its details.
3. Click **Select Action**, and then select the **Run Box Action** tile.
4. (Optional.) If you have more than one USM Anywhere Sensor configured for the BlueApp for Box, select the sensor that you want to use for the action.
5. In the App Action list, select **Disable Box User**.

Important: If you create your own alarm rule for Box events, keep in mind that the Disable Box User action only works when the alarm rule selects *source_userid* as one of the Highlight Fields.

6. Click **Run**.

   After USM Anywhere initiates the action for the alarm, it displays a confirmation dialog box.



7. If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** and define the new rule. If not, click **OK**.

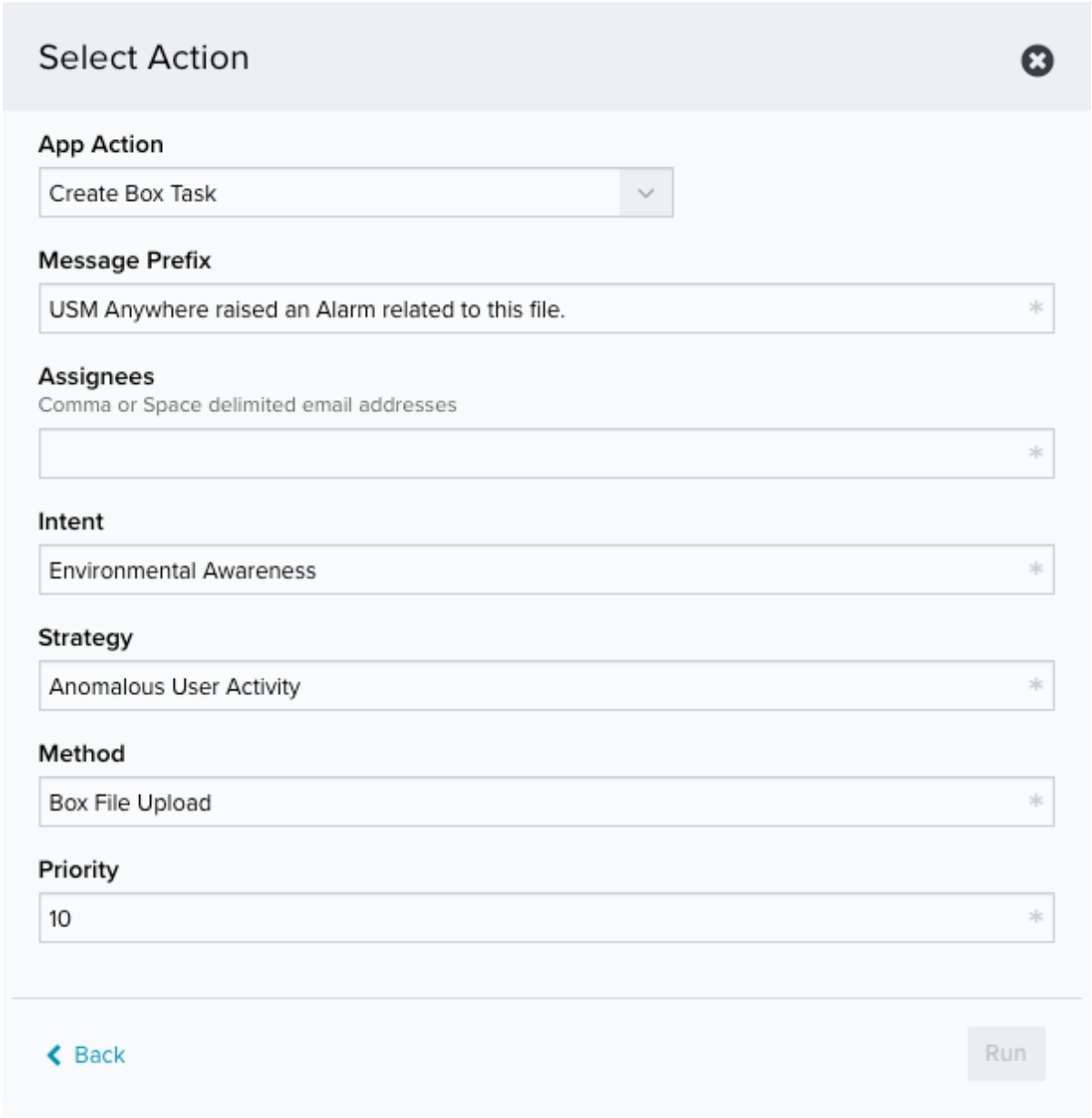
If the alarm is related to a file in you Box environment and you want it to be investigated, you can launch an action to create a task on the specific file. If you want to apply the action to similar alarms that occur in the future, you can create an orchestration rule after you apply the action.

To launch the Create Box Task action for an alarm

1. Go to **Activity > Alarms**.
2. Review the alarms generated on the Box events, and then click the alarm to open its details.
3. Click **Select Action**, and then select the **Run Box Action** tile.
4. (Optional.) If you have more than one USM Anywhere Sensor configured for the BlueApp for Box, select the sensor that you want to use for the action.
5. In the App Action list, select **Create Box Task**.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

   For your convenience, USM Anywhere populates some of the fields with the information it has collected, but you can modify them accordingly.

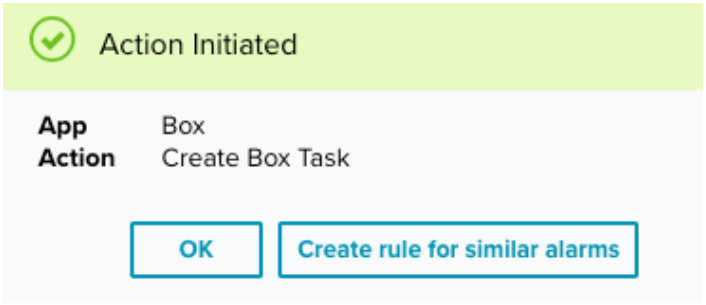


- In Message Prefix, provide a brief reasoning for the investigation.
- In Assignees, enter the email addresses of users who you want to notify about this task. These users should be the owner of the file or the administrator of the account.

Important: If you create your own alarm rule for Box events, keep in mind that the Create Box Task action only works when the alarm rule has *file_id* and *file_owner* selected as Highlight Fields.

6. Click **Run**.

After USM Anywhere initiates the action for the alarm, it displays a confirmation dialog box.



7. If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** and define the new rule. If not, click **OK**.

Creating Box Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Box response action when alarms match the criteria that you specify. For example, you can create a rule where USM Anywhere automatically disables the user when authentication to Box from a known malicious host occurs.

Warning: Be careful when automating the disabling of users because an error in the logic could result in all of your users, including administrators, being locked out. The only way to recover would be to contact Box support.

After you create a rule, new alarms that match the rule conditions will trigger the Box response action. The rule does *not* trigger for existing alarms.

You can create a new rule in one of two ways:

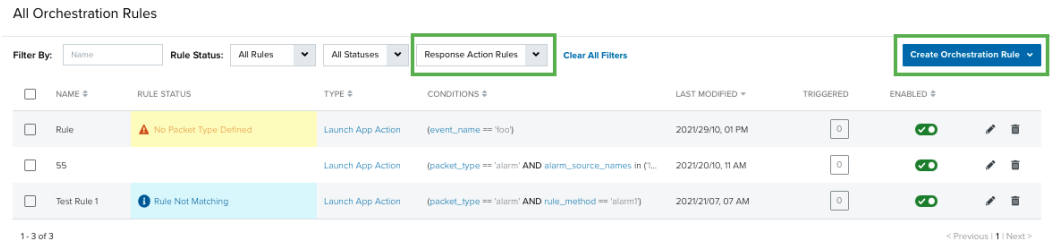
- **From an Applied Response Action**: You can create a rule using the response action that you apply to an existing alarm. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

  In the confirmation dialog box, click **Create rule for similar alarms**.

- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the

specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

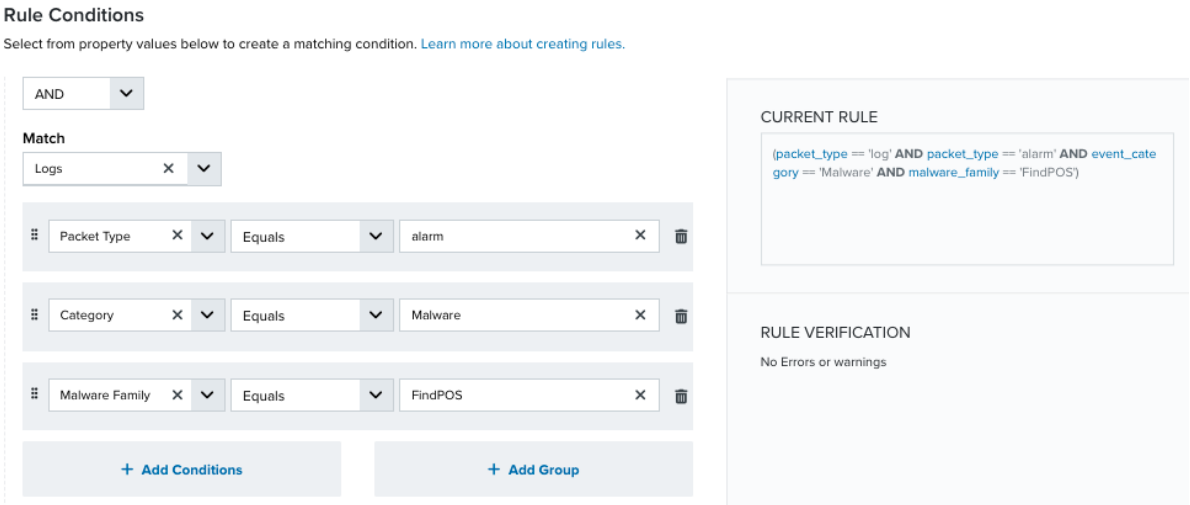
In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click **Create Orchestration Rule > Response Action Rule** to define the new rule.



To define a new Box response action rule

1. Enter a name for the rule.
2. In the Action Type list, select **Box**.
3. In the App Action list, select the action you want to use.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
4. Fill out the required fields.
5. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the  icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

6. Click **Save Rule**.
7. In the confirmation dialog box, click **OK**.

BlueApp for VMware Carbon Black Cloud

The BlueApp for VMware Carbon Black Cloud adds support for Carbon Black's cloud-hosted EDR Service. The AlienApp supports log collection via the Carbon Black API, detects Carbon Black devices, and adds them to the USM Anywhere asset inventory. It also includes the essential response actions needed to react to threats. Analysts can isolate or unisolate a system or move a system to a different policy group.

Edition: The BlueApp for VMware Carbon Black Cloud is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for VMware Carbon Black Cloud

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To configure the BlueApp for VMware Carbon Black Cloud in USM Anywhere, you first need to configure API key credentials. You also need to provide the hostname and Org Key for your Carbon Black Cloud instance.

Set up Carbon Black Cloud API

Follow the instructions listed in the VMware Carbon Black Cloud documentation to configure your API key credentials. Here are some guidelines on how to configure the API key credentials required for USM Appliance.

Note: Because VMware has announced that they are phasing out all preconfigured key types, creating your API keys with the Custom type may mean your BlueApp for VMware Carbon Black Cloud is more future-proof.

- LevelBlue does not recommend configuring Super User API keys for use with this app, as that API key type is far more permissive than this app requires.
- At minimum, your API key must be configured with the Manage Roles and Manage Users permissions from the Organization Settings category, as well as all permissions granted to users.
- If you are not planning to use a preconfigured API key type, you must configure and save your Custom API key type before creating your new API key.
- Once you have created your API key, you can view your credentials at any time by opening the Actions dropdown within Carbon Black Cloud settings and selecting API Credentials.

To view your Org Key, navigate to **Settings > API Access > API Keys** within the VMware Carbon Black Cloud console.

Configure the BlueApp for VMware Carbon Black Cloud in USM Anywhere

To enable the BlueApp for VMware Carbon Black Cloud

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.

5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the hostname, Org Key, and API key credentials.

7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.

4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for VMware Carbon Black Cloud Actions

The BlueApp for VMware Carbon Black Cloud provides a set of orchestration actions that you can use in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for VMware Carbon Black Cloud

Action	Description
Unquarantine Devices from Rule	This action unquarantines a VMware Carbon Black device from a rule.
Update Policy from Rule	This action updates a Carbon Black Cloud policy to a new policy from a rule.

Actions for the BlueApp for VMware Carbon Black Cloud (Continued)

Action	Description
Create a Note for an Alert	This action creates or deletes a note for an alert from an event, alarm, or rule.
Disable Bypass of Device	This action disables the bypass of a VMware Carbon Black device from an event or alarm.
Quarantine Devices	This action quarantines a specified device from an event or alarm. This action is not available on devices running a Linux operating system.
Create a Note for Threat	This action creates a note for a threat from an event, alarm, or rule.
Delete a Note from a Threat	This action deletes a note for a threat from an event or alarm.
Update Tags from Rule	This action adds tags to a threat from a rule.
Enable Bypass of Device	This action enables the bypass of a VMware Carbon Black device from an event or alarm.
Disable Bypass from Rule	This action disables the bypass of a VMware Carbon Black device from a rule.
Quarantine Devices from Rule	This action quarantines VMware Carbon Black devices from a rule.
Enable Bypass from Rule	This action enables the bypass of a VMware Carbon Black device from a rule.
Unquarantine Devices	This action unquarantines a specified quarantined device from an event or alarm. This action is not available on devices running a Linux operating system.
Delete a Note from an Alert	This action deletes a note for an alert from an event or alarm.
Update Tags	This action adds tags to a threat from an event or alarm.
Update Policy	This action moves VMware Carbon Black device to a new policy from an event or alarm.
Delete a Tag	This action deletes a tag for a threat from an event or alarm.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms and Events

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or an event.

To launch a Carbon Black Cloud response action for an Alarm or Event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Carbon Black Cloud Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create Rule for Similar Alarms** or **Create Rule for Similar Events** and define the new rule. If not, click **OK**.

BlueApp for VMware Carbon Black Cloud Asset Discovery and Management

The BlueApp for VMware Carbon Black Cloud features powerful vulnerability assessment capabilities that can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow Carbon Black Cloud to create assets that are discovered in scans, as well as merge the asset information provided from the Carbon Black Cloud scan with the existing asset information in USM Anywhere.

Asset Creation from the BlueApp for VMware Carbon Black Cloud

When Carbon Black Cloud runs a scan, it identifies all assets and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in the app's configuration menu. Assets created from a Carbon Black Cloud scan include the information ported from Carbon Black Cloud in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in Carbon Black Cloud scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the Carbon Black Cloud configuration menu, USM Anywhere merges the information from the Carbon Black Cloud scan with the existing asset. Assets are matched by comparing source IDs from the Carbon Black Cloud scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the Carbon Black Cloud configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for VMware Carbon Black Cloud page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the Carbon Black Cloud scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the Carbon Black Cloud scan.
- **Merge:** Merge the information from the Carbon Black Cloud scan with the matching asset details in USM Anywhere.
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a Carbon Black Cloud profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window displays showing the existing asset and the new asset that will be created once the two are split.
4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for Carbon Black EDR

The BlueApp for Carbon Black EDR enhances the threat detection capabilities of USM Anywhere by collecting and analyzing log data from your Carbon Black EDR, and provides orchestration actions to streamline incident response activities. This BlueApp combines USM Anywhere advanced threat detection and the ability to automatically isolate compromised systems with Carbon Black EDR.

Edition: The BlueApp for Carbon Black EDR is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Collecting Logs from Carbon Black EDR

Role Availability	Read-Only	Investigator	Analyst	Manager

To fully integrate USM Anywhere with your Carbon Black EDR implementation, you should configure Carbon Black EDR to send syslog message to USM Anywhere so that it can collect and normalize the raw data. The combination of processing the log data and connecting the BlueApp to the Carbon Black EDR API provides a full scope of data analysis and response within USM Anywhere.

Send Carbon Black EDR Logs to the Sensor

Before configuring the log collection, you must have the IP address of the USM Anywhere Sensor.

To send log data from Carbon Black EDR to USM Anywhere

1. Install and configure the cb-event-forwarder. See the Carbon Black Event Forwarder Quickstart Guide for instructions.

   Events exported from Carbon Black Event Forwarder can be in JavaScript Object Notation (JSON) or Log Event Extended Format (LEEF) format.

2. Modify the `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` file, include the following item:

   ```
   udpout=<USM-Anywhere-Sensor-IP-Address>:514
   ```

Assign Assets to the BlueApp

To help BlueApp for Carbon Black EDR identify the relevant logs, you must associate this app with the asset that is forwarding the logs.

To assign assets to the BlueApp

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Assign Asset**.
5. Search for your asset using its name or IP address, and then click **Assign**.
6. If your asset is not in USM Anywhere, click **Create Asset** to add it.

7. Select the method that the USM Anywhere Sensor should use to collect logs from your asset.

   Syslog is the default method, but USM Anywhere can also collect logs from an Amazon S3 bucket or Amazon CloudWatch.

8. In the Format field, click the icon and select **JSON** from the drop-down.

   Events exported from Carbon Black Event Forwarder are in a normalized JSON format; therefore you must set the Format field to JSON.

Configuring the BlueApp for Carbon Black EDR

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

When the BlueApp for Carbon Black EDR is enabled and connected to your Carbon Black Response deployment, you can launch app actions and create orchestration rules to send data from USM Anywhere to Carbon Black Response. See BlueApp for Carbon Black EDR Actions for more information about the orchestration actions supported by the BlueApp for Carbon Black EDR.

Note: To fully integrate USM Anywhere with your Carbon Black implementation, you should also have the Carbon Black log collection enabled so that USM Anywhere can retrieve and normalize raw log data from the Carbon Black applications. See Collecting Logs from Carbon Black EDR for information about raw log data retrieval.

Generate a Carbon Black API Token

Before you can use the Carbon Black orchestration actions within USM Anywhere, you must have an API token that USM Anywhere can use to connect to your Carbon Black server. Carbon Black generates this token for use by your user account.

Important: You must have global administrator privileges to generate a valid API token for integration with the BlueApp for Carbon Black EDR.

To acquire the API token for Carbon Black EDR

1. Go to https://developer.carbonblack.com/reference/enterprise-response/authentication/ and follow the vendor instructions to generate the API token.
2. Copy the token to be entered in USM Anywhere.

Important: If you generate a new API token or key at some point in the future, it will revoke the existing token making the connection unauthorized. Therefore, you must update the token in USM Anywhere accordingly.

Enable the API Connection

After you generate a Carbon Black API token and copy the value, you're ready to enable the BlueApp for Carbon Black EDR in USM Anywhere.

To enable the Carbon Black API connection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Specify the connection information for your Carbon Black EDR server:
   - **Server address:** Enter the IP address or hostname of your Carbon Black EDR server.
   - **API token**: Click **Change API token** and enter the API token created in Carbon Black EDR.
   - **(Optional.) Custom Certificate Authority Public Certificate:** If you want to use a security certificate for the authentication, select the checkbox and add your certificate to establish a trusted Secure Sockets Layer (SSL) connection between your Carbon Black EDR server and USM Anywhere.
7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Carbon Black EDR APIs, a icon displays in the Health column.

If the ⊗ icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Carbon Black EDR connection.

BlueApp for Carbon Black EDR Actions

With the BlueApp for Carbon Black EDR, USM Anywhere can send a request to Carbon Black EDR to isolate an endpoint instantly — through a user-executed action or an automated rule — to coordinate threat detection and response in a single action. The bidirectional capabilities of the BlueApp for Carbon Black EDR enable USM Anywhere to incorporate data from Carbon Black (see Collecting Logs from Carbon Black EDR) into its threat analysis and orchestrate response actions by passing compromised endpoints identified by USM Anywhere to Carbon Black EDR.

Important: Using the BlueApp for Carbon Black EDR orchestration actions require that the BlueApp is enabled on a deployed USM Anywhere Sensor with a configured integration to the Carbon Black EDR API. See Configuring the BlueApp for Carbon Black EDR for more information.

As USM Anywhere surfaces events and alarms, your team determines which items require a response action from the BlueApp for Carbon Black EDR. Rather than manually isolating an affected endpoint within Carbon Black EDR, you can use the orchestration actions to respond to threats identified in the event or alarm. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Carbon Black EDR

Action	Description
Isolate Hosts from Alarm	Run this action directly from an alarm to send a request to Carbon Black EDR to isolate the associated endpoint(s)
Isolate Hosts from Orchestration Rule	Run this action in an orchestration rule to send a request to Carbon Black EDR to isolate the associated endpoint(s) for future events that trigger the rule

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

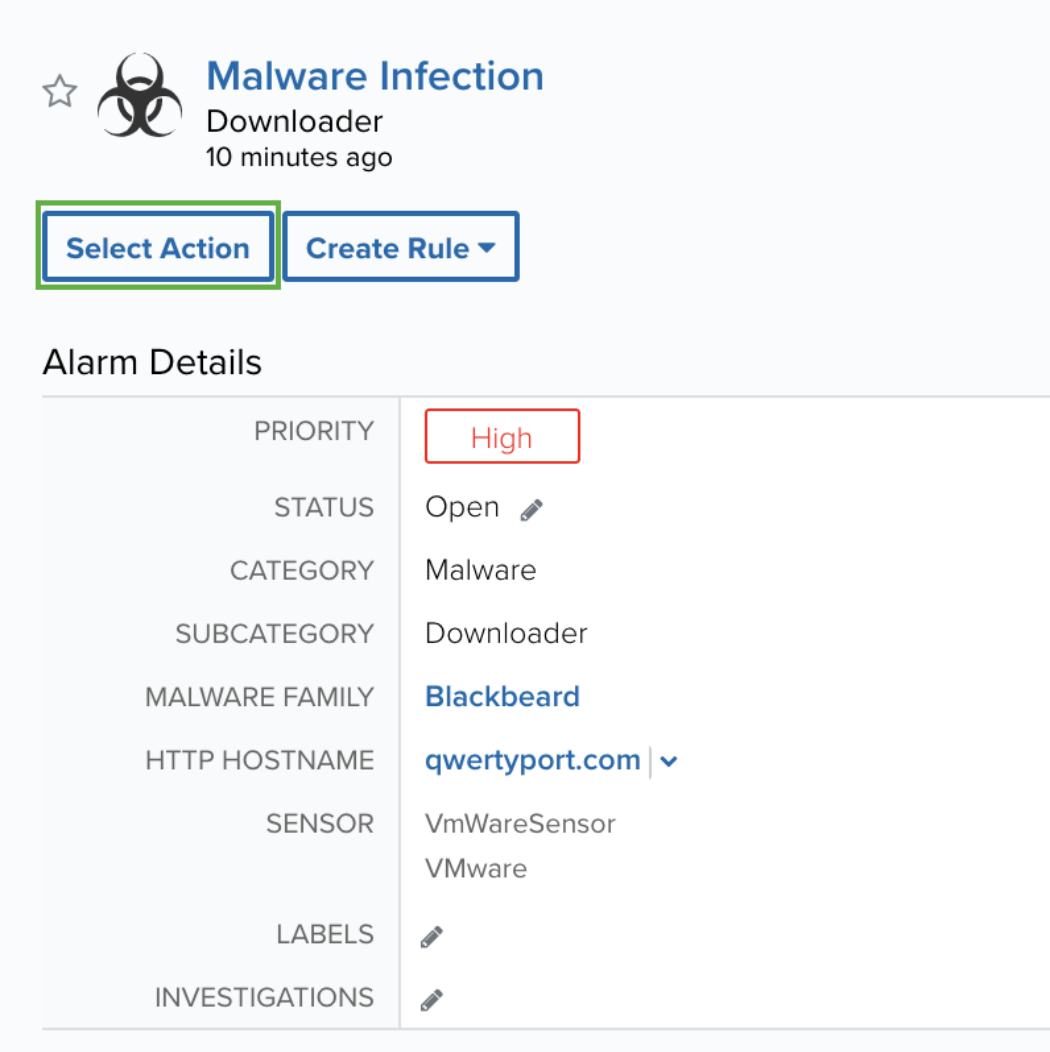
Launch Actions from USM Anywhere

If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

Note: Before launching a Carbon Black EDR action, the BlueApp for Carbon Black EDR must be enabled and configured. See Configuring the BlueApp for Carbon Black EDR for more information.

To launch a Carbon Black EDR action for an alarm

1. Go to **Activity > Alarms**.
2. Click the alarm to open the alarm details.
3. Click **Select Action**.

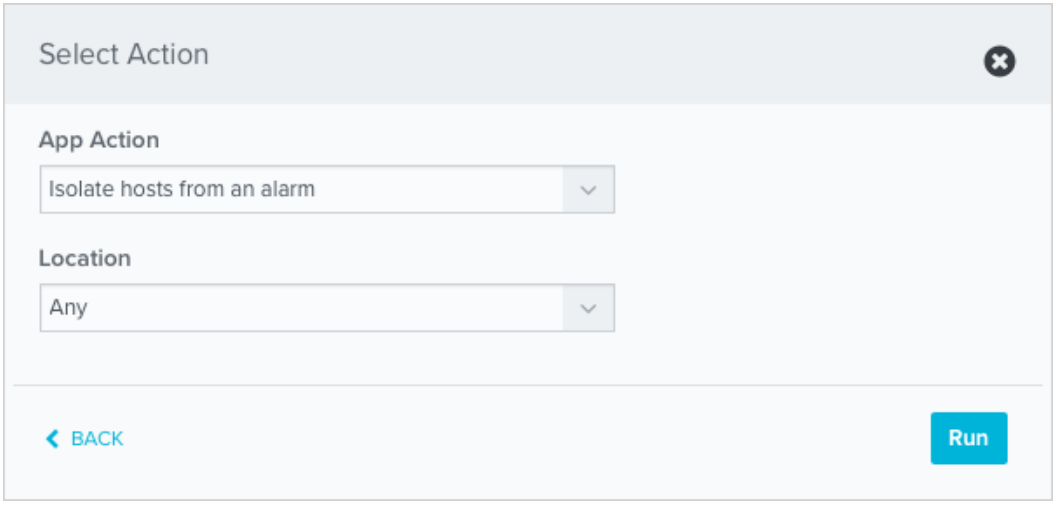


4. In the Select Action dialog box, select the **Carbon Black** tile.

   This displays the options for the selected response app.

5. (Optional.) If you have more than one sensor where the BlueApp for Carbon Black EDR is enabled and configured, select the sensor that you want to use to execute the action.

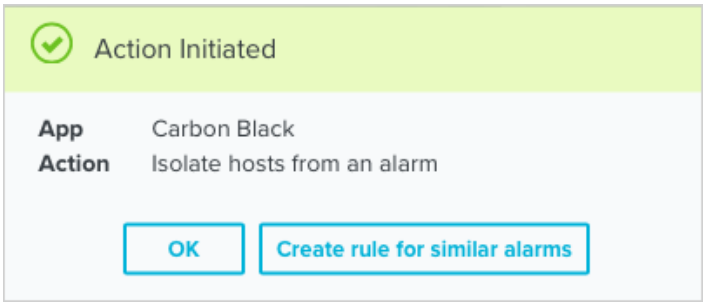
6. Select the **Location** to be isolated.



- **Source**: Use this option to isolate the source endpoint of the alarm.
- **Destination**: Use this option to isolate the destination endpoint of the alarm.
- **Any**: Use this option to let the system search for the Carbon Black endpoints using the IP addresses in the alarm and isolate those that are identified.

7. Click **Run**.

   After USM Anywhere initiates the action, a confirmation dialog box displays:



   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** and define the new rule. If not, click **OK**.

Creating Carbon Black EDR Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a response action when events match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically sends the host information for malware infections that it identifies to Carbon Black EDR as a request to isolate the endpoint.

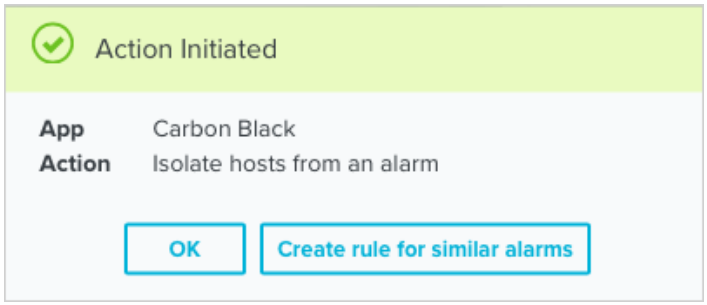
Note: Before creating an orchestration rule or launching a response action, the BlueApp for Carbon Black EDR must be enabled and configured. See Configuring the BlueApp for Carbon Black EDR for more information.

After you create a rule, new alarms or events that match the rule conditions will trigger the Carbon Black action to isolate an endpoint. The rule does *not* trigger for your existing alarms or events.

You can create a new rule in one of two ways:

- **From an Applied Response Action**: You can automatically create a rule using the response action that you apply to an existing alarm. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

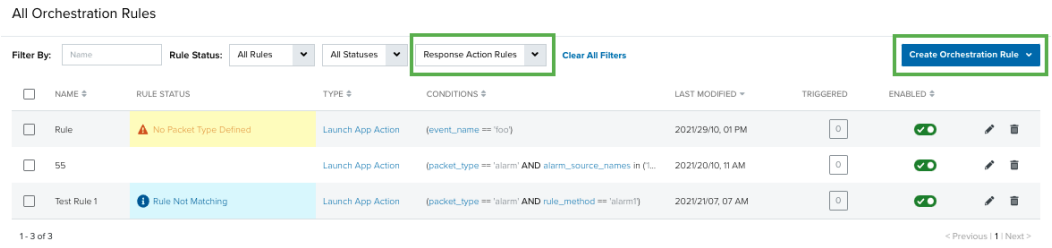
  In the confirmation dialog box, click **Create rule for similar alarms**.



- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

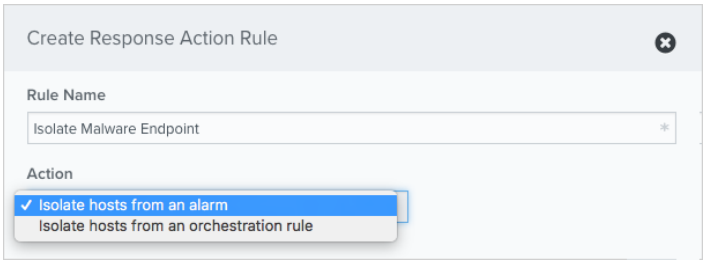
  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click

Create Orchestration Rule > Response Action Rule to define the new rule.



To define a new response action rule

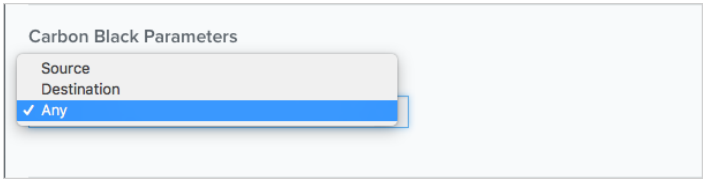
1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the action.



The parameters you can set for Carbon Black EDR depends on the action that you select:

Isolate hosts from an alarm

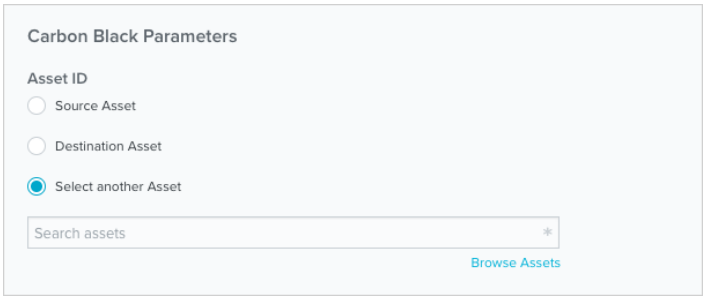
This is the default action. Use this action to trigger the rule for alarms that satisfy the matching criteria. Select a **Location** for the triggered action.



- **Source**: Use this option to isolate the source endpoint of the alarm.
- **Destination**: Use this option to isolate the destination endpoint of the alarm.
- **Any**: Use this option to let the system search for the Carbon Black EDR endpoints using the IP addresses in the alarm and isolate those that are identified.

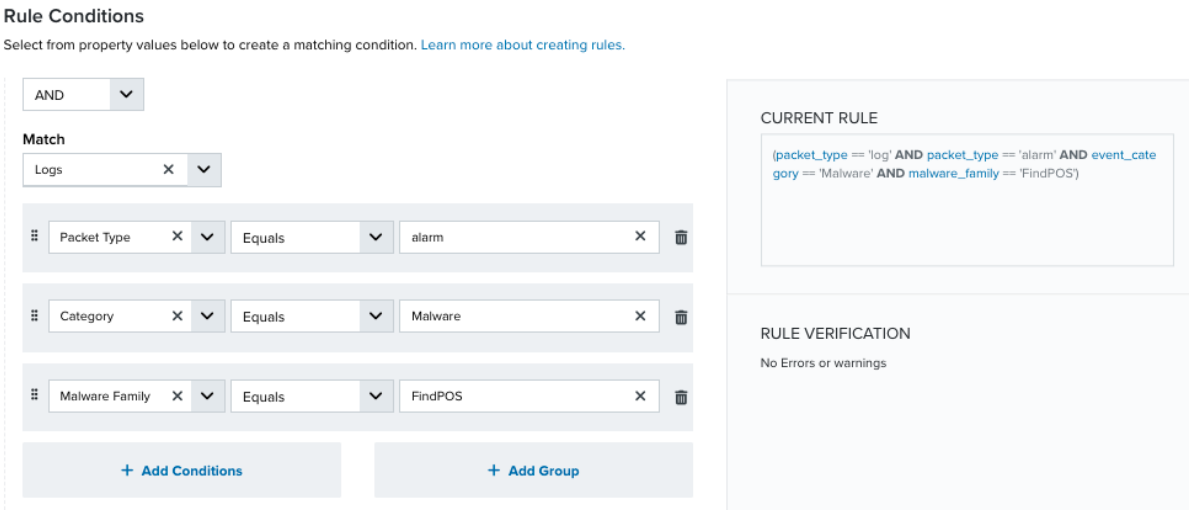
Isolate hosts from an orchestration rule

Select the asset to be isolated.



- **Source Asset**: Use this option to isolate the source endpoint of the alarm.
- **Destination Asset**: Use this option to isolate the destination endpoint of the alarm.
- **Select another Asset**: Use this option to isolate the endpoint for a specified asset. Use the search field or click **Select from List** to locate and select the asset.

3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.

- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

Viewing Alarms with Applied Carbon Black EDR Response Actions

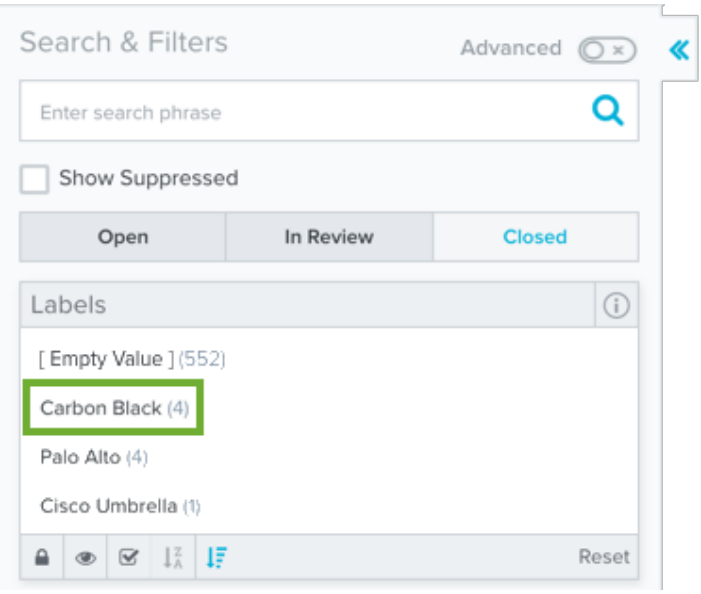
Role Availability ✔ **Read-Only** ✔ **Investigator** ✔ **Analyst** ✔ **Manager**

USM Anywhere uses labels as a mechanism to classify alarms. These labels make it easy to filter items by an applied label so that you can locate them easily and track their status. When the BlueApp for Carbon Black EDR executes a response action for an alarm, it automatically applies the *Carbon Black* label to it. You can select this label as a filter so that a page displays data for only the items related to an BlueApp for Carbon Black EDR action.

To view alarms with applied response actions

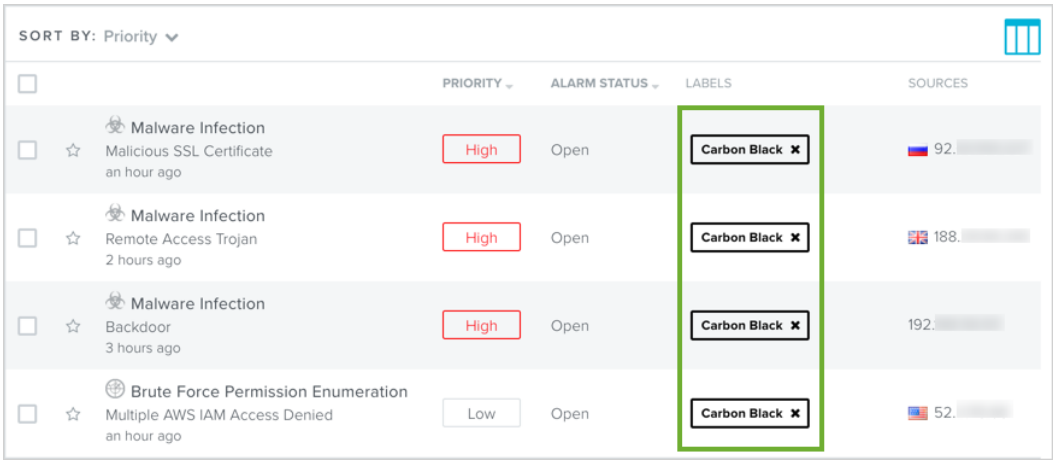
1. Open the Alarms page.
2. If the Search & Filters panel is not displayed, click the  icon to expand it.

   USM Anywhere includes several filters displayed by default.
3. Locate the Labels filter and select **Carbon Black**.



If the Labels filter is not displayed, click **Configure Filters** at the bottom of the Search & Filters pane to configure filters for the page. See Managing Filters in the *USM Anywhere User Guide* for more information about configuring filters for the page display.

In the displayed list, you can scroll the list to the right and view the Labels column.



BlueApp for Check Point

The BlueApp for Check Point enables you to automate threat detection and response activities between USM Anywhere and Check Point. The BlueApp for Check Point enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to

streamline incident response activities from your Check Point firewall and provides orchestration actions to streamline incident response activities based on risk identified in USM Anywhere.

Edition: The BlueApp for Check Point is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Check Point

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

Before you can begin configuration, you must have the following information from your Check Point instance:

- IP address or hostname
- Port
- Username and password
- (Optional) Certificate Authority (CA) certificates

Check Point Configurations

You need to have the API configured to automatically start in order for USM Anywhere to communicate with the API. You should also allow API calls from all IP addresses. You also need a user account with read and write user permissions.

To set up your Check Point API

1. Log in to the Check Point SmartConsole.
2. Go to **Manage & Settings > Blades > Management API** and click the **Advanced Settings** button.

3. Under Startup Settings, select the **Automatic Start** checkbox.
4. Under Access Settings, select **All IP addresses**.
5. Click **OK**.

To make sure your account has read and write permissions

1. Log in to the Check Point SmartConsole.
2. Go to **Manage & Settings > Permissions and Administrators**.
3. Double click on your account.
4. Under Permissions, click the **Permissions Profile** box and select **Read Write All**.
5. Click **OK**.

To enable the AlienApp for Check Point

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the following items:
   - IP address or hostname
   - Port
   - Username
   - Password
7. Optionally, check **Require CA certificate** and **Validate HTTPS host name** if you want to use this option, and then enter the CA certificate.

> **Note:** If you want to deploy into your network and use a self-signed CA certificate, then you will need to upload it here. The certificate can be found in the `/web/conf/server.crt` file path.

8. Click **Save** .
9. Verify the connection.

   After USM Anywhere completes a successful connection to the Check Point APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Check Point connection.

Forward Check Point Syslog Messages to USM Anywhere

To fully integrate USM Anywhere with the BlueApp for Check Point, you need to configure syslog forwarding in the Check Point device or management server to send the events to your sensor. See the Check Point Log Exporter guide and follow the steps outlined in the Basic Deployment section to configure syslog forwarding.

Assign Your Assets

Because the AlienApp for Check Point is not auto-discovered, you must manually assign the BlueApp to the asset representing the Check Point device or management server's IP address in USM Anywhere. If the BlueApp isn't assigned to any assets, the Check Point events will be handled by the LevelBlue Generic Data Source, which will result in some of the data from the log not being properly parsed or associated with the BlueApp.

See Assign Assets to BlueApps for instructions on how to assign your assets to AlienApp for Check Point.

BlueApp for Check Point Actions

The BlueApp for Check Point provides a set of orchestration actions that you can use to identify and categorize items to send to your firewall as a response to threats identified by USM Anywhere.

As USM Anywhere surfaces events, vulnerabilities, and alarms, your team determines which items require a response action. Rather than manually tagging threats, you can use the BlueApp for Check Point orchestration actions to enforce protection based on the information associated with the event or alarm. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Check Point

Action	Description
Tag Source IP Address	Run this action to label the source IP address based on an event
Tag Destination IP Address	Run this action to label the destination IP address based on an event
Tag Source IP Address from Alarm	Run this action to label the source IP address from an alarm
Tag Destination IP Address from Alarm	Run this action to label the destination IP address from an alarm
Tag Source IP from Rule	Run this action to label the source IP address from a predefined rule
Tag Destination IP Address from Rule	Run this action to label the destination IP address from a predefined rule
Add a Threat Indicator from Event Using File Hash	Run this action to add a threat indicator from an event using a file hash
Add a Threat Indicator from Event Using Source IP Address	Run this action to add a threat indicator from an event using the source IP address
Add a Threat Indicator from Event Using URL	Run this action to add a threat indicator from an event using a URL
Add a Threat Indicator from Event Using Source Domain	Run this action to add a threat indicator from an event using the source domain
Add a Threat Indicator from Event Using Destination Domain	Run this action to add a threat indicator from an event using the destination domain
Add a Threat Indicator from Event Using Destination IP Address	Run this action to add a threat indicator from an event using the destination IP address

Actions for the BlueApp for Check Point (Continued)

Action	Description
Add a Threat Indicator from Alarm Using Source IP	Run this action to add a threat indicator from an alarm using the source IP address
Add Threat Indicator from Alarm Using Destination IP	Run this action to add a threat indicator from an alarm using the destination IP address
Add Threat Indicator from Alarm Using File Hash	Run this action to add a threat indicator from an alarm using a file hash for enhanced security
Add Threat Indicator from Alarm Using URL	Run this action to add a threat indicator from an alarm using a URL
Add Threat Indicator from Alarm Using Source Domain	Run this action to add a threat indicator from an alarm using the source domain
Add Threat Indicator from Alarm Using Destination Domain	Run this action to add a threat indicator from an alarm using the destination domain
Add Threat Indicator from Rule Using URL	Run this action to add a threat indicator from a predefined rule using a URL
Add Threat Indicator from Rule Using Source Domain	Run this action to add a threat indicator from a predefined rule using the source domain
Add Threat Indicator from Rule Using Destination Domain	Run this action to add a threat indicator from a predefined rule using the destination domain
Add Threat Indicator from Rule Using File Hash	Run this action to add a threat indicator from a predefined rule using a file hash for improved security analysis
Add Threat Indicator from Rule Using Source IP	Run this action to add a threat indicator from a predefined rule based on the source IP address
Add Threat Indicator from Rule Using Destination IP	Run this action to add a threat indicator from a predefined rule based on the destination IP address

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

To launch a Check Point orchestration action for an alarm

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **Check Point** tile.
5. For the App Action, select the action you want to launch.

   You can launch an action to add or remove an IP address to the allowed list, add an IP address to the blocked list, or add the IP address to a custom category.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Check Point Response Action Rules

Role Availability | Read-Only | Investigator | Analyst | Manager

Use the BlueApp for Check Point to access the Check Point response actions, which enable you to quickly respond to threats identified by USM Anywhere. You can create response action rules in USM Anywhere that automatically trigger when alarms or events match the criteria that you specify.

After you create a rule, new events or alarms that match the rule will trigger the Check Point action to tag to the associated source or the destination host. The rule does *not* trigger for your existing alarms or events.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

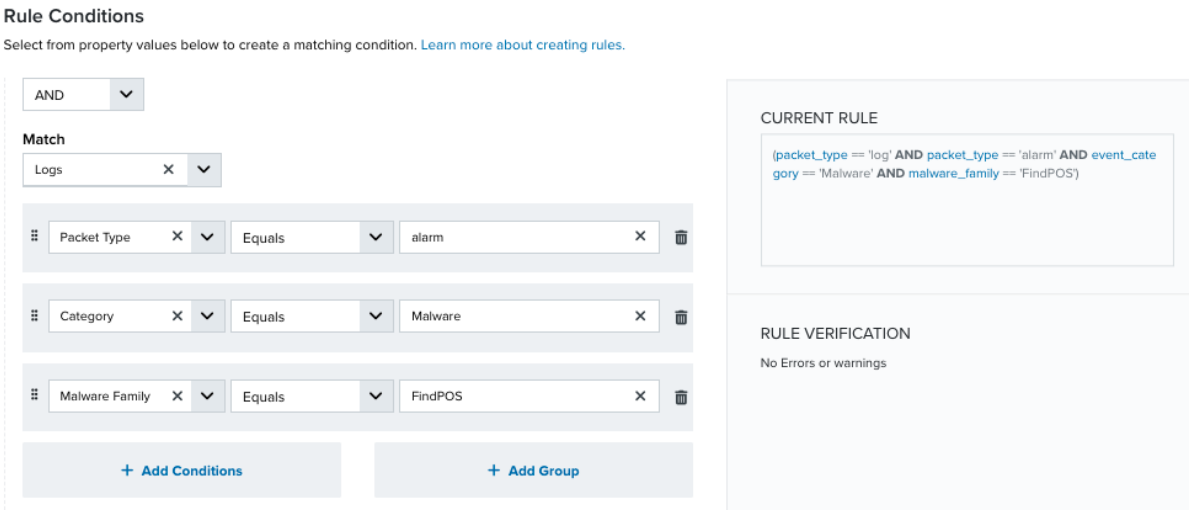
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation pane. Then click **Create Response Action Rule** to define the new rule.

To define a new Check Point response action rule

1. Enter a name for the rule.
2. Select the action you want to launch from the **Action** drop-down menu.

   You can launch an action to tag the destination host or source for an alarm or an event.

3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. Click **OK** in the confirmation dialog box.

BlueApp for Cisco Duo

The BlueApp for Cisco Duo enables you to collect security events with the user's authentication on Cisco systems and merge users from Cisco systems into USM Anywhere. The BlueApp for Cisco Duo enhances the threat response capabilities of USM Anywhere by

providing orchestration and response actions to isolate or unisolate hosts based on risks identified in USM Anywhere. The BlueApp for Cisco Duo also allows you to collect hourly events from Cisco Duo through the USM Anywhere Job Scheduler.

Edition: The BlueApp for Cisco Secure Endpoint is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Cisco Duo

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the BlueApp for Cisco Duo in USM Anywhere, you first need to log in to Cisco Duo to create an API hostname, integration key, and secret key.

Under **Settings**, select the following minimum API permissions:

- Grant write resource
- Grant read log
- Grant read resource

To get the API credentials from Cisco Duo

Follow the Cisco documentation on how to create API credentials to obtain the API hostname, integration key, and secret key.

If you are using more than one Cisco Duo Admin API, you can rename your new Duo Admin API to track its use separately.

Connecting the Cisco Duo App in USM Anywhere

After you obtain the credentials, you must configure the connection within USM Anywhere.

To enable the AlienApp for Cisco Duo

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the information you generated from the Cisco Duo admin panel into the following fields:
   - API hostname
   - Integration key
   - Secret key
7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Cisco Secure Endpoint Representational State Transfer (REST) APIs, a  icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Cisco Secure Endpoint connection.

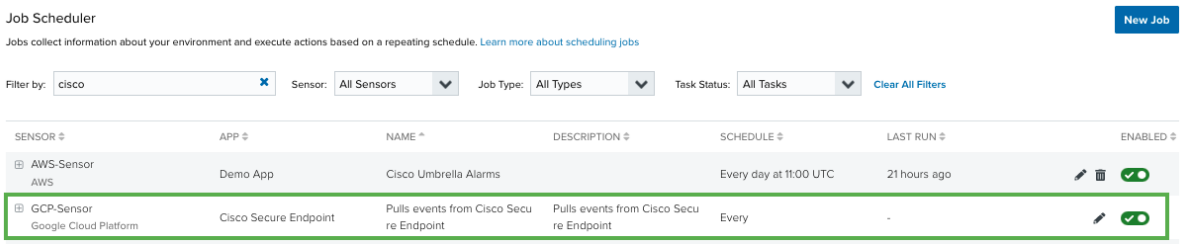
Cisco Duo Event Collection

Once the BlueApp for Cisco Duo has been configured, you can choose to have USM Anywhere collect Cisco Duo events from the app on an hourly basis.

To configure Cisco Duo event collection

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the Cisco Secure Endpoint app on the sensor it was deployed to.
3. In the enabled column, click the icon for the inactive Cisco Secure Endpoint events job.

   The icon turns green and hourly event collection from Cisco Secure Endpoint is enabled.



4. (Optional.) Click the icon to customize the frequency of the event collection.

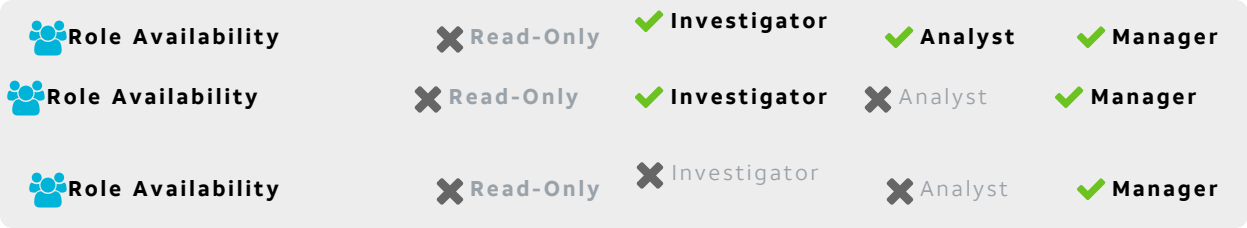
BlueApp for Cisco Firepower Management

The BlueApp for Cisco Firepower Management enables you to act on the Cisco firewalls infrastructure with one or several responses from USM Anywhere. The BlueApp for Cisco Firepower Management enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from the Cisco Firepower Management Center and provides orchestration actions to implement Cisco incident response activities based on the risk identified in USM Anywhere.

Edition: The BlueApp for Cisco Firepower Management is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Cisco Firepower Management



To configure the BlueApp for Cisco Firepower Management in USM Anywhere, you need to have the host URL and a set of user credentials granted administrator level permissions.

Set up the Cisco Firepower Management API

Follow the instructions listed in the Cisco Firepower Management Center documentation to locate the host URL. Here are the instructions on how to configure the BlueApp for Cisco Firepower Management.

Configure the BlueApp for Cisco Firepower Management in USM Anywhere

To enable the BlueApp for Cisco Firepower Management

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the host URL and either your user credentials or your CA cert.
7. Click **Save**.

BlueApp for Cisco Meraki

The BlueApp for Cisco Meraki enables you to integrate the Cisco Meraki capabilities with your USM Anywhere instance. The BlueApp for Cisco Meraki enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from Cisco Meraki and provides orchestration actions to implement Meraki incident response activities based on the risk identified in USM Anywhere.

Edition: The BlueApp for Cisco Meraki is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Cisco Meraki

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To configure the BlueApp for Cisco Meraki in USM Anywhere, you need to have the API key, which you will obtain from your Cisco support team.

Set up Cisco Meraki API

Follow the instructions listed in the Cisco product documentation. Here are the instructions on how to configure Cisco Meraki to push logs to your USM Anywhere™ Sensor.

1. Open your Meraki dashboard and navigate to **Organization > Settings**.
2. Ensure that the API Access is set to *Enable access to the Cisco Meraki Dashboard API*.
3. Within the Cisco Meraki dashboard, navigate to a device you would like to configure to send logs to USM Anywhere™.
4. Click **Alerts & Administration**.
5. Scroll to the Logging section and click **Add a syslog server**.
6. Enter the IP Address of your syslog server and the correct port number.
7. Using the Roles field, select the type of events you would like to export:

- **Event Log**: The messages from the dashboard under Monitor > Event Log.
- **Flows**: Syslog messages generated by inbound and outbound traffic flows, including the source, destination, and port numbers.
- **URL**: Syslog messages generated by HTTP GET requests.

Note: You can direct each type of traffic to a different syslog server.

Configure the BlueApp for Cisco Meraki in USM Anywhere

To enable the BlueApp for Cisco Meraki

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the API key you received from your Cisco support team.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

The  icon turns green, and collection is enabled.

4. (Optional.) Click the  icon to customize the frequency of the event collection.

BlueApp for Cisco Meraki Asset Discovery and Management

The BlueApp for Cisco Meraki features powerful vulnerability assessment capabilities that can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow Cisco Meraki to create assets that are discovered in scans, as well as merge the asset information provided from the Cisco Meraki scan with the existing asset information in USM Anywhere.

Asset Creation from BlueApp for Cisco Meraki

When Cisco Meraki runs a scan, it identifies all assets and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in the app's configuration menu. Assets created from a Cisco Meraki scan include the information ported from Cisco Meraki in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in Cisco Meraki scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the Cisco Meraki configuration menu, USM Anywhere merges the information from the Cisco Meraki scan with the existing asset. Assets are matched by comparing the MAC addresses detected during the Cisco Meraki scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the Cisco Meraki configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for Cisco Meraki page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the Cisco Meraki scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the Cisco Meraki scan.

- **Merge:** Merge the information from the Cisco Meraki scan with the matching asset details in USM Anywhere.
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a Cisco Meraki profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window displays showing the existing asset and the new asset that will be created once the two are split.
4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for Cisco Meraki Actions

The BlueApp for Cisco Merakiprovides a set of orchestration actions that you can use to integrate your Cisco Meraki capabilities in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Cisco Meraki

Action	Description
Remove Network Device	Run this action to remove the network device from the asset inventory, event, or alarm
Network Security Events Collector	Run this action to collect network security events
Network Desktop Events Collector	Run this action to collect network desktop events

Actions for the BlueApp for Cisco Meraki (Continued)

Action	Description
Organization Security Events Collector	Run this action to collect organization security events
Provision Network Client	Run this action to provision network clients This action is available from an event, alarm, or orchestration rule
Organization Network Events Collector	Run this action to collect organization network events
Remove Network Device	Run this action to remove the network device from an event or alarm
Provision Network Client	Run this action to provision network clients from an asset
Network Client Security Events Collector	Run this action to collect organization network client security events
Asset Discovery	Run this action to collect matched assets from Cisco Meraki
Provision Network Device from Asset	Run this action to provision the network device using information from the asset inventory
Provision Network Device from Event/Alarm	Run this action to provision the network device based on information from an event or alarm
Provision Network Device from Rule	Run this action to provision the network device according to predefined rules
Remove Network Device from Rule	Run this action to remove a network device from a predefined rule

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms, Events, and Assets

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an Alarm, Event, or an Asset.

To launch a Cisco Meraki response action for a an Alarm, Event, or an Asset

1. Go to [**Environment > Assets**, **Activity > Alarms**, or **Activity > Events**
2. Click the Alarm, Event, or Asset to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Cisco Meraki Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click [**Create rule for similar assets Create rule for similar alarms** or **Create rule for similar events**] and define the new rule. If not, click **OK**.

Creating Cisco Meraki Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Cisco Meraki response action when [alarms, events, and assets match the criteria that you specify. After you create a rule, new vulnerabilities that match the rule conditions trigger the Meraki response action to create a new incident. The rule does *not* trigger for existing alarms, events, or assets.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the

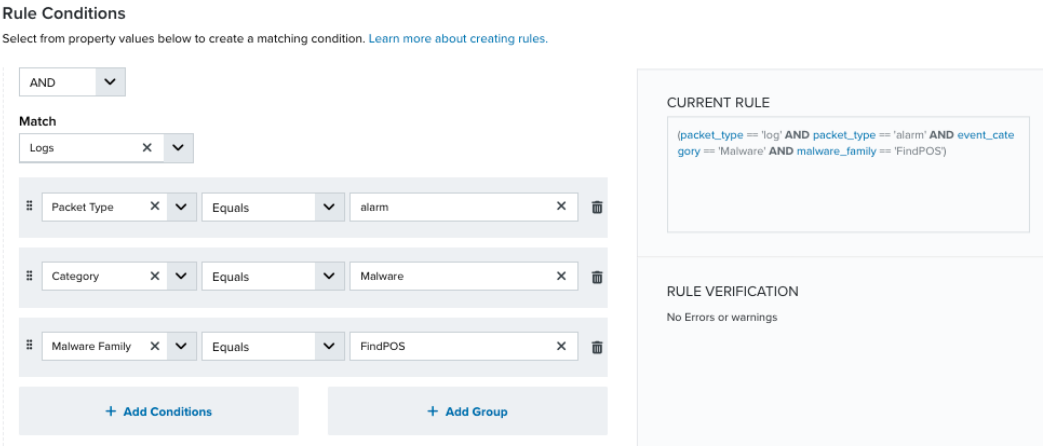
specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the app**: Go to the BlueApp for Cisco Meraki page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new Cisco Meraki response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the [appvariable] incident.
3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red

border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Cisco Secure Endpoint

The BlueApp for Cisco Secure Endpoint enables you to automate threat detection and response activities between USM Anywhere and Cisco Secure Endpoint. The BlueApp for Cisco Secure Endpoint enhances the threat response capabilities of USM Anywhere by providing orchestration and response actions to isolate or unisolate hosts based on risks identified in USM Anywhere. The BlueApp for Cisco Secure Endpoint also allows you to collect hourly events from Cisco Secure Endpoint through the USM Anywhere Job Scheduler.

Edition: The BlueApp for Cisco Secure Endpoint is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Cisco Secure Endpoint

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the BlueApp for Cisco Secure Endpoint in USM Anywhere, you first need to log in to Cisco Secure Endpoint to create the API credentials.

To get the API credentials from Cisco Secure Endpoint

Follow the Cisco documentation on how to create API credentials to obtain the third-party API client identification and API key.

Connecting the Cisco Secure Endpoint App in USM Anywhere

After you obtain the credentials, you must configure the connection within USM Anywhere.

To enable the AlienApp for Cisco Secure Endpoint

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. In the EndPoint Host URL section, click the dropdown and select the appropriate URL for your region:
   - **api.amp.cisco.com** – North America region
   - **api.apjc.amp.cisco.com** – Asia Pacific, Japan, and China regions
   - **api.eu.amp.cisco.com** – Europe region
7. Enter your information into the following fields:
   - Client ID
   - API Key
8. In the **Event Type ID** field, you can specify the event types (separated by a comma) you want the BlueApp for Cisco Secure Endpoint to collect.

   When the Event Type ID field is left blank, BlueApp for Cisco Secure Endpoint collects all event types. See the Cisco Secure Endpoint documentation for more details on event types.
9. Click **Save**.
10. Verify the connection.

    After USM Anywhere completes a successful connection to the Cisco Secure Endpoint Representational State Transfer (REST) APIs, a icon displays in the Health column.

    If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Cisco Secure Endpoint connection.

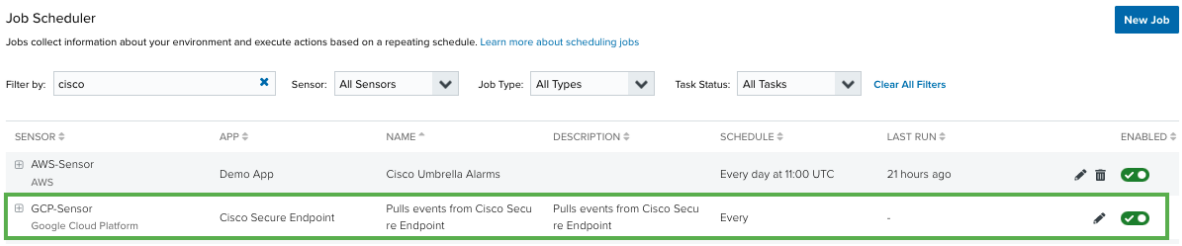
Cisco Secure Endpoint Event Collection

Once the BlueApp for Cisco Secure Endpoint has been configured, you can choose to have USM Anywhere collect Cisco Secure Endpoint events from the app on an hourly basis.

To configure Cisco Secure Endpoint event collection

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the Cisco Secure Endpoint app on the sensor it was deployed to.
3. In the enabled column, click the icon for the inactive Cisco Secure Endpoint events job.

   The icon turns green and hourly event collection from Cisco Secure Endpoint is enabled.



4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Cisco Secure Endpoint Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use the information to trigger actions in your Cisco Secure Endpoint environment. Rather than manually isolating or unisolating hosts, you can use the BlueApp for Cisco Secure Endpoint response actions to automatically respond to events detected in your USM Anywhere environment to isolate potential threats. The following table lists the available actions from the BlueApp.

Important: To protect against unintended consequences, BlueApp for Cisco Secure Endpoint only isolates single hosts; running the action against events or alarms with multiple hosts will not isolate any hosts.

Actions for the BlueApp for Cisco Secure Endpoint

Action	Description
Isolate Hosts Using FileHash	Run this action to isolate a host based on the FileHash identified.
Isolate Hosts Using Source IP	Run this action to isolate a host based on the source IP address identified.
Isolate Hosts Using Destination IP	Run this action to isolate a host based on the destination IP address identified.
Unisolate Hosts Using FileHash	Run this action to unisolate a host based on the FileHash identified.
Unisolate Hosts Using Source IP	Run this action to unisolate a host based on the source IP address identified.
Unisolate Hosts Using Destination IP	Run this action to unisolate a host based on the destination IP address identified.

Note: Before launching a Cisco Secure Endpoint response action or creating a Cisco Secure Endpoint response action rule, the BlueApp for Cisco Secure Endpoint must be enabled and connected to your Cisco Secure Endpoint instance. See Configuring the BlueApp for Cisco Secure Endpoint for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch a Cisco Secure Endpoint response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Cisco Secure Endpoint Action**.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
5. Modify the information for the action for the following fields:
   - Sensor
   - App Action
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Cisco Secure Endpoint Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Cisco Secure Endpoint response action when events, alarms, or vulnerabilities match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically triggers an action in your Cisco Secure Endpoint environment when malware is detected so that a member of your response team can manage and address the issue.

After you create a rule, new events, alarms, or vulnerabilities that match the rule conditions will trigger the Cisco Secure Endpoint response action. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

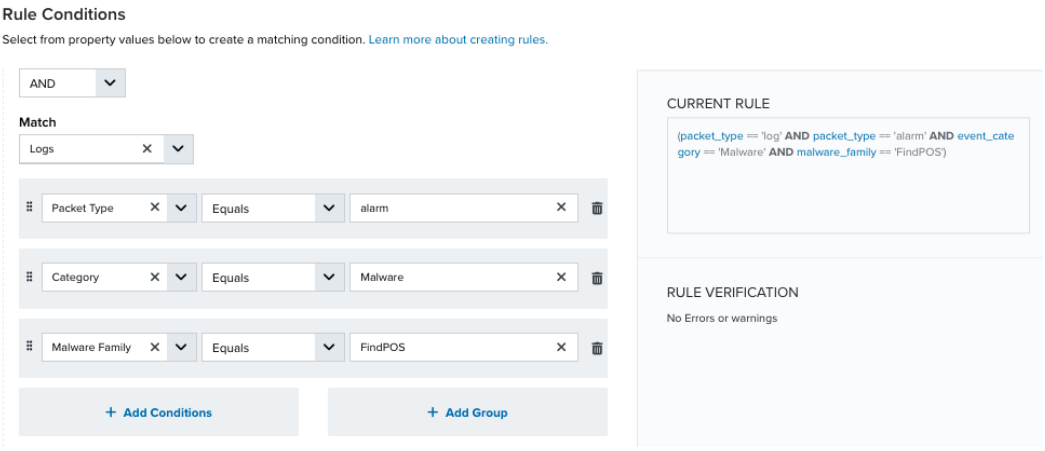
You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new Cisco Secure Endpoint response action rule

1. Enter a name for the rule.
2. Select the **Sensor**.
3. Select the **App Action** for the rule.
4. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions

for the rule.

- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not

trigger.

5. Click **Save Rule**.
6. In the confirmation dialog box, click **OK**.

BlueApp for Cisco Secure Firewall ASA

The BlueApp for Cisco Secure Firewall Adaptive Security Appliance (ASA) combines Cisco's firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities with your USM Anywhere environment. The BlueApp for Cisco Secure Firewall ASA helps enhance your preventative threat defense capabilities in USM Anywhere to stop attacks before they spread through the network.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Cisco Secure Firewall ASA

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the BlueApp for Cisco Secure Firewall Adaptive Security Appliance (ASA) in USM Anywhere, you need to perform the following steps in you Cisco Secure Firewall ASA environment:

- Download and install the Cisco Secure Firewall ASA Representational State Transfer (REST) API agent.
- Enable the REST API agent.
- Create a Cisco Secure Firewall ASA user profile with a privilege level of 15 to be able to communicate with USM Anywhere.

To install and configure the Cisco Secure Firewall ASA REST API agent

1. Follow the steps listed in Install and Configure the Secure Firewall ASA REST API Agent and Client from the Cisco Secure Firewall ASA REST API Quick Start Guide.
2. Open the command-line interface (CLI), and enter the following:

```
username <USER_NAME> password <PASSWORD> privilege 15
```

This creates the user account with a privilege level 15.

To enable BlueApp for Cisco Secure Firewall ASA in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Cisco Secure Firewall ASA Management IP Address or Host Name, Port, Username, and Password.
7. (Optional.) Select **Require CA certificate** and **Validate HTTPS host name** if you want to use this option, and then enter the certificate authority (CA) certificate.
8. Click **Save**.
9. Verify the connection.

   After USM Anywhere completes a successful connection to the Cisco Secure Firewall ASA REST APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Cisco Secure Firewall ASA connection.

Forward Cisco Secure Firewall ASA Syslog Messages to USM Anywhere

To fully integrate USM Anywhere with the BlueApp for Cisco Secure Firewall ASA, you need to configure syslog forwarding in the Cisco Secure Firewall ASA device to send the logs to your sensor. You can use the Cisco Adaptive Security Device Manager (ASDM) to enable logging and send all the syslog messages to the USM Anywhere Sensor IP address. See ASA 8.2: Configure Syslog using ASDM for detailed instructions from the vendor.

Assign Your Assets

Because the AlienApp for Cisco ASA is not auto-discovered, you must manually assign the BlueApp to the asset representing the Cisco ASA device or management server's IP address in USM Anywhere. If the BlueApp isn't assigned to any assets, the Cisco ASA events will be handled by the LevelBlue Generic Data Source, which will result in some of the data from the log not being properly parsed or associated with the BlueApp.

See Assign Assets to BlueApps for instructions on how to assign your assets to AlienApp for Cisco ASA.

BlueApp for Cisco Secure Firewall ASA Actions

With the BlueApp for Cisco Secure Firewall Adaptive Security Appliance (ASA) configured with USM Anywhere, you can respond to threats or suspicious activity by sending IP addresses directly to your Cisco environment. The following table lists the available actions from the BlueApp.

Actions for the AlienApp for Cisco Secure Firewall ASA

Action	Description
Tag Source IP from Event	Run this action to label the source IP address based on an event
Tag Destination IP from Event	Run this action to label the destination IP address based on an event
Tag Source IP from Alarm	Run this action to label the source IP address based on an alarm
Tag Destination IP from Alarm	Run this action to label the destination IP address based on an alarm

Actions for the AlienApp for Cisco Secure Firewall ASA (Continued)

Action	Description
Tag Source IP Address from Rule	Run this action to label the source IP address based on a predefined rule
Tag Destination IP Address from Rule	Run this action to label the destination IP address based on a predefined rule
Remove Tag from Source IP Address	Run this action to remove a tag from the source IP address
Remove Tag from Destination IP Address	Run this action to remove a tag from the destination IP address based on an event
Remove Tag from Source IP from Alarm	Run this action to remove a tag from the source IP address associated with an alarm
Remove Tag from Destination IP from Alarm	Run this action to remove a tag from the destination IP address associated with an alarm

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

When reviewing an alarm originated from a Cisco Secure Firewall ASA event, should you conclude that the Cisco Secure Firewall ASA user account has been compromised, you can launch an action to inactivate the Cisco Secure Firewall ASA user account associated with that alarm. If you want to apply the action to similar alarms that occur in the future, you can create an orchestration rule after you apply the action.

To launch a Cisco Secure Firewall ASA response action

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Cisco Secure Firewall ASA Action** and enter the Cisco Secure Firewall ASA Group Name and Group Description.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

   Additionally, you can choose to clear the active IP connections by selecting the **Clear Active Connections** checkbox.
5. Click **Run**.

   After USM Anywhere initiates the action for the alarm, it displays a confirmation dialog box.

Creating Cisco Secure Firewall ASA Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Cisco Secure Firewall Adaptive Security Appliance (ASA) response action when events, alarms, or vulnerabilities match the criteria that you specify.

After you create a rule, if there are new events, alarms, or vulnerabilities that match the conditions, they will trigger the Cisco Secure Firewall ASA response action to create a new incident. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new Cisco Secure Firewall ASA response action rule

1. Enter a name for the rule and select the sensor.
2. Select the action to tag either a source or destination IP address and enter the Cisco Secure Firewall ASA Group Name and Group Description.

   Additionally, you can choose to clear the active IP connections with the **Clear Active Connections** checkbox.

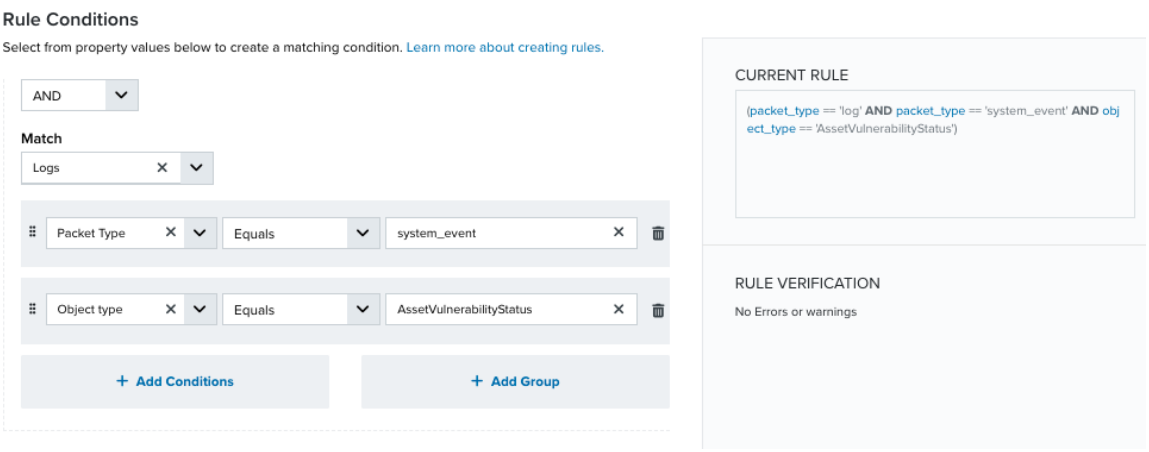
   - Create a New Incident from a Vulnerability Status Update

     This is the default action if you create the rule after applying a Cisco Secure Firewall ASA response action to a vulnerability.

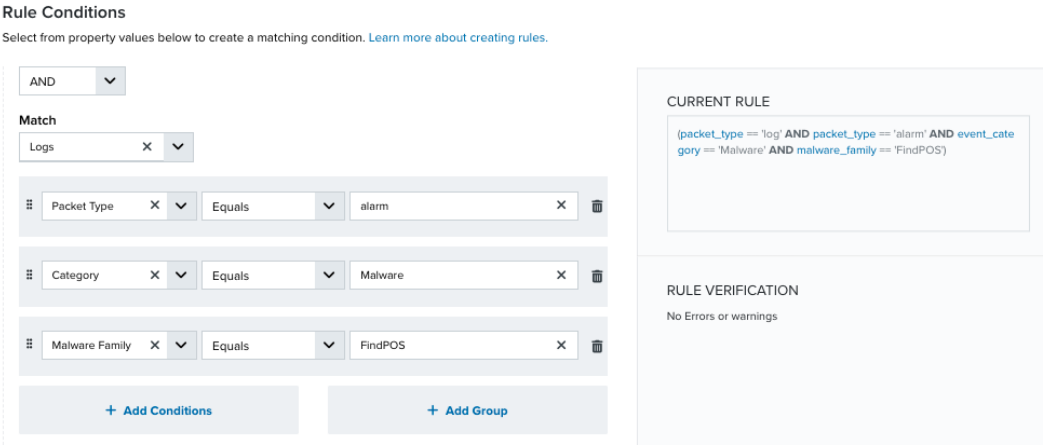
     Important: To match vulnerability status updates, your rule must include the following criteria: `(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus')`.

     However, it is important to be aware that this will return all vulnerability status changes matching these rules. It is advisable to narrow the rule with further conditions. Additionally, you can create a similar alarm rule first to test the amount of responses it would generate when active before you use the rule to

create Cisco Secure Firewall ASA rules.



3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Cisco Umbrella

Cisco Umbrella (formerly known as OpenDNS) is a cloud-delivered secure internet gateway that stops current and emergent threats over all ports and protocols. It blocks access to malicious domains, URLs, IPs, and files before a connection is established or a file is downloaded.

The BlueApp for Cisco Umbrella provides functional support to easily ingest data from Cisco Umbrella to USM Anywhere for analysis, and to enable orchestration for triggering actions within Cisco Umbrella based on risks identified in USM Anywhere.

The BlueApp leverages two features from Cisco Umbrella:

- **Amazon Simple Storage Service (S3) log management**: The BlueApp collects Cisco Umbrella logs through an Amazon S3 bucket.
- **Enforcement API**: The BlueApp sends response actions to Cisco Umbrella based on the malicious records identified by USM Anywhere.

Note: As the BlueApp for Cisco Umbrella relies on Amazon S3 buckets, it is only compatible if your sensor is deployed in an AWS environment.

All three new Cisco Umbrella packages, *DNS Security Essentials*, *DNS Security Advantage*, and *Secure Internet Gateway (SIG) Essentials*, support both features. Therefore, BlueApp for Cisco Umbrella should work regardless which package you have. See the vendor website for more information about the Cisco Umbrella product packages.

Note: If you are using the old Cisco Umbrella packages (*Professional*, *Insights*, and *Platform*), only the Platform package supports both features. The Insights package does not support Enforcement API, while the Professional package does not support either. Therefore, to fully integrate with the BlueApp, you need to have the Platform package.

Edition: The BlueApp for Cisco Umbrella response actions are available in the Standard and Premium editions of USM Anywhere.

See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Collecting Logs from Cisco Umbrella

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

To fully integrate USM Anywhere with your Cisco Umbrella (formerly, OpenDNS) implementation, you should configure log collection so that USM Anywhere can retrieve and normalize raw log data from Cisco Umbrella. The combination of the Cisco Umbrella data source integration and configuration of the BlueApp for Cisco Umbrella provides a full scope of data and analysis within USM Anywhere.

Important: The BlueApp collects logs through an Amazon Simple Storage Service (S3) bucket. Therefore, you must have a Cisco Umbrella package that supports Amazon S3 log management. See Cisco Umbrella Packages page for more information.

Amazon S3 Log Management

Before USM Anywhere can collect the Cisco Umbrella log data, you must set up Amazon S3 log management in your Cisco Umbrella deployment. This requires that you have a self-managed Amazon S3 bucket in an AWS account that is configured to accept uploads from the Cisco Umbrella Service. See the Cisco Umbrella Documentation Enable Logging to Your Own S3 Bucket for detailed information about this configuration.

Note: USM Anywhere currently does not support the Cisco-managed buckets in Amazon S3.

To verify Amazon S3 log management in Cisco Umbrella

1. Log in to the Cisco Umbrella (OpenDNS) dashboard.
2. Go to **Settings > Log Management**.
3. Click **Amazon S3**.
4. In the Bucket Name field, enter the exact Amazon S3 bucket name.
5. Click **Verify**.

   A confirmation message in the dashboard indicates that the bucket has been successfully verified.

Scheduling Log Collection

After you verify that Cisco Umbrella is configured to send log data to an Amazon S3 bucket for an account where you have a deployed USM Anywhere Sensor, you can set up a log collection job for USM Anywhere to retrieve that data.

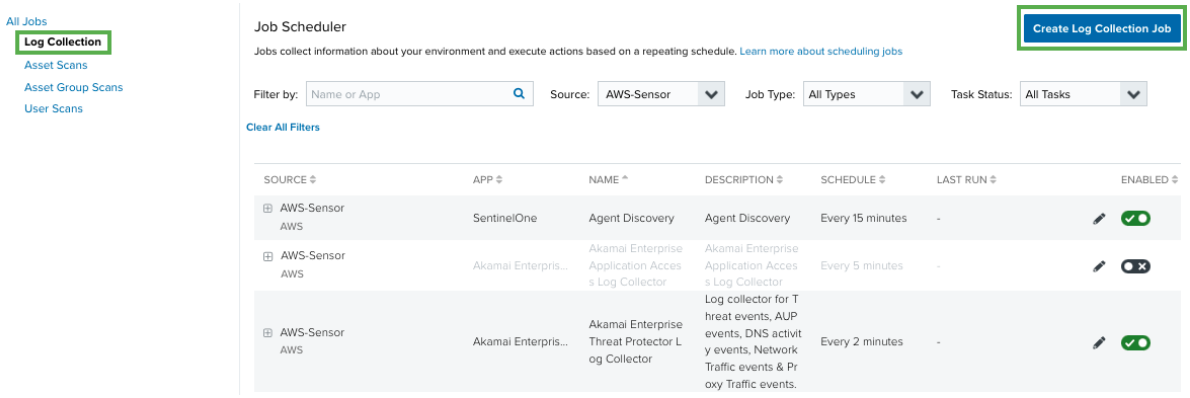
Note: If you want to deploy a sensor to facilitate Cisco Umbrella log collection, see About AWS Sensor Deployment in the *USM Anywhere Deployment Guide*.

To schedule Cisco Umbrella log collection

1. Go to **Settings > Scheduler**.
2. In the left navigation menu, click **Log Collection**.

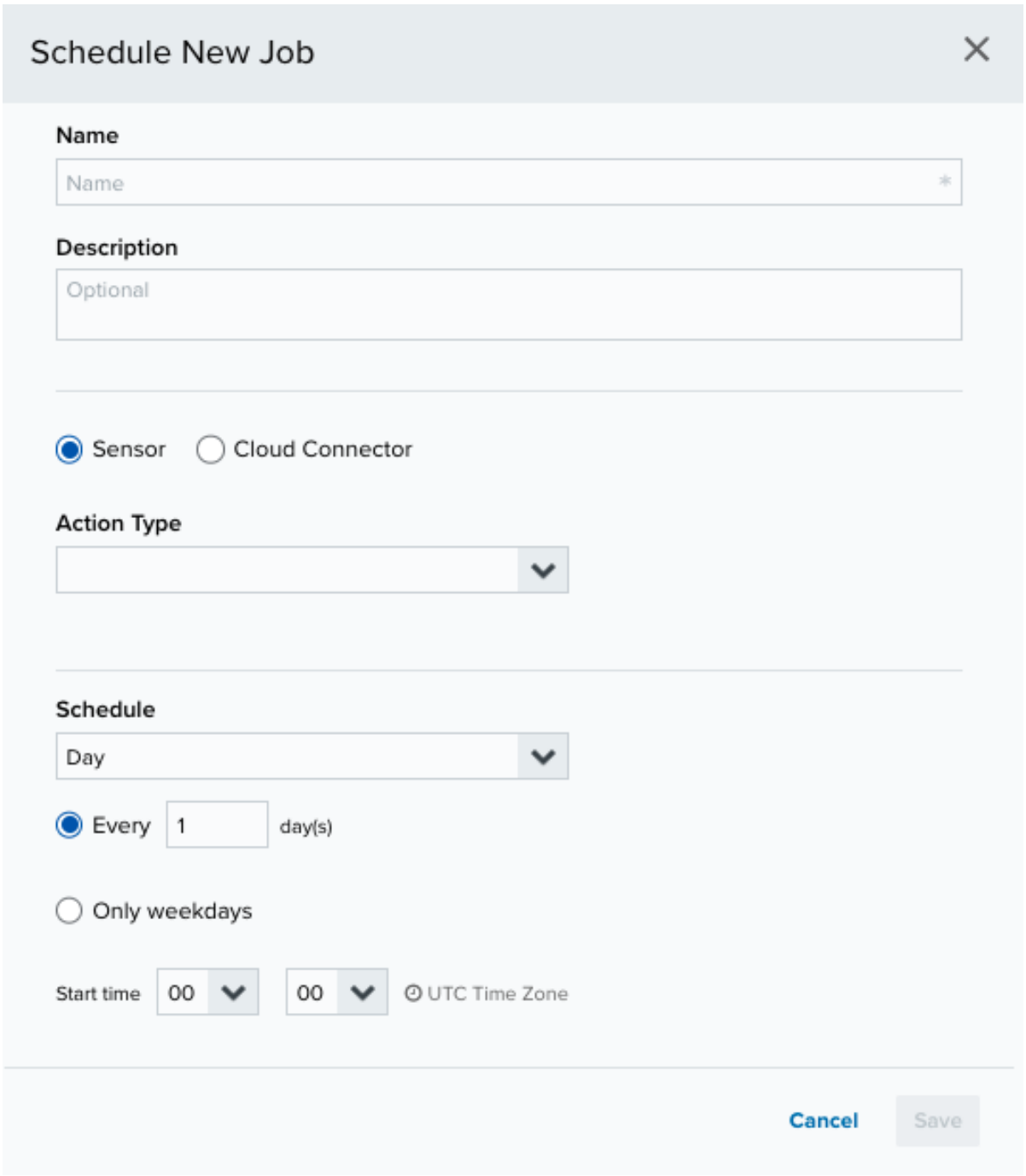
   Note: You can use the Sensor filter at the top of the list to review the available log collection jobs on your AWS Sensor.

3. Click **Create Log Collection Job**.



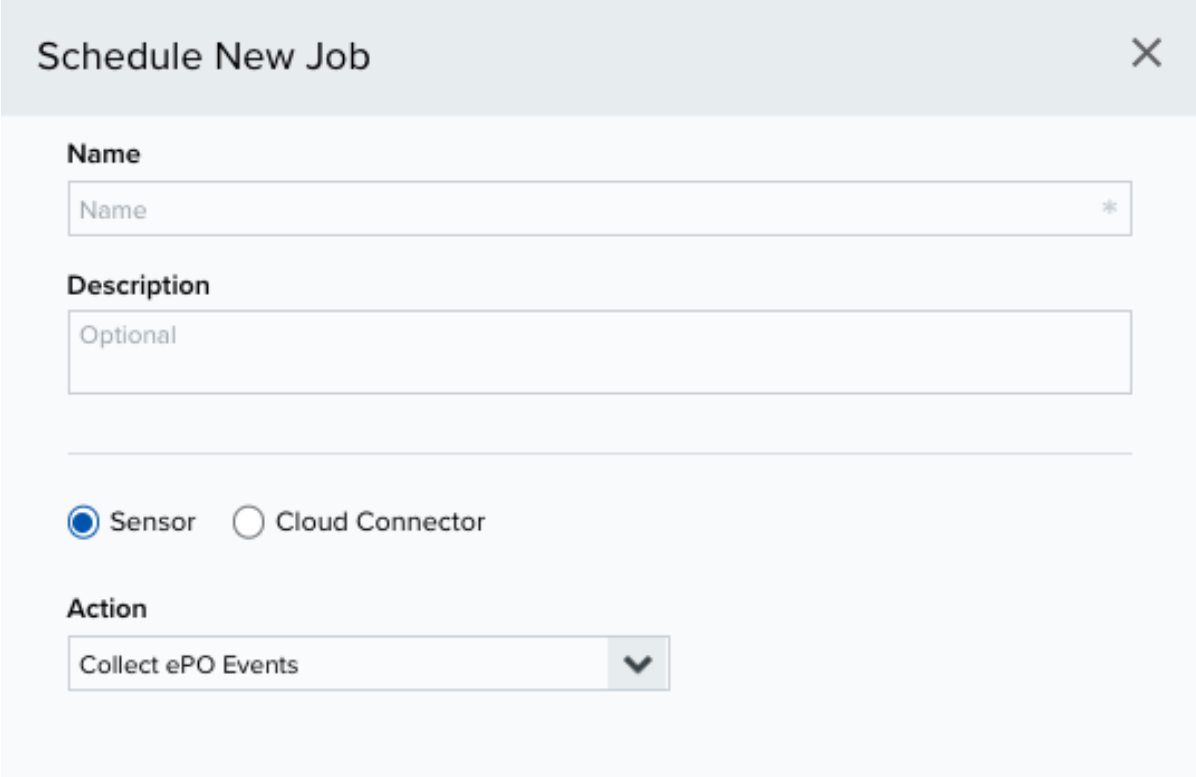
Note: If you have recently deployed a new USM Anywhere Sensor, it can take up to 20 minutes for USM Anywhere to discover the various log sources. After it discovers the logs, you must manually enable the AWS log collection jobs you want before the system collects the log data.

The Schedule New Job dialog box opens.

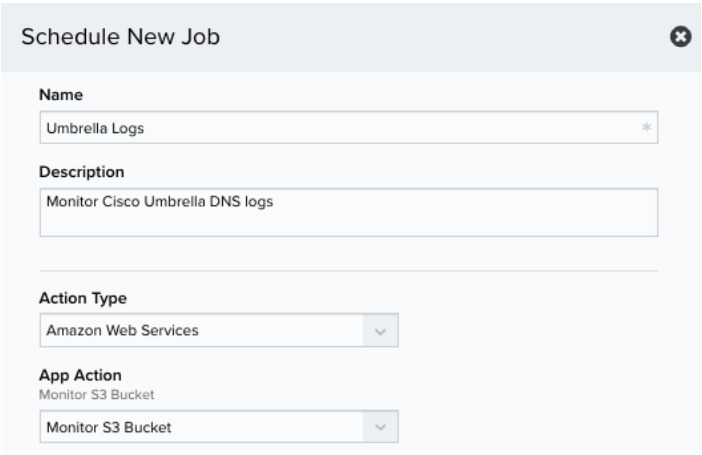


4. Enter the name and description for the job.

   The description is optional, but it is a best practice to provide this information so that others can easily understand what it does.

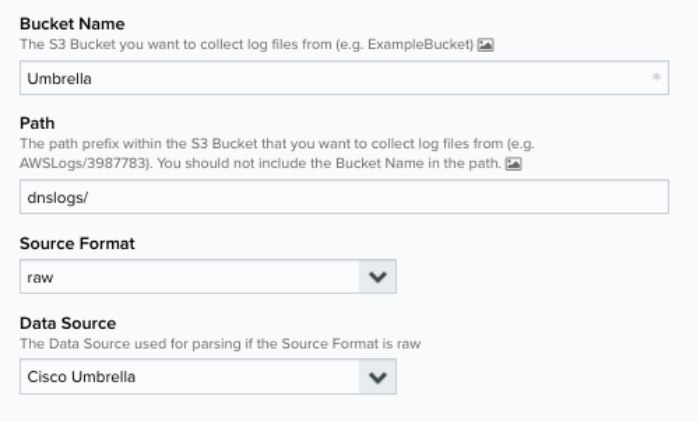


5. For the Action Type option, select **Amazon Web Services**.
6. If you have more than one deployed USM Anywhere Sensor, select the Sensor on which the job should run.
7. For the App Action option, select **Monitor S3 bucket**.



8. In the Bucket Name field, enter the name of the Amazon S3 bucket that is configured in Cisco Umbrella log management.

9. In the Path field, enter the path on the bucket where the logs reside (in this case, `dns-logs/`).
10. For the Source Format option, select **raw**.
11. For the Data Source option, select **Cisco Umbrella**.

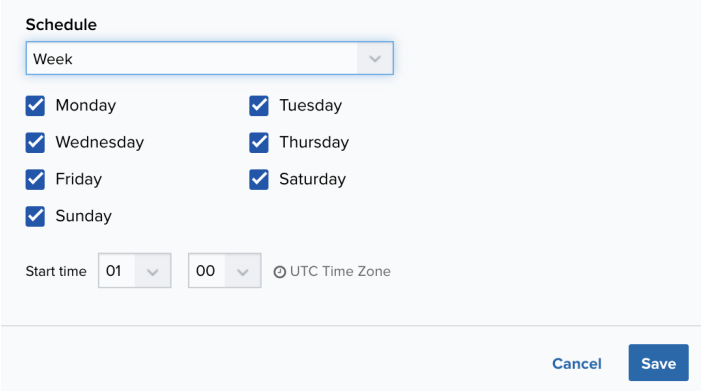


12. In the Schedule section, specify when USM Anywhere runs the job:
    a. Select the increment as **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

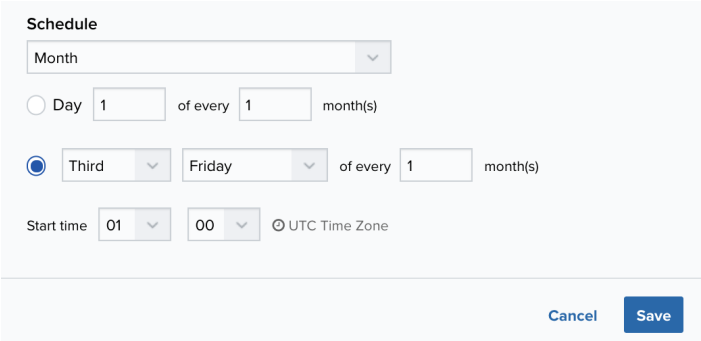
> **Warning:** After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See USM Anywhere System Monitor for more information.

    b. Set the interval options for the increment.

    The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.



Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.



Important: USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

c. Set the start time.

   This is the time that the job starts at the specified interval. It uses the time zone configured for your USM Anywhere instance (the default is Coordinated Universal Time [UTC]).

13. Click **Save**.

    You should start seeing new Cisco Umbrella events in USM Anywhere shortly after the initial raw log data collection and normalization.

Configuring the BlueApp for Cisco Umbrella

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

When the BlueApp for Cisco Umbrella is connected to your Cisco Umbrella environment, you can launch app actions and create orchestration rules to send data from USM Anywhere to Cisco Umbrella. See BlueApp for Cisco Umbrella Actions for more information about the orchestration actions supported by the BlueApp for Cisco Umbrella.

For example, you might create a rule where USM Anywhere automatically sends the URLs of suspicious domains that it identifies to Cisco Umbrella. See Creating Cisco Umbrella Response Action Rules for information about adding these types of orchestration rules for the BlueApp.

Note: To fully integrate USM Anywhere with your Cisco Umbrella implementation, you should also have the Cisco Umbrella log collection enabled so that USM Anywhere can retrieve and normalize raw log data from Cisco Umbrella. See Collecting Logs from Cisco Umbrella for information about raw log data retrieval.

Creating a Cisco Umbrella Integration

Before you can use the Cisco Umbrella orchestration actions within USM Anywhere, you must establish an integration point in your Cisco Umbrella console to be used by USM Anywhere.

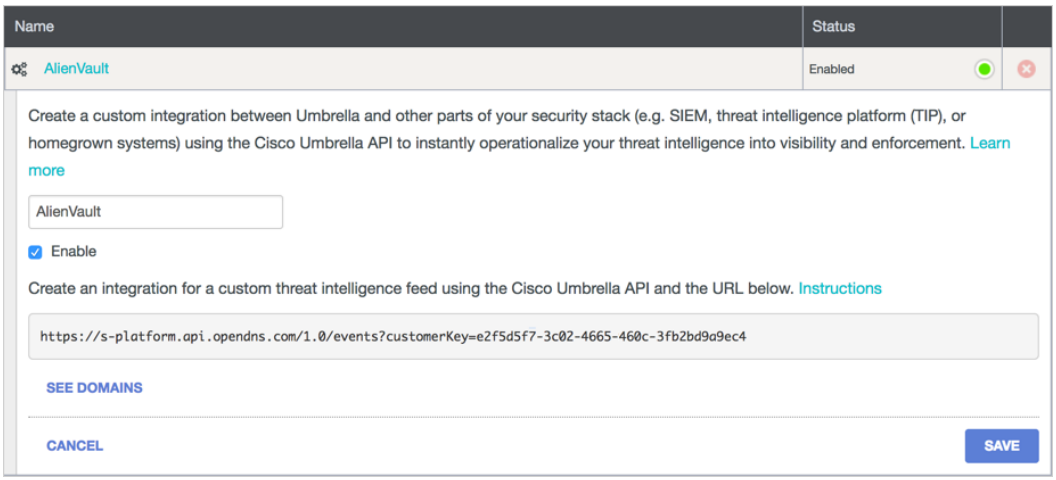
Note: You must have a Cisco Umbrella package that supports the Enforcement API.

To add an integration in Cisco Umbrella

1. Open your Cisco Umbrella dashboard and go to **Policies > Policy Components > Integrations**.
2. At the top of the page, click the icon.
3. Add a name for the custom integration, and click **Create**.
4. Click the new custom integration to expand it and display the details.
5. Select the **Enable** checkbox.
6. Copy the customer key value displayed in the integration URL to be entered in USM Anywhere.

   In the following example, the value to copy is `e2f5d5f7-3c02-4665-460c-3fb2bd9a9ec4`:

   ```
   https://s-platform.api.opendns.com/1.0/events?customerKey=e2f5d5f7-3c02-4665-460c-3fb2bd9a9ec4
   ```



7. Click **Save**.

Configuring the BlueApp for Cisco Umbrella Connection

After you create the Cisco Umbrella integration and copy the key value, you're ready to establish the BlueApp for Cisco Umbrella connection in USM Anywhere. The USM Anywhere Sensor that you use to configure the BlueApp must have connectivity to the Umbrella Enforcement API at https://s-platform.api.opendns.com.

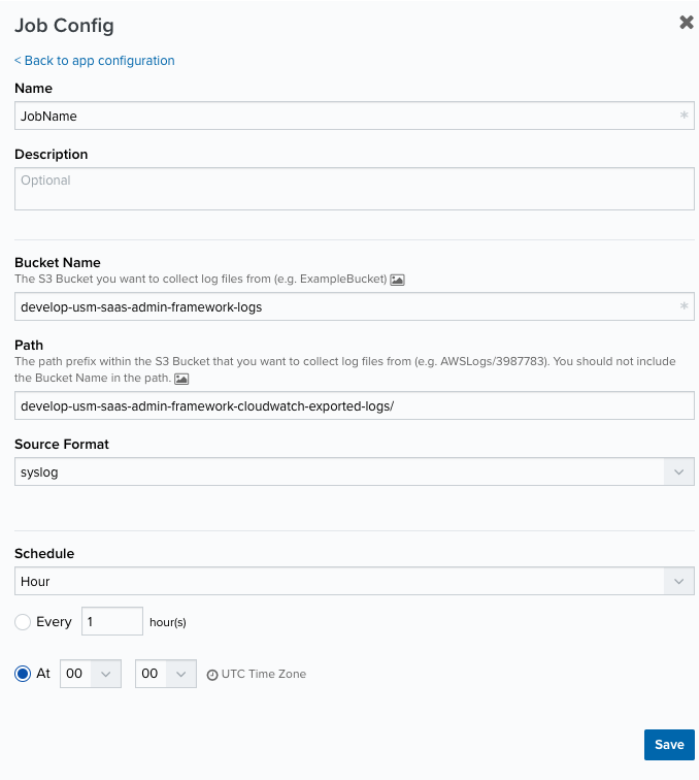
To enable the BlueApp for Cisco Umbrella

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Paste the `customerKey` value you copied in the previous task into the Customer Key field.
7. Click **Next**.

   Note: The Next button is only available for AWS Sensors.
8. Enter a name to identify the job.

9. (Optional.) Enter a description for the job.
10. In the Bucket Name field, enter the Amazon Simple Storage Service (S3) bucket name from which you want to collect files.
11. In the Path field, enter the path prefix within the Amazon S3 bucket from which you want to collect log files.
12. In the Schedule field, set a frequency for the job to run.



13. Click **Save**.
14. Verify the connection.

    After USM Anywhere completes a successful connection to the Cisco Umbrella APIs, a icon displays in the Health column.

    If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Cisco Umbrella connection.

BlueApp for Cisco Umbrella Actions

With the BlueApp for Cisco Umbrella, USM Anywhere can pass malicious domains to Cisco Umbrella instantly — through a user-executed action or an automated rule — to coordinate threat detection and response in a single action. The bidirectional capabilities of the BlueApp for Cisco Umbrella enable USM Anywhere to incorporate data from Cisco Umbrella (see Collecting Logs from Cisco Umbrella) into its threat analysis and orchestrate response actions by passing malicious domains identified by USM Anywhere to Cisco Umbrella.

Note: For the BlueApp to send response actions, you must have a Cisco Umbrella package that supports the Enforcement API. See the vendor website for more information about the Cisco Umbrella product packages.

Important: Using the BlueApp for Cisco Umbrella orchestration actions requires that the BlueApp is enabled on a deployed USM Anywhere Sensor with a configured integration to your Cisco Umbrella account. See Configuring the BlueApp for Cisco Umbrella for more information.

As USM Anywhere surfaces events and alarms, your team determines which items require a response action. Rather than manually updating the domains list within Cisco Umbrella for enforcement purposes, you can use the BlueApp for Cisco Umbrella orchestration actions to enforce protection based on domains associated with the event or alarm. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Cisco Umbrella

Action	Description
Report names found on an alarm	Run this action to send the alarm information to your Cisco Umbrella environment. This action is available only when you launch an app action directly from an alarm.
Report by a HTTP hostname found on an event	Run this action to send the HTTP hostname associated with an event to your Cisco Umbrella environment. This action is available when you launch an app action in an orchestration rule.

Actions for the BlueApp for Cisco Umbrella (Continued)

Action	Description
Report by an URL found on an event	Run this action to send the URL associated with an event to your Cisco Umbrella environment. This action is available when you launch an app action in an orchestration rule.
Report by a DNS record found on an event	Run this action to send the DNS associated with an event to your Cisco Umbrella environment. This action is available when you launch an app action in an orchestration rule.

If it passes validation (for example, it's unknown and safe to block), Cisco Umbrella adds it to a destination list associated with that custom integration and surfaces the item within the Umbrella dashboard as a custom security category.

To view information about these actions in USM Anywhere

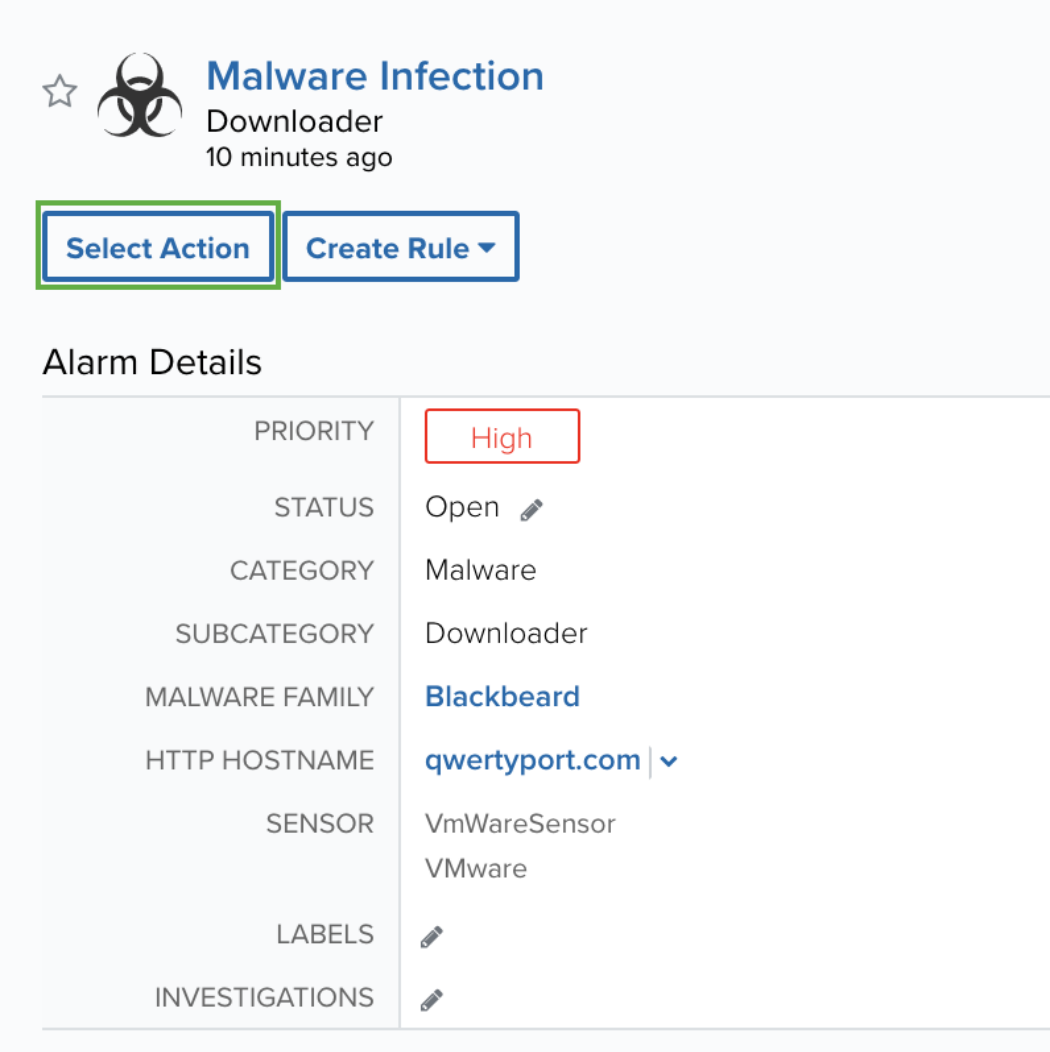
1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

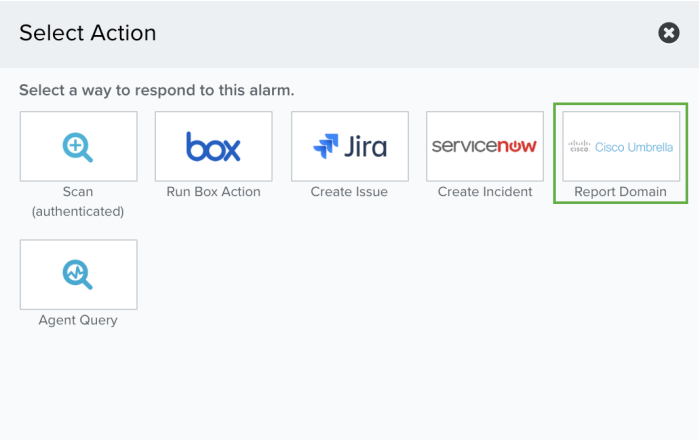
If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch a Cisco Umbrella orchestration action for an alarm or event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.



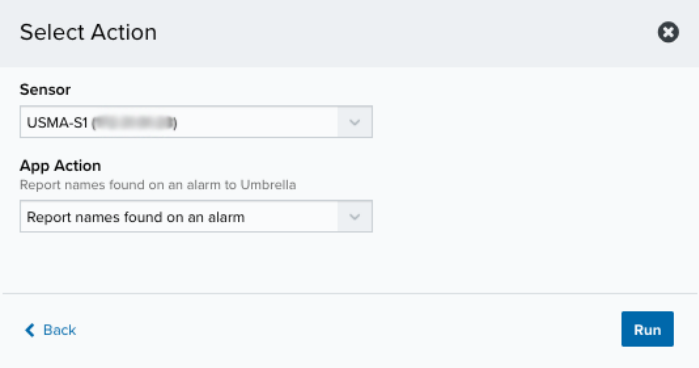
4. In the Select Action dialog box, select the **Cisco Umbrella** tile.



This displays the options for the selected response app. It automatically sets the App Action to **Report names found on an alarm**.

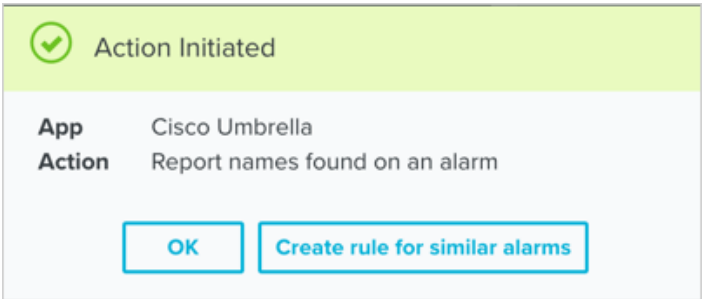
Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

5. If you have more than one sensor installed, select the sensor where the BlueApp for Cisco Umbrella is enabled.



6. Click **Run**.

After USM Anywhere initiates the action, it displays a confirmation dialog box.



If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Cisco Umbrella Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

The BlueApp for Cisco Umbrella allows you to create orchestration rules that automatically send suspicious domains to your Cisco Umbrella environment. There are four actions you can trigger with orchestration rules to report domains to Cisco Umbrella when matching events or alarms occur:

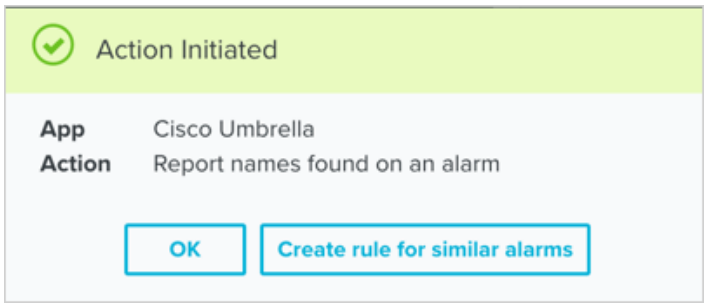
- Report by HTTP hostname on an event
- Report by URL on an event
- Report by Domain Name System (DNS) record on an event
- Report names found on an alarm

Before you can create an orchestration rule that triggers one of these actions, the BlueApp for Cisco Umbrella must be enabled and configured for a deployed USM Anywhere Sensor. For more information, see Configuring the BlueApp for Cisco Umbrella for Orchestration.

All rules include a rule name and conditional expression. They can also include optional multiple occurrence and window length parameters. There are multiple methods for creating a new BlueApp for Cisco Umbrella orchestration rule in USM Anywhere:

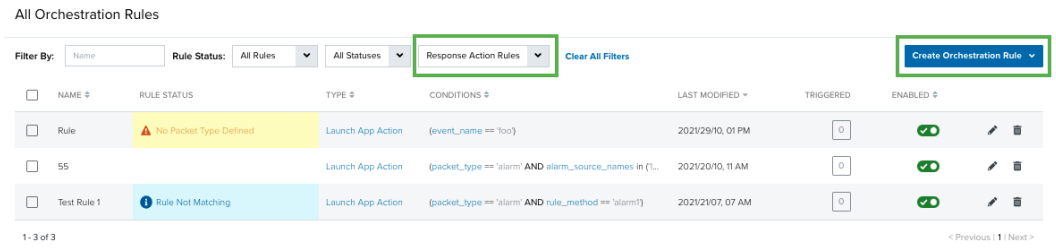
- **On the Rules tab of the BlueApp page**: This tab provides various tools that you can use to create and manage the orchestration rules that use the BlueApp for Cisco Umbrella actions. For easy rule creation, you can use a suggested rule as the basis for the new orchestration rule. This tab also provides a method to easily create a new rule based on your own matching criteria where the sensor and app are already selected, and displays all rules associated with the BlueApp so that you can easily enable or disable rules as needed.
- **From an Applied Response Action**: You can automatically create a rule using the response action that you apply to an existing alarm or event. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

  In the confirmation dialog box, click **Create rule for similar alarms** or **Create rule for similar events**.



- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click **Create Orchestration Rule > Response Action Rule** to define the new rule.



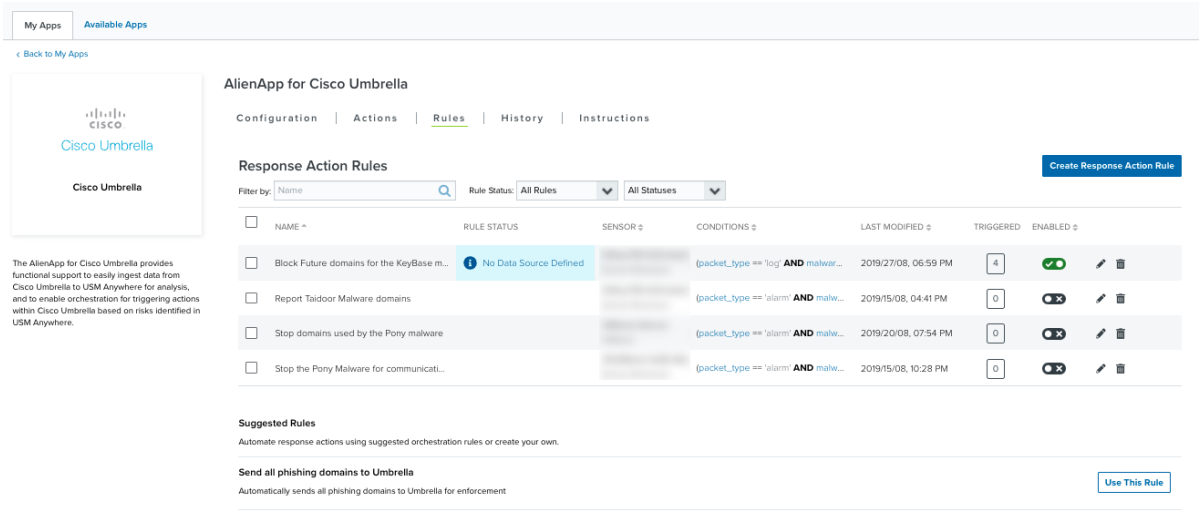
Depending on your Cisco Umbrella configuration and how it processes the domain information, these actions will result in events that USM Anywhere retrieves through Cisco Umbrella log collection.

Using a Suggested Rule

When you use one of the suggested rules, you can start with a set of matching criteria for common use cases, such as sending the HTTP hostname from phishing events to Cisco Umbrella.

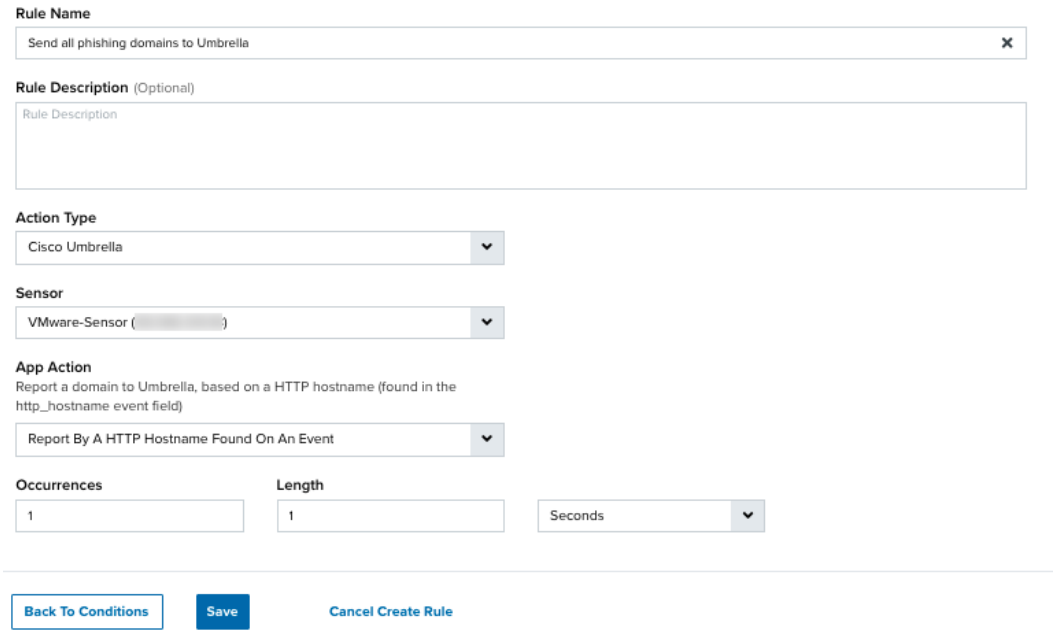
To create a new rule from a suggested rule

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Select the **Rules** tab.



5. Locate the rule that matches your use case and click **Use this Rule**.

   This opens the Create Rule dialog box with preconfigured options for the new rule. You can keep these options exactly as they are, or make some changes according to your specific needs.



6. (Optional.) Modify any of default rule settings, if needed:

- Change the name of the rule.
- Select a different Action.
- Add one or more Rule Condition items to narrow the scope for a matching event or alarm.
- Include a multiple occurrence parameter (click the **More** link to display the fields).

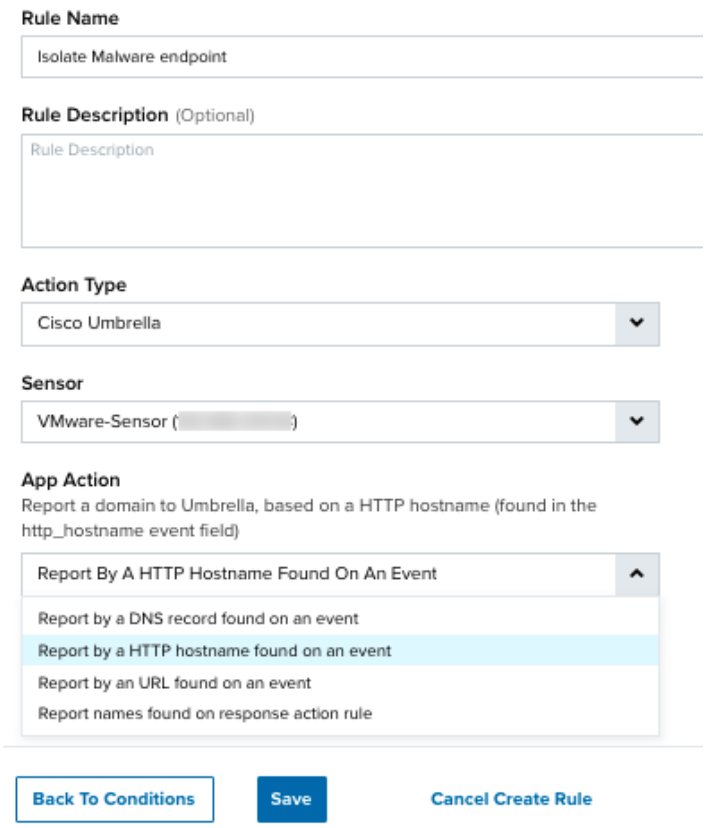
7. Click **Save Rule**.

Defining the Response Action Rule

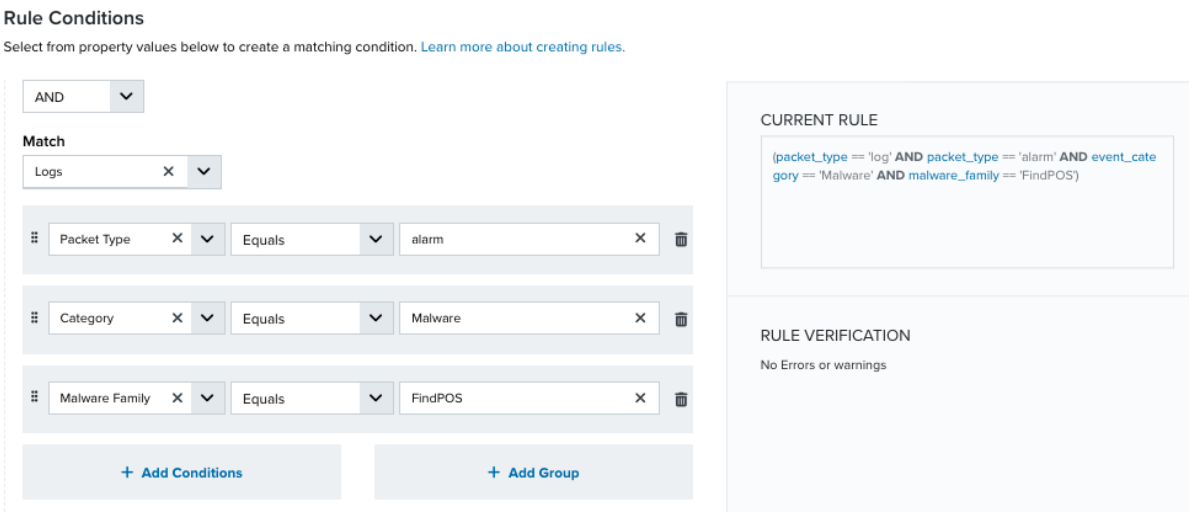
Use the Create Rule dialog box to specify the new rule, including the Cisco Umbrella action to run and the criteria for a matching event or alarm that triggers the rule.

To define a Cisco Umbrella response action rule

1. Enter a unique name for the rule.
2. Select the App Action for the rule.



3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.

Viewing Alarms with Applied Cisco Umbrella Response Actions

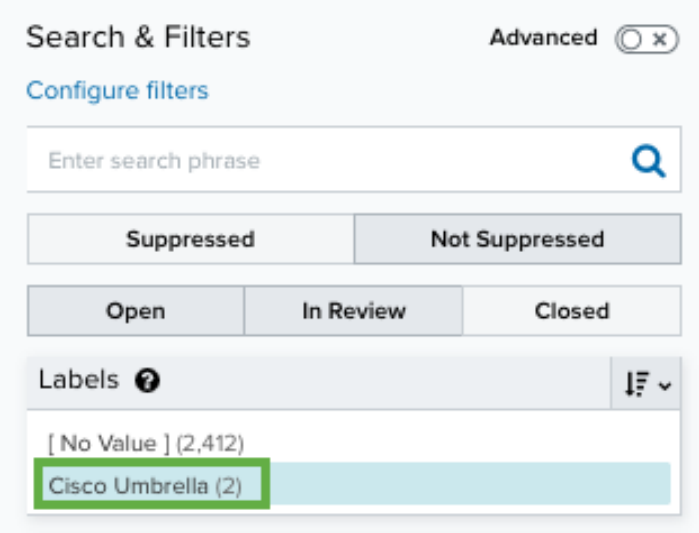
Role Availability ✔ Read-Only ✔ Investigator ✔ Analyst ✔ Manager

USM Anywhere uses labels as a mechanism to classify alarms. These labels make it easy to filter items by an applied label so that you can locate them easily and track their status. When the BlueApp for Cisco Umbrella executes a response action for an alarm, it automatically applies the **Cisco Umbrella** label to it. You can select this label as a filter so that a page displays data for only the items related to an BlueApp for Cisco Umbrella response action.

To view alarms with applied Cisco Umbrella response actions

1. Open the Alarms page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

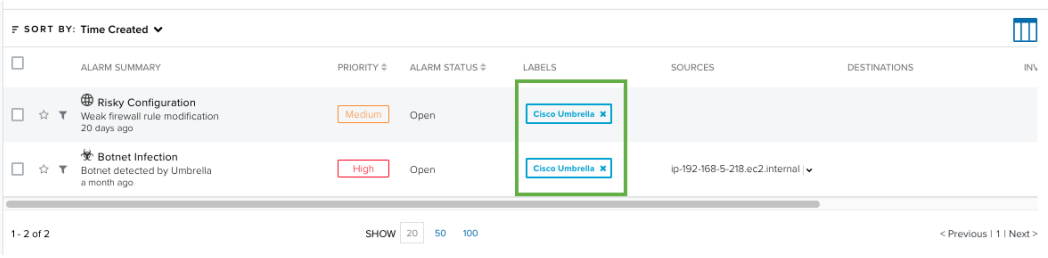
   USM Anywhere includes several filters displayed by default.
3. Locate the Labels filter and select the **Cisco Umbrella** label.



If the Labels filter is not displayed, click **Configure Filters** at the bottom of the Search & Filters pane to configure filters for the page. See Managing Filters in the *USM Anywhere*

User Guide for more information about configuring filters for the page display.

In the displayed list, you can scroll the list to the right and view the Labels column.



BlueApp for Cloudflare

The BlueApp for Cloudflare enhances the capabilities of USM Anywhere by collecting and analyzing log data from Cloudflare Enterprise, which provides optimization and protection for websites, APIs, software as a service (SaaS), and other resources connected to the Internet. With a configured BlueApp for Cloudflare, you can monitor your Cloudflare activity and detect threats directly from USM Anywhere, providing a single pane of glass for all your security monitoring and compliance needs.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Cloudflare

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

Cloudflare Enterprise customers have access to the Cloudflare Logs service, which is a REpresentational State Transfer (REST) API used to consume request logs over HTTP. This REST API includes a method for accessing a domain's request logs using a client API key.

When the BlueApp for Cloudflare is enabled and connected to your Cloudflare Enterprise service, the predefined, scheduled job collects log data from Cloudflare every 20 minutes. After USM Anywhere collects and analyzes the first of these events, you can view them in the Events page.

Getting Your Cloudflare API Key

Before you can use the BlueApp for Cloudflare to collect and analyze Cloudflare log data within USM Anywhere, you must have an API key that can be used to connect to your Cloudflare service. Cloudflare issues an API key for a specific user account and all requests with that key act on behalf of that user.

To acquire the API key for Cloudflare

1. Go to the Cloudflare Managing API Tokens and Keys page and follow the View API Key instructions.
2. Copy the Global API Key value to be entered in USM Anywhere.

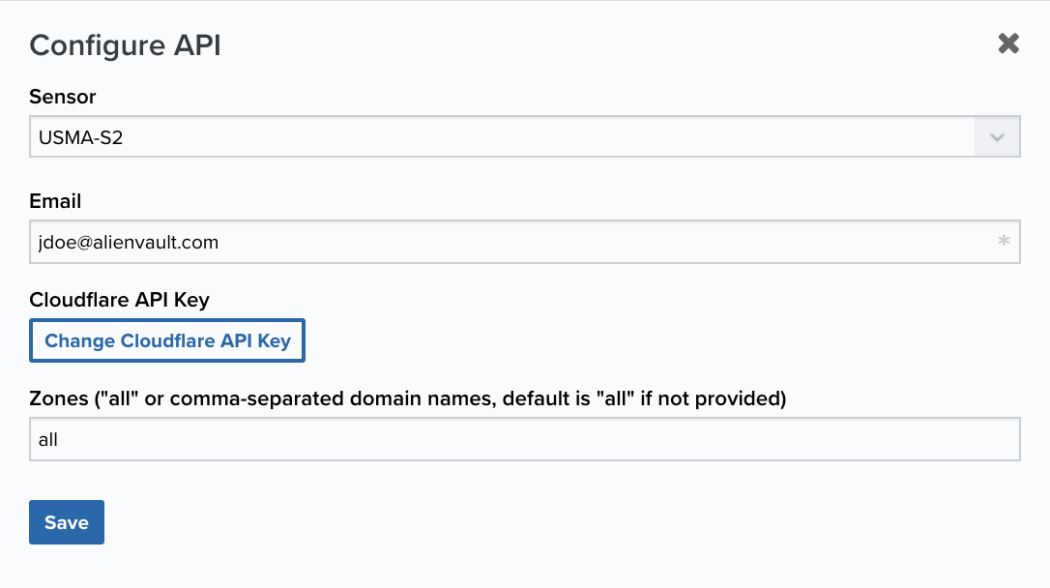
Enabling the BlueApp for Cloudflare API Connection

After you have your Cloudflare API key value, you're ready to enable the BlueApp for Cloudflare in USM Anywhere.

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the connection information for your Cloudflare service:



   - **Email:** Enter the email for the Cloudflare user account to use for API authentication.
   - **Cloudflare API Key**: Click **Change Cloudflare API Key** and enter the API key value associated with that user account.
   - **Zones**: (Optional.) If you want to limit the zones from which the BlueApp pulls data, list the identifications (IDs) you do want the app to pull from here. To pull from all zones, leave this field blank or enter **all**.
7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Cloudflare APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Cloudflare connection.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

Scaling BlueApp for Cloudflare Across Multiple Sensors

If you have multiple zones managed in Cloudflare and those zones are outputting so many events that they overwhelm the USM Anywhere Sensor, you may want to consider scaling your zones across multiple sensors. If you find that the BlueApp for Cloudflare is often entering throttling mode, this may be a sign that you should scale to multiple sensors. See Understanding the Status of the Cloudflare App for more information about throttling mode.

To distribute the load of your BlueApp for Cloudflare across multiple sensors, distribute your zones among the sensors such that no sensor should be receiving more than a total of 1000 events per second (EPS).

Note: If any single zone is producing 1000 EPS or more, its data will still be throttled to reduce the load. This scaling will not be able to prevent throttling due to a single zone's high EPS.

To configure your sensor to monitor specific zones

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. From the sensor drop-down list, select the first sensor you want to configure.
6. Enter the connection information for your Cloudflare service.
7. Configure the Zones field, list only the zones you want this sensor to monitor.
8. Go to to **Settings > Scheduler**, enable the *Collect Cloudflare events* job that corresponds to that sensor.
9. Repeat step 4 through 8 to configure anothor sensor to monitor a different zone.

Important: If you do not assign a zone to any sensor, it will not be monitored unless one of your sensors is configured to monitor all zones.

Managing Your Cloudflare Data Collection and Events

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

After you configure the BlueApp for Cloudflare and have a successful connection, you should make sure that the scheduled collection job is enabled. For each deployed sensor, USM Anywhere includes an out-of-the-box log collection job to support BlueApp for Cloudflare data collection. You can then use rules to manage the events that USM Anywhere generates and stores, as well as the alarms that it generates from specific types of events.

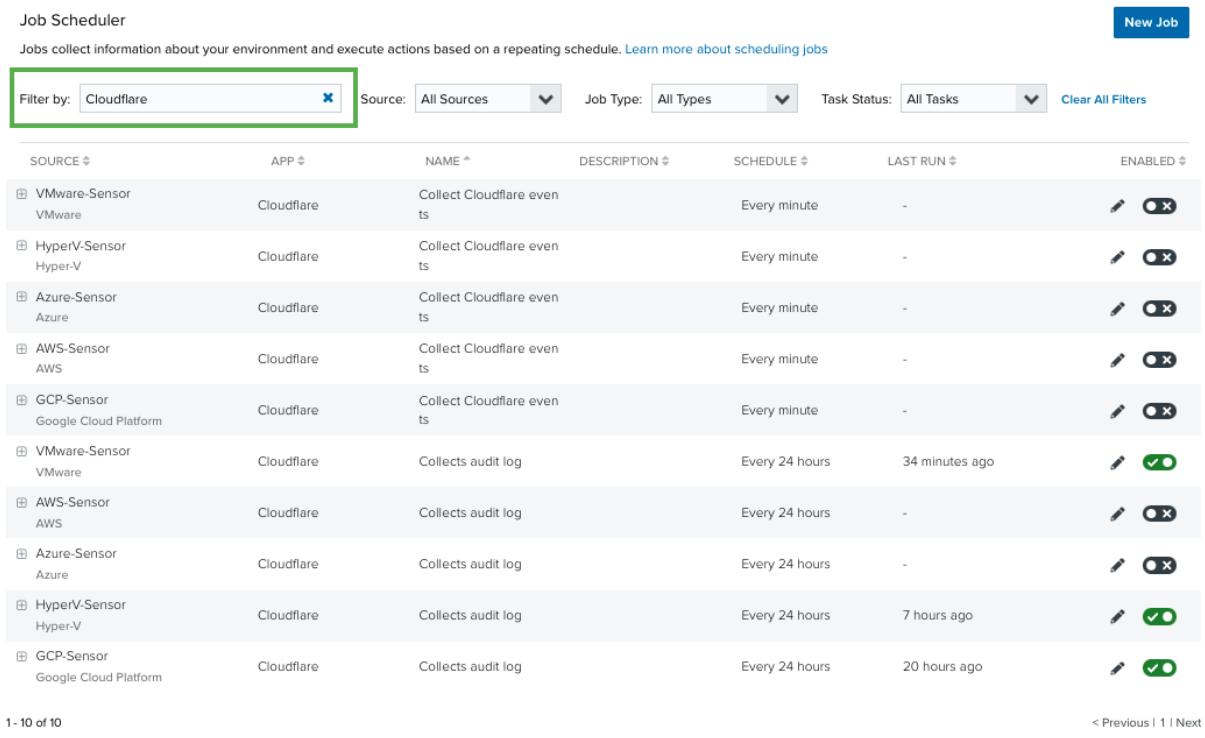
Important: The Cloudflare service can generate numerous log messages, depending on the traffic and number of the website assets it manages. When you have BlueApp for Cloudflare configured, and the log collection job enabled, the number of events produced in USM Anywhere could be excessive and consume large amounts of data storage. To address this, you should add the suggested filtering rule to eliminate standard "HTTP OK" events.

Verifying the Log Collection Job

You can view log collection jobs in the Job Scheduler page and make sure that the job is enabled for the sensor where you configured the BlueApp for Cloudflare.

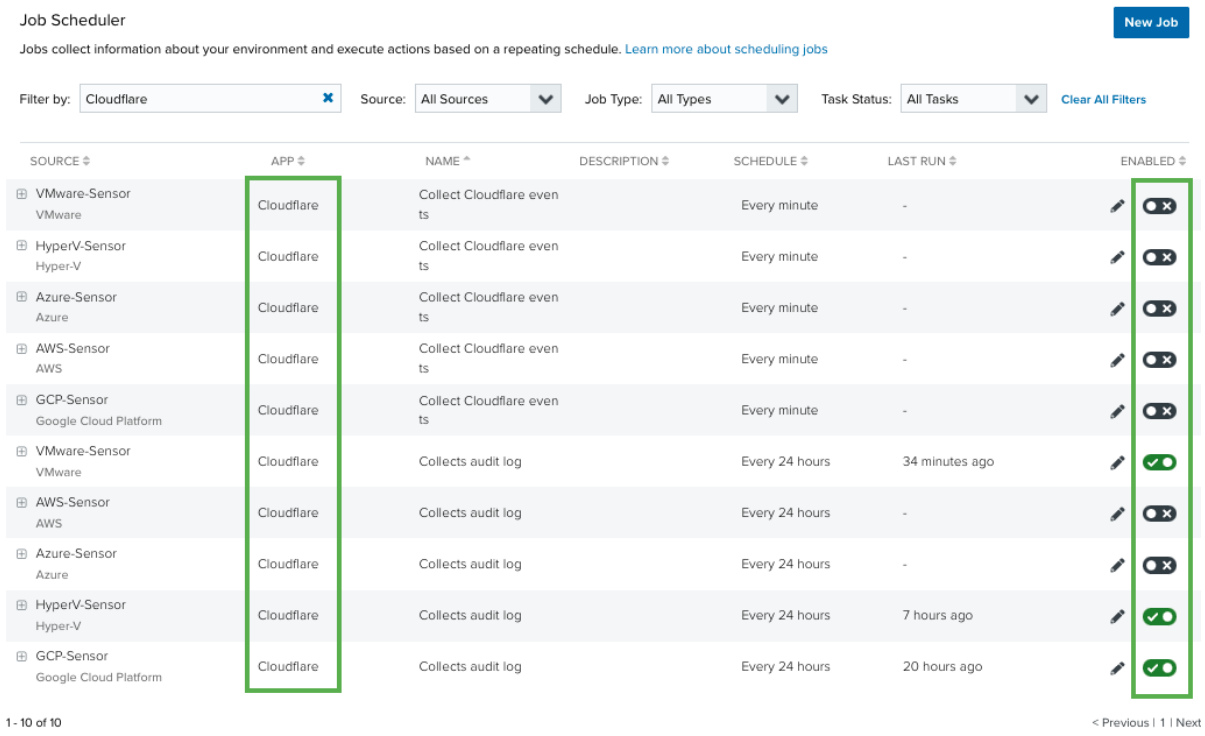
To verify the Cloudflare collection job

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the *Filter by* field at the top of the list, enter **Cloudflare** to filter the displayed list for the Cloudflare App jobs.



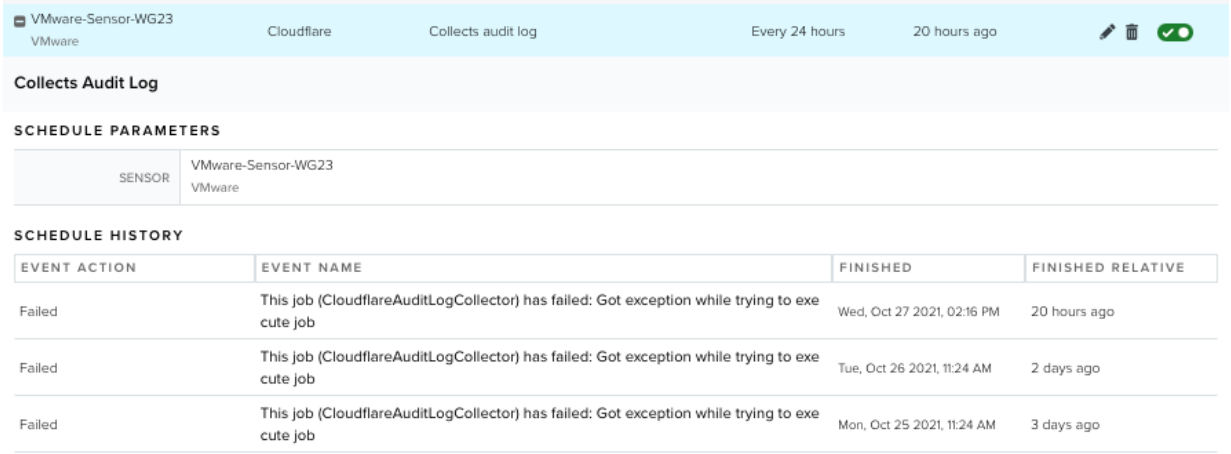
Jobs that are currently enabled display the icon.

3. If the jobs for the sensor are not enabled, click the icon to toggle it.



After the collection job runs a few times, you can select the job to view detailed information about the data collected for each job execution. This includes the number of zones scanned, the number of events retrieved per zone, and if the zones were completed or not.

Note: A job run may not be able to complete a zone if the BlueApp for Cloudflare hits the Cloudflare API connection limitation during collection. If a zone is not completed, the next job run will prioritize that zone to collect the missed data. However, if there are incomplete zones in successive jobs, there could be missed events.



Adding the Suggested Filtering Rule

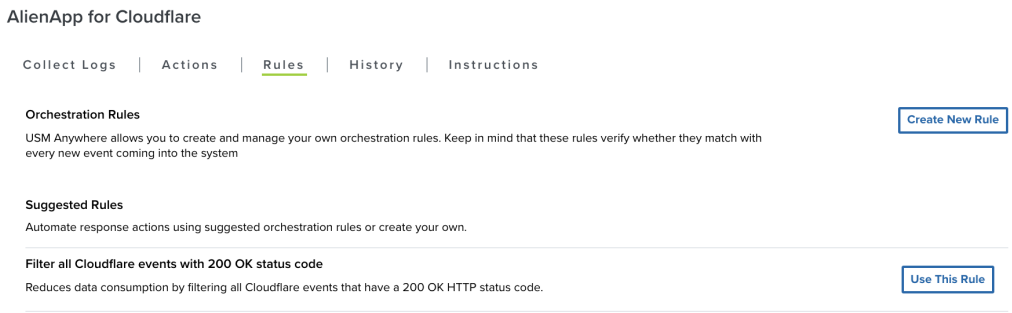
In USM Anywhere, a filtering rule instructs your deployed sensors to drop future events that match the specified criteria. The matching events are neither correlated nor stored. Filtering rules enable you to control the event data that you are going to store in USM Anywhere and manage the data consumption associated with your subscription.

The Rules tab of the BlueApp for Cloudflare page provides a suggested rule as the basis for a Cloudflare filtering rule. This suggested rule automatically includes a set of matching criteria for eliminating standard "HTTP OK" log messages to reduce noise and data storage consumption.

Important: Filtering rules are *not* retroactive, the new rule will apply only to new events and does not eliminate existing events that are a match for the rule.

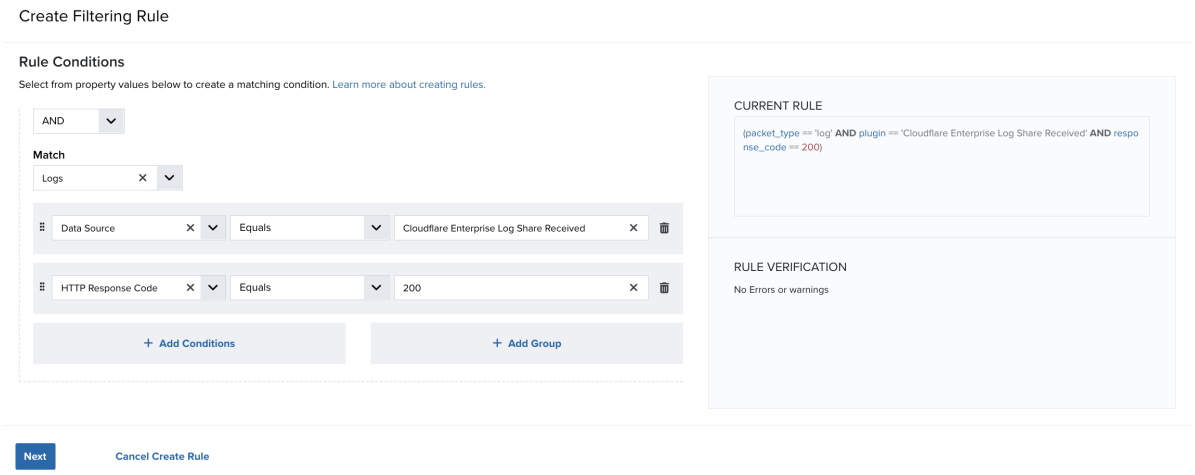
To add the suggested Cloudflare filtering rule

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Rules** tab.



5. Click **Use This Rule**.

   This opens the Create Filtering Rule dialog box with preconfigured options for the new rule. You can keep these options exactly as they are, or make some changes according to your specific needs.



Important: If you choose to modify the conditions, the rule may not effectively reduce data storage for Cloudflare events. Excessive events could cause you to go over the storage tier for your subscription.

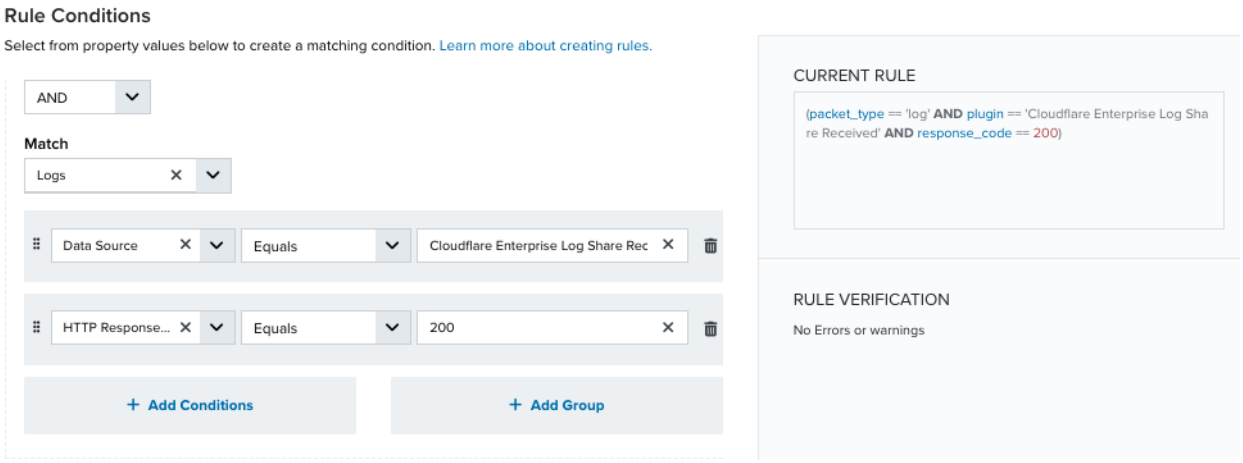
6. Click **Next**.
7. Add a name for the rule (for example, Filter all Cloudflare events with 200 OK status code).
8. (Optional.) Enter a description for identifying this rule.
9. Click **Save**.

Adding a Cloudflare Alarm Rule

There are no out-of-the-box correlation rules that produce alarms from identified Cloudflare events. However, you can create your own alarm rules to generate alarms from Cloudflare events according to your specified criteria. The easiest way to do this is from an event. When you see a Cloudflare event that indicates a potential threat or something that requires high-visibility for you or your team, you can quickly create a new alarm rule from the event so that USM Anywhere generates alarms from similar events in the future.

See Creating Alarm Rules from the Events page in the *USM Anywhere User Guide* for detailed information about creating an alarm rule.

When you set the conditions for the alarm rule, make sure to select **Data Source**, **Equals**, and **Cloudflare Enterprise Log Share Received** respectively, to create alarms that are specific to events from the BlueApp for Cloudflare.



Cloudflare Response Actions

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

After USM Anywhere identifies Cloudflare events and alarms, you determine which Cloudflare activities are suspicious and should be investigated, and use the Cloudflare workflow to notify the investigator. For example, if you see a file upload event and think it should be investigated, rather than manually notifying the investigator, you can use the BlueApp for Cloudflare response action to create a firewall action to block the suspicious upload.

The BlueApp for Cloudflare enables you to create firewall actions based on either the destination IP address or source IP address. These actions are available when you launch a response action directly from an alarm or event (described in the table below) or launch a response action in an orchestration rule.

Action	Description
Create a Cloudflare action from an alarm	Run this action to create a Cloudflare firewall rule (Block, Challenge, JS Challenge, Allow, Log) from an alarm.
Create a Cloudflare action from an event	Run this action to create a Cloudflare firewall rule (Block, Challenge, JS Challenge, Allow, Log) from an event.

Note: Before launching a Cloudflare response action, you must have enabled and connected the BlueApp for Cloudflare to your Cloudflare Enterprise account. See Configuring the BlueApp for Cloudflare for more information.

When reviewing an alarm or event originated from a Cloudflare event, if you conclude that the source is compromised you can launch an action to block incoming data from the IP address associated with that alarm. If you want to apply the action to similar alarms or events that occur in the future, you can create an orchestration rule after you apply the action.

To launch the Create Firewall Action for an alarm

1. Go to **Activity > Alarms**.
2. Review the alarms generated on the Cloudflare events, and then click the alarm to open its details.
3. Click **Select Action**, and then select the **Run Cloudflare Action** tile.
4. (Optional.) If you have more than one USM Anywhere Sensor configured for the BlueApp for Cloudflare, select the sensor that you want to use for the action.
5. From the App Action drop-down list, select **Create firewall action from the destination IP Address** or **Create firewall action from the source IP Address**, depending on your needs.
6. From the Zone Name drop-down list, select the appropriate zone.
7. From the Action Type drop-down list, select the appropriate action type:
   - **Block**: Blocks requests from accessing the site.
   - **Challenge**: Forces the user to pass a Google reCAPTCHA challenge before proceeding.

     If the user passes this challenge, Cloudflare accepts the request. If they fail, the request is blocked.
   - **JS Challenge**: Forces the user to pass a Cloudflare Javascript challenge before proceeding.

     If the user passes this challenge, Cloudflare accepts the request. If they fail, the request is blocked.
   - **Allow**: Explicitly allows all matching requests, as long as no other Cloudflare firewall fea-

tures block it.

- **Log**: Logs the request in Cloudflare Logs.

  Note: This action type is only available to Cloudflare Enterprise customers.

8. Click **Run**.

   After USM Anywhere initiates the action for the alarm, it displays a confirmation.

If the alarm is related to a file in your Cloudflare environment and you want it to be investigated, you can launch an action to create a task on the specific file. If you want to apply the action to similar alarms that occur in the future, you can create an orchestration rule after you apply the action.

Creating Cloudflare Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Cloudflare response action when alarms match the criteria that you specify. For example, you can create a rule where USM Anywhere automatically blocks traffic when its origin is from a known malicious source.

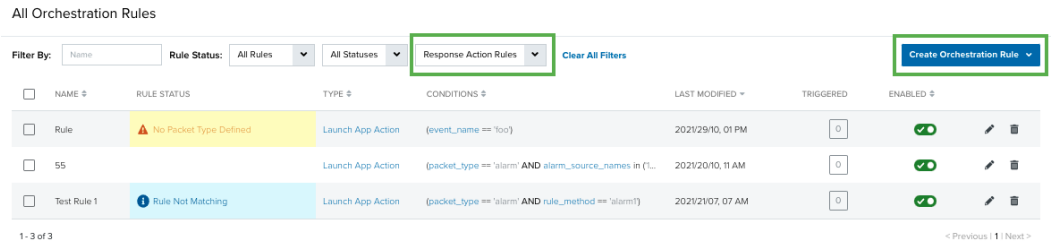
After you create a rule, new alarms that match the rule conditions will trigger the Cloudflare response action. The rule does *not* trigger for existing alarms.

You can create a new rule:

- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

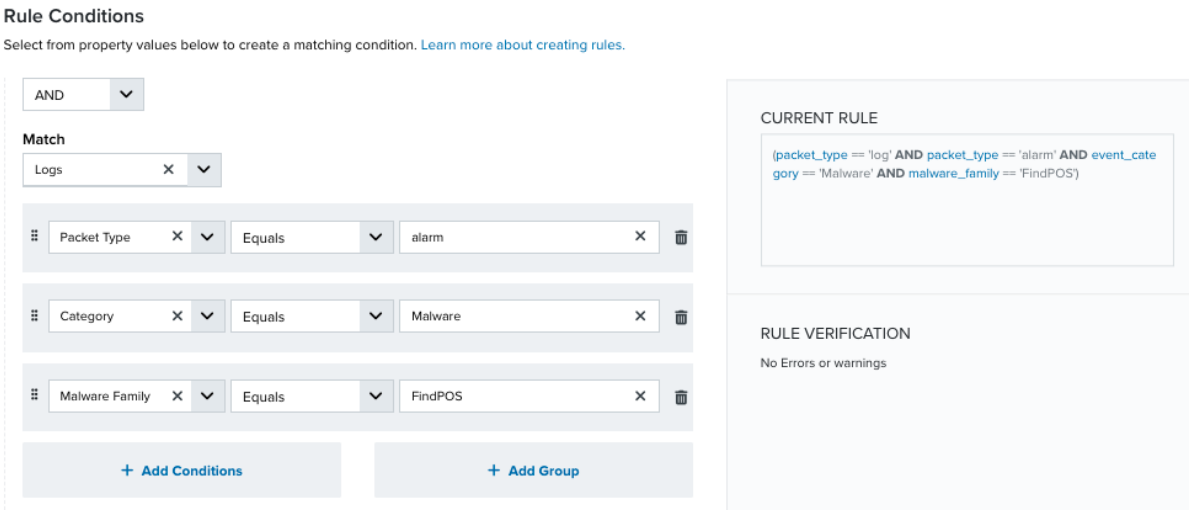
  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click

Create Orchestration Rule > Response Action Rule to define the new rule.



To define a new Cloudflare response action rule

1. Enter a name for the rule.
2. In the Action Type list, select **Cloudflare V2**.
3. In the App Action list, select the action you want to use.
4. Fill out the required fields.
5. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.

- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

6. Click **Save Rule**.
7. In the confirmation dialog box, click **OK**.

BlueApp for Cloudflare Statistics

Role Availability ✔ **Read-Only** ✔ **Investigator** ✔ **Analyst** ✔ **Manager**

The BlueApp for Cloudflare presents a number of diagnostic statistics and related feedback, enabling you to assess the status of the BlueApp without having to delve into the sensor log.

The statistics reported on the BlueApp's page are as follows:

- **Zone Activity**: Each zone's status indicates whether logs are available to be monitored, or whether enterprise log share is disabled for that zone
- **Error Rate**: The number of errors the app detects in its logic, displayed as *Errors per Second*

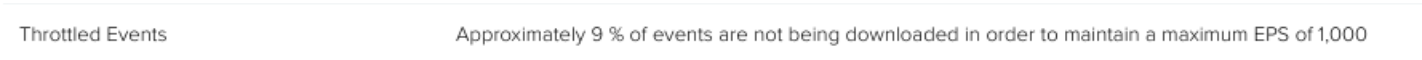
  Important: The app will retry potentially recoverable errors three times before giving up. See Error Recovery for more information.
- **Throttled Events**: The percentage of events that are ignored during throttling mode
- **Orchestration Action Count**: The number of orchestration actions invoked since the last time the sensor was restarted
- **Average Event Age**: The average age of events coming from Cloudflare

Throttling Mode

In the event that your sensor is being overloaded by an unusual amount of events per second (EPS), your app may enter throttling mode in an effort to reduce strain on your sensor or lower the bandwidth it is consuming. Throttling mode is automatically enabled any time the app detects that more than 1000 EPS are being generated. When the actual EPS has remained under 1000 for a minute, the app will disengage throttling mode.

While your app is in throttling mode, it throttles the data coming to the sensor to limit the data being pulled. Doing this helps the app to maintain its threshold below 1000 EPS.

When your app is in sampling mode, the Status page indicates this and displays approximately what percentage of data is being skipped:



Error Recovery

In the event that the job receives a potentially recoverable error, it will retry that job up to three times before giving up. If it cannot collect the data after the third retry, you will see the failure noted in the scheduler history and the next scheduled job will try to collect the data from the failed job in addition to its own data.

When this happens, you may see some jobs labeled "already running". This means that the job before it took over a minute to complete, so the next scheduled job was skipped because the previous job was still running. The job after a skipped job will then collect both its data and the data from the skipped job, proceeding in this cycle until the app is caught up.

Average Event Age

This metric represents the latency between an event's timestamp in Cloudflare and the moment it is processed by the app. The age of each zone's most recent event is taken and all are averaged to provide the average event age for your app.

BlueApp for ConnectWise

Service management teams that use ConnectWise Manage can deploy and provision USM Anywhere and manage those deployments for their customers. With configuration of the BlueApp for ConnectWise on each USM Anywhere instance, teams can leverage automated service ticket creation from alarms and vulnerabilities identified by USM Anywhere as well as synchronization of asset information with ConnectWise Manage configurations.

Edition: The BlueApp for ConnectWise is available in the Standard and Premium editions of USM Anywhere. See https://cybersecurity.att.com/pricing for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

BlueApp for ConnectWise Requirements

Before you can configure and use the BlueApp for ConnectWise, you must have the following requirements in place:

- A ConnectWise Manage environment
- A USM Anywhere instance with a USM Anywhere Sensor deployed in the customer's network
- The company name used to access your ConnectWise environment
- The company identification (ID) for the managed company (customer) defined in ConnectWise Manage to be associated with the USM Anywhere deployment
- The member name defined in ConnectWise Manage that you will use for the integration with USM Anywhere, with all rights needed for service ticket creation and configuration update for the managed company
- Rights to create API keys for the designated member account

Configuring the BlueApp for ConnectWise

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

When the BlueApp for ConnectWise is enabled and connected to your ConnectWise Manage environment, USM Anywhere sends data to automatically generate new service tickets from alarms and vulnerabilities and synchronize assets with the Configurations catalog. See BlueApp for ConnectWise Actions for more information about these BlueApp for ConnectWise response actions.

Important: Before you configure the BlueApp for ConnectWise, make sure to review the requirements.

A configured connection also provides a user interface (UI) integration, so that you can access USM Anywhere directly from your ConnectWise Manage console. See USM Anywhere and ConnectWise Manage UI Integration for more information about this feature.

Obtain the API Keys

A set of ConnectWise Manage API keys are required to authenticate USM Anywhere for communications with ConnectWise Manage.

To get the API keys from ConnectWise

1. Log in to your ConnectWise Manage account using the web UI or client application.
2. Go to **System > Members** and click the **API Member** tab.
3. If you do not already have a member account that you can use for the integration, create a new (API Only) member account.

   Note: Although it is a best practice to use an API Member account for integrations, you can create API keys from your current member account. API Member accounts do not require a ConnectWise Manage License and cannot access the ConnectWise Manage UI.

   The member account that you use must have the Role ID field set to Admin.

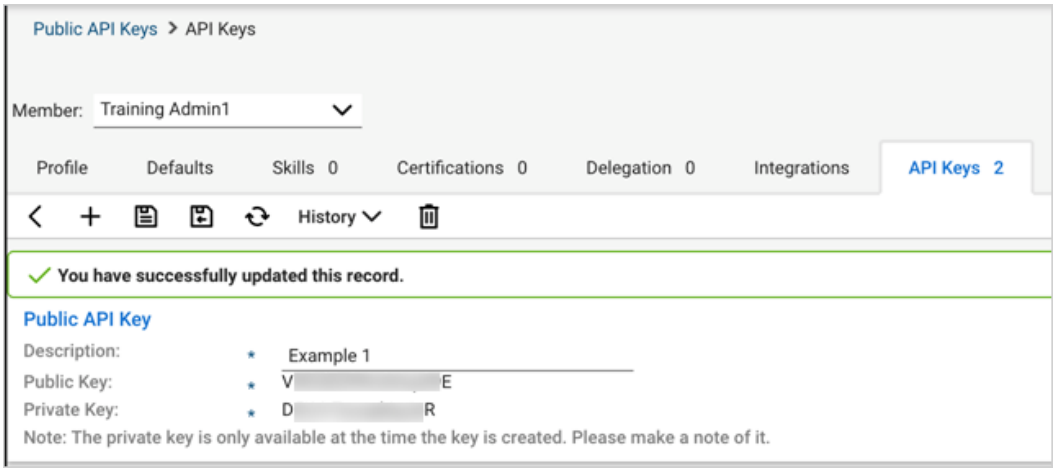
   a. Click the + icon and define the new member.

   b. Click the icon to save your changes.
4. Click the **API Keys** tab.
5. Click the **+** icon and enter a description for the Public API Key.
6. Save your changes.

   The page displays both the public and private API keys.

   Important: The private key is visible only at the time that you generate the API keys. After that, it is no longer accessible. It is a best practice to make a copy of both the

public and private keys and store them in a secured location.



7. Copy both of the key values to be entered in USM Anywhere.

Important: If you generate a new API token or key at some point in the future, it will revoke the existing token making the connection unauthorized. Therefore, you must update the token in USM Anywhere accordingly.

Configure the BlueApp for ConnectWise Connection

To enable BlueApp for ConnectWise functions, you must configure a connection with your ConnectWise Manage environment and define the associated customer (managed company). This connection enables the BlueApp to perform operations using the ConnectWise Manage Representational State Transfer (REST) APIs.

To configure the ConnectWise Manage connection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Specify the connection information for ConnectWise:

- **Manage site URL**: Select the site you use to access your ConnectWise Manage environment.

  For example, if you access the browser version of ConnectWise Manage at https://mysite.connectwise.net, you specify *mysite.connectwise.net* for this option.

- **Company**: Enter the company name that you use when you log in to your ConnectWise account.

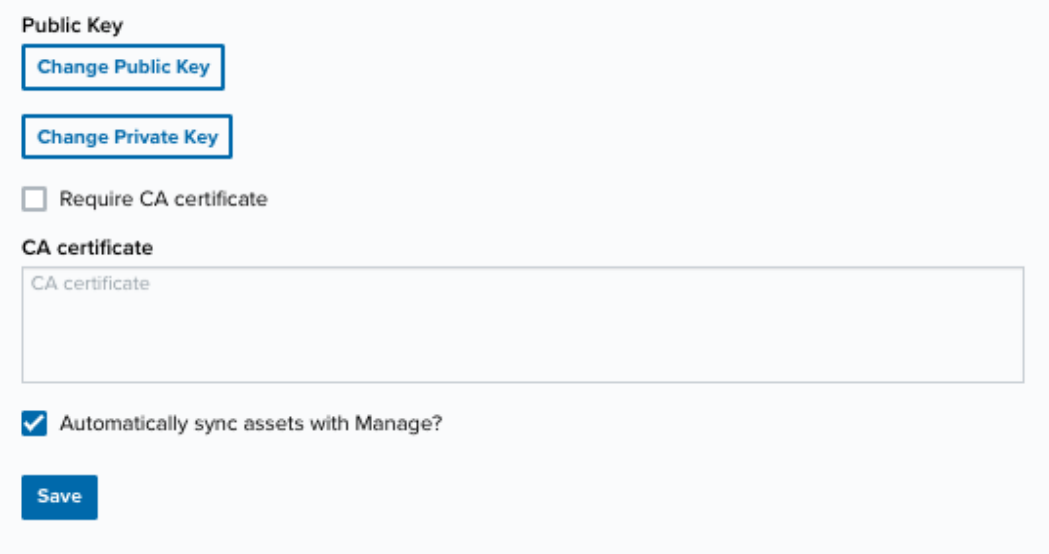
- **Managed company**: Enter the company identification (ID) that you want to associate with the USM Anywhere deployment.

  This is the company ID of a customer (active company) specified in your ConnectWise Manage environment. You can use the Company Search function in ConnectWise Manage to locate the correct company ID.

- **Member**: Enter the name for the member account that you used to generate the API keys.

- **Board name**: Enter the name for the ConnectWise board where you want to manage the created service tickets.

7. Add the public and private keys that you generated in ConnectWise Manage:



   - Click **Change Public Key** and paste the copied public key value in the text box.
   - Click **Change Private Key** and paste the copied private key value in the text box.

8. (Optional.) If you want to use your own Secure Sockets Layer (SSL) certificate for connection to your ConnectWise environment, select the **Require CA certificate** checkbox and enter the certificate in the CA certificate field.

   The SSL certificate must be configured in ConnectWise. See the ConnectWise documentation for more information about ConnectWise SSL support and enablement (requires a ConnectWise University login).

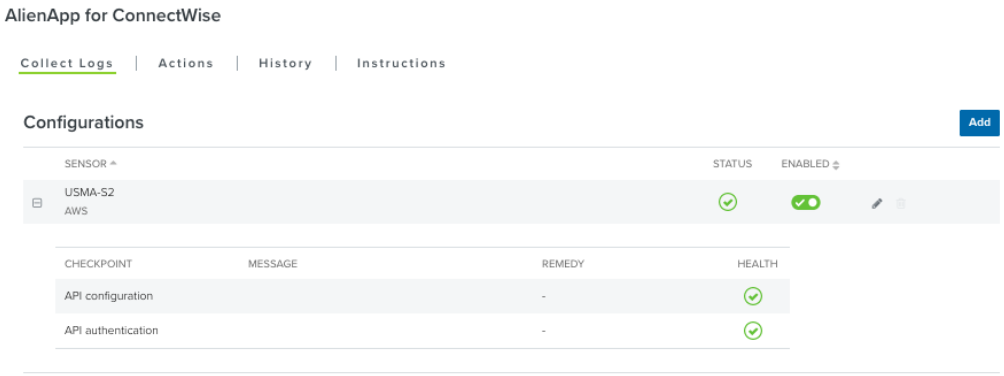
9. (Optional.) If you want to synchronize assets discovered by USM Anywhere with the configurations defined in ConnectWise Manage, select the **Automatically sync assets with Manage** checkbox.

   When this option is selected, USM Anywhere runs an automated job every hour to update the Configurations catalog in ConnectWise Manage to add or update discovered assets.

10. Click **Save**.

11. Verify the connection.

    After USM Anywhere completes a successful connection to the ConnectWise Manage REST APIs, a icon displays in the Health column.



If the ⊗ icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your ConnectWise connection.

BlueApp for ConnectWise Actions

The BlueApp for ConnectWise provides a set of orchestration actions that automate the creation of service tickets in ConnectWise Manage as a response to threats detected by USM Anywhere, and the management of the Configurations catalog in ConnectWise Manage as a response to asset scans performed by USM Anywhere. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for ConnectWise

Action	Description
Add Tickets to the Manage Database	This action creates and updates the tickets from USM Anywhere alarms and vulnerabilities. USM Anywhere includes the *Update the Ticket database* job in the Scheduler, which executes this action every five minutes. When you configure the BlueApp for ConnectWise, this job is enabled by default. **Note:** Currently, configuration issues identified by USM Anywhere are not included in the job to create and update Manage service tickets.
Add Configurations to the Manage Database	This action updates the Configurations catalog in ConnectWise Manage to reflect the most recent asset scan by USM Anywhere. USM Anywhere includes the *Update Configurations catalog* job in the Scheduler, which executes this action every 60 minutes. When you configure the BlueApp for ConnectWise and select **Automatically sync assets with Manage**, this job is enabled by default. **Note:** If an asset that USM Anywhere previously discovered is no longer present in the most recent asset scan, the status changes to *inactive*. If it discovers the asset in another future scan, the status changes to *active*.

If you choose to disable one of these jobs for the USM Anywhere instance, you can go to Settings > Scheduler. When you select a ConnectWise job in the page, you can also access history information that is specific to that job. See USM Anywhere Scheduler in the *USM Anywhere User Guide* for more information.

Important: The BlueApp for ConnectWise must be enabled and connected to your Manage environment for successful execution of these jobs. See Configuring the BlueApp for ConnectWise for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch an AT&T Secure Web Gateway orchestration action for an alarm

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **ConnectWise** tile.
5. For the App Action, select the action you want to launch.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Enter the name of the category you want the IP added to, if applicable.
7. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

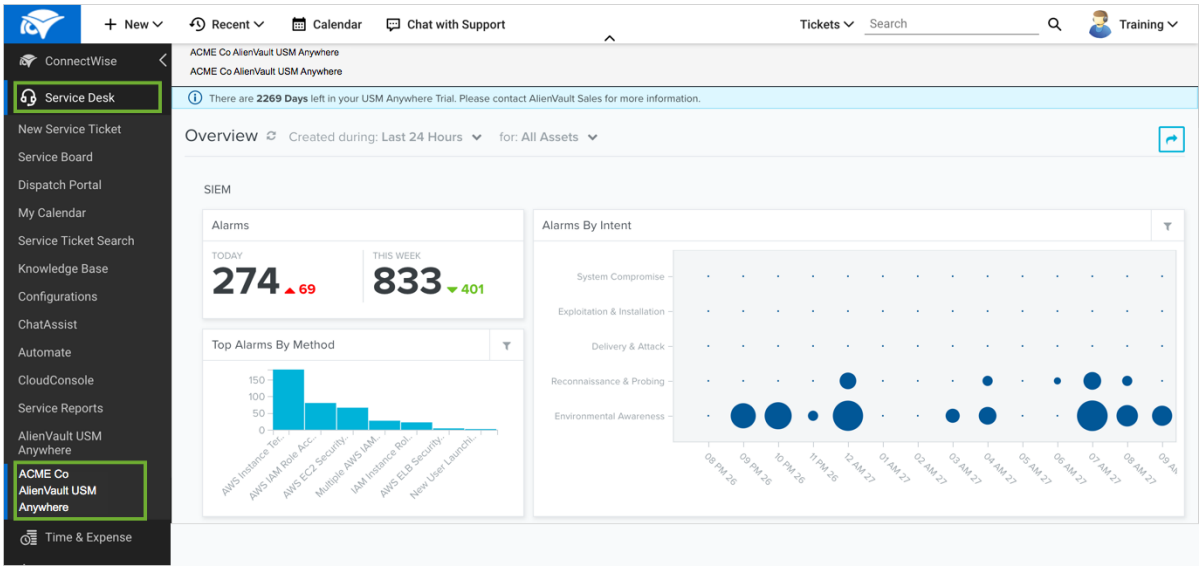
USM Anywhere and ConnectWise Manage UI Integration

With a successful connection to your ConnectWise environment, the BlueApp for ConnectWise supports a user interface (UI) integration to launch the USM Anywhere console directly from the ConnectWise Manage UI. As a Managed Service Provider using ConnectWise Manage, you can easily launch each instance when you have more than one USM Anywhere instance deployed for your end customers.

To access a USM Anywhere console from ConnectWise Manage

1. In ConnectWise Manage, select **Service Desk** to expand the menu.
2. Scroll to the bottom of the Service Desk items and select the connected USM Anywhere instance.
3. Enter a username and password for the USM Anywhere instance and click **Login**.

   The ConnectWise Manage UI loads the USM Anywhere console in the context page.



Accessing USM Anywhere Tickets in ConnectWise Manage

With a successful connection to your ConnectWise Manage environment, the BlueApp for ConnectWise provides a scheduled job to update the ConnectWise Manage ticket database to reflect the alarms and vulnerabilities identified by USM Anywhere. You can manage these service tickets in the ConnectWise Manage user interface (UI) according to your established practices.

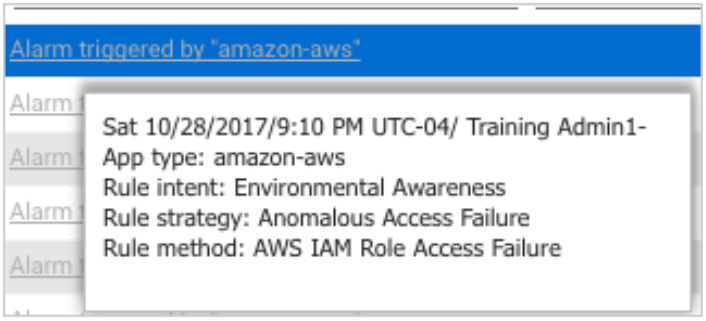
When the status for an alarm or vulnerability changes to cleared in USM Anywhere, the next execution of the job updates the status of the associated ticket to *closed* in ConnectWise Manage. Because this job runs every 5 minutes, there will be a delay to see the change in the ConnectWise Manage UI.

Important: Currently, changing the status of the service ticket in ConnectWise Manage does not result in a status change for the related alarm or vulnerability in USM Anywhere.

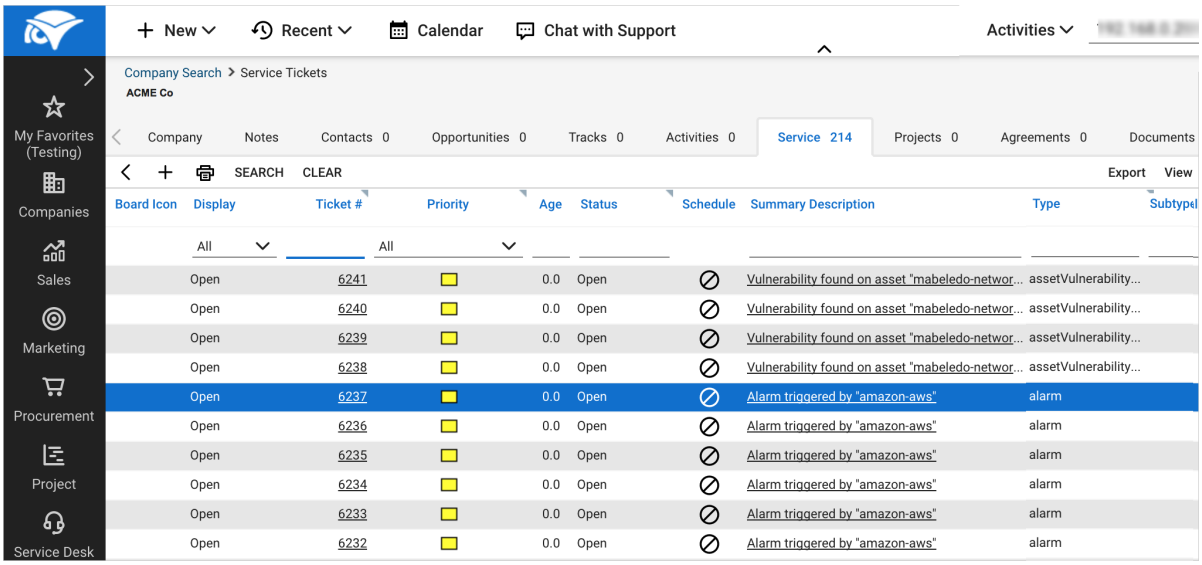
ConnectWise Manage provides multiple ways to access service tickets for your customers. The following procedure outlines one of the most common methods for investigating service tickets for a managed company.

To access USM Anywhere-generated tickets in the ConnectWise Manage UI

1. In ConnectWise Manage, open the page for the managed company (customer).
2. Click the **Service** tab.
3. Hover the cursor over the displayed alarm and vulnerability items to view information high-level information provided by USM Anywhere.

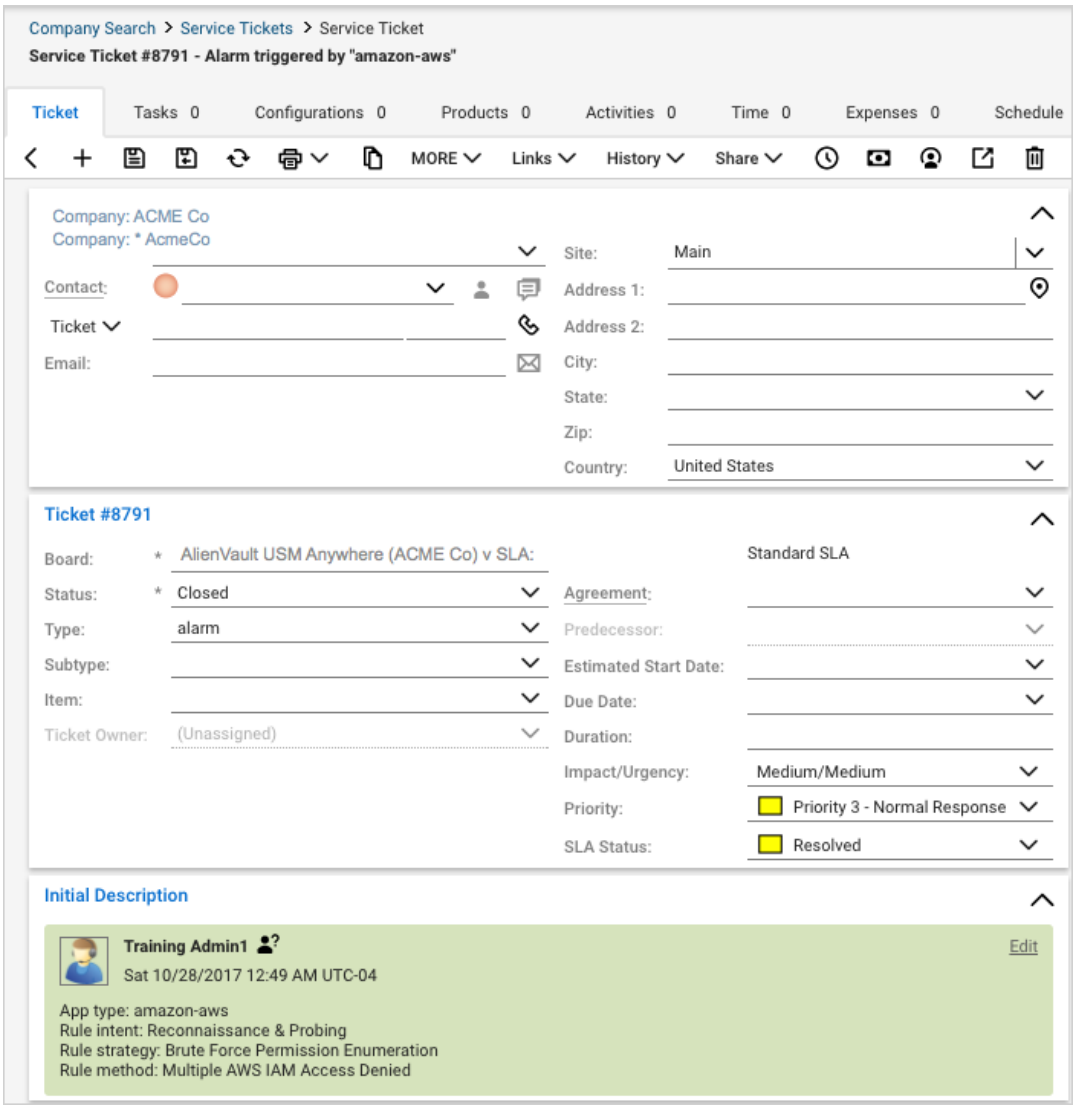


4. Select the alarm or vulnerability item in the list to open the ticket.



5. Review the detailed information for the service ticket.

   As you scroll through the page, you can make changes so that your team can address the issue.



Accessing USM Anywhere Asset Information in ConnectWise Manage

With a successful connection to your ConnectWise Manage environment, the BlueApp for ConnectWise provides a scheduled job to update the ConnectWise Manage Configurations catalog to reflect the assets identified by USM Anywhere. You can manage these configurations in the ConnectWise Manage user interface (UI) according to your established practices.

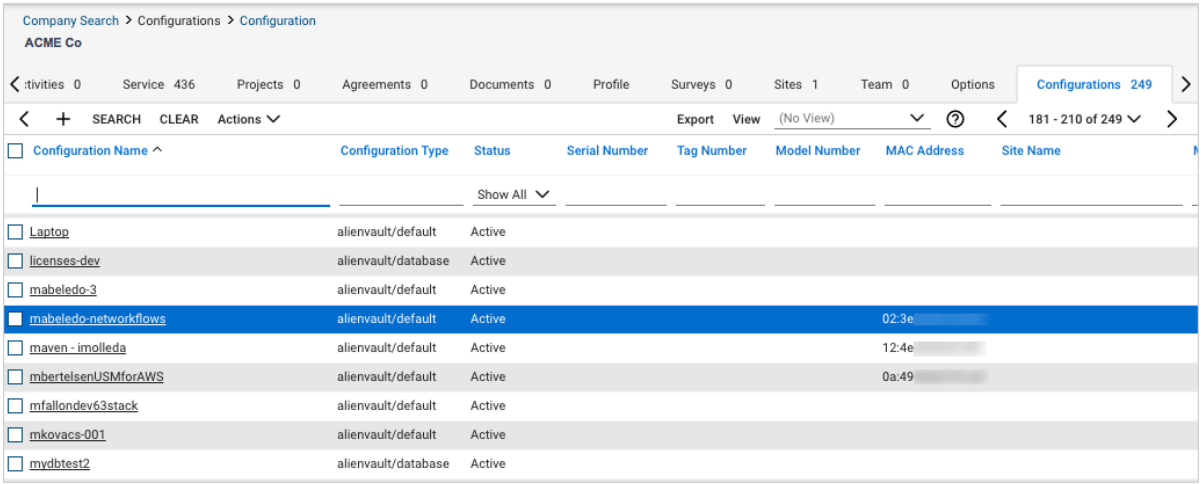
When USM Anywhere detects changes to an asset during an asset scan, the next execution of the job updates the associated configuration in ConnectWise Manage. If an asset that USM Anywhere previously discovered is no longer present in the most recent asset scan, the status changes to *inactive*. If it discovers the asset in another future scan, the status changes to *active* in the next job. Because this job runs every 60 minutes, there will be a delay in seeing these changes in the ConnectWise Manage UI.

Important: Currently, changing parameters of a configuration in ConnectWise Manage does not result in a change for the asset in USM Anywhere.

ConnectWise Manage provides multiple ways to access configurations (assets) for your customers. The following procedure outlines one of the most common methods for investigating configurations for a managed company.

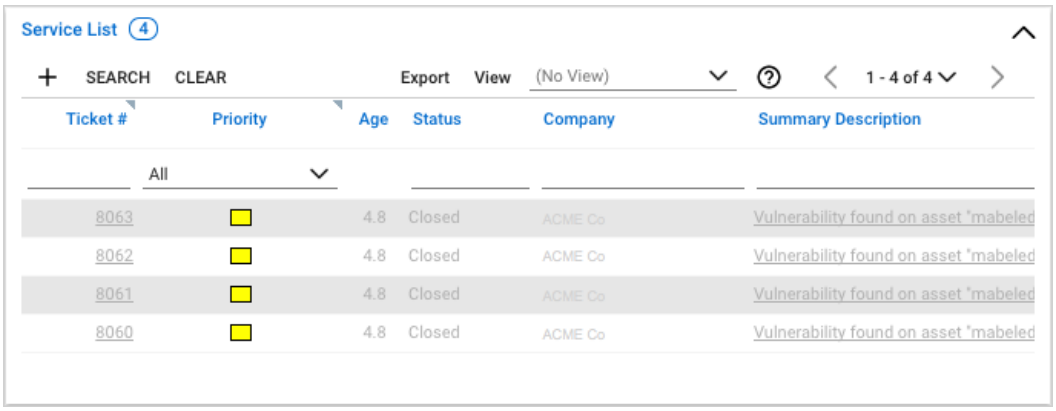
To access USM Anywhere-reported configurations in the ConnectWise Manage UI

1. In ConnectWise Manage, open the page for the managed company (customer).
2. Click the **Configurations** tab.
3. Select the configuration item in the list to view the details.



4. Review the information for the configuration.

You can scroll through the configuration record to the Service List section and view the tickets generated by USM Anywhere for alarms or vulnerabilities associated with the asset.



BlueApp for CrowdStrike Falcon

The BlueApp for CrowdStrike Falcon enables you to ingest incident and detection logs from your CrowdStrike app into USM Anywhere. The BlueApp for CrowdStrike Falcon enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from CrowdStrike and provides orchestration actions to implement CrowdStrike incident response activities based on the risk identified in USM Anywhere.

Edition: The BlueApp for CrowdStrike Falcon is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for CrowdStrike Falcon

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To configure the BlueApp for CrowdStrike Falcon in USM Anywhere, you need to have the Host URL, Client ID, and Client Secret for authorization. This information can be obtained from your Crowdstrike support team.

Set up Crowdstrike API

Follow the instructions listed in the Crowdstrike site to read more about connecting with Crowdstrike.

Important: The BlueApp for CrowdStrike Falcon requires Falcon X, Falcon Prevent, Falcon Insight, or Endpoint Detection and Response (EDR) to work properly.

Configure BlueApp for CrowdStrike Falcon in USM Anywhere

To enable the BlueApp for CrowdStrike Falcon

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Host URL, Client ID, and Client Secret for authorization.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for CrowdStrike Falcon Actions

The BlueApp for CrowdStrike Falcon provides a set of orchestration actions that you can use to ingest incident and detection logs from your Crowdstrike app into your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for CrowdStrike Falcon

Action	Description
Contain a host	Contain a host within your environment, stopping any network communications as defined in your Crowdstrike containment policy
Lift containment	Restores network communications to a previously-contained host

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms and Events

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an Alarm or an Event.

To launch a Crowdstrike response action for an Alarm or Event

1. Go to **Activity > Alarms** or **Activity > Events**
2. Click the Alarm or Event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Crowdstrike Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

BlueApp for DDI Frontline VM

The AlienApp for Digital Defense, Inc. (DDI) Frontline Vulnerability Manager (VM) enables you to synchronize asset inventory information and threat detection and response activities between USM Anywhere and your DDI Frontline VM. The BlueApp for DDI Frontline VM enhances the capabilities of your threat detection management by taking the DDI Frontline VM asset-scanning results (vulnerabilities) and asset-management capabilities and merging them with USM Anywhere. You can create, update, and merge assets, and schedule scans in USM Anywhere, based on the information provided from the BlueApp for DDI Frontline VM. Where applicable, the BlueApp for DDI Frontline VM will enhance this information with Common Vulnerabilities and Exposures (CVE) scores, detection sources, and more.

Edition: The BlueApp for DDI Frontline VM is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for DDI Frontline VM

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ Manager

DDI Frontline VM Configuration

Important: In addition to the following configuration steps, you must also create a business group in your DDI portal and ensure that your user account is added to that business group.

To configure the AlienApp for Digital Defense, Inc. (DDI) Frontline Vulnerability Manager (VM) in USM Anywhere, you need to generate an API key in your DDI Frontline VM instance and enter it into USM Anywhere.

To set up your DDI Frontline API

1. Log in to your DDI Frontline VM instance.
2. Go to **My Profile > API Tokens > Create new token**.
3. In the Add New Token window, enter a name for the API token and click **OK**.
4. Click **Click to show key** to see your API key.

   Copy this API key to enter into USM Anywhere.
5. Go to **System > Scanner Management**.
6. Navigate to the scanner profiles and click to open the profile you need to configure.
7. In the **IP & Ports** field, add the IP range that your BlueApp for DDI Frontline VM should scan to cover all of your assets.

To enable the BlueApp for DDI Frontline VM

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the API Key.
7. Select **Allow Asset Creation** to allow DDI Frontline VM scans to create new assets in USM Anywhere.

   Select **Merge Duplicate Assets** if you allow USM Anywhere to run a match against the DDI Frontline asset VM identification to merge the assets found with existing USM Anywhere assets.

   See BlueApp for DDI Frontline VM Asset Discovery and Management for more details on the asset creation and merging processes.
8. Click **Save**.

The BlueApp for DDI Frontline VM and the BlueApp for AT&T Managed Vulnerability Platform

Because both the BlueApp for DDI Frontline VM and the BlueApp for AT&T Managed Vulnerability Platform share configuration components through BlueApp for DDI Frontline VM, configuring one BlueApp will cause the other to appear as configured in your My Apps page. This is expected behavior. Do not delete or disable the BlueApp for DDI Frontline VM or the BlueApp for AT&T Managed Vulnerability Platform. Changes to one BlueApp will cause configuration errors with the other BlueApp.

BlueApp for DDI Frontline VM Asset Discovery and Management

The AlienApp for Digital Defense, Inc. (DDI) Frontline Vulnerability Manager (VM) features powerful vulnerability assessment capabilities that can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you can allow DDI Frontline VM to create assets that are discovered in scans, and merge the asset information provided from the DDI Frontline VM scan with the existing asset information in USM Anywhere.

Asset Creation from BlueApp for DDI Frontline VM

When DDI Frontline VM runs a scan, it identifies all assets and assigns them an individual DDI Frontline VM identifier (ID). These assets can be added to USM anywhere by selecting the **Allow Asset Creation** checkbox in the app's configuration menu. Assets created from a DDI

Frontline VM scan will include the DDI network profile ID, DDIv NetBios smartname, and the DDI Domain Name System (DNS) smartname in the asset details.

The BlueApp for DDI Frontline VM *Asset Source* filter only displays assets that were created by the app's asset scan. Assets that were originally created by other means (for example, existed in USM Anywhere before the asset scan or were ingested by another app) will not be shown by this filter. To view all assets, including those not ingested by this app, use one of the app's custom filters or the *DDI host name* filter. The BlueApp for DDI Frontline VM cannot scan any asset that was not ingested through the app.

Duplicate Asset Merge

Assets discovered in DDI Frontline VM scans may duplicate the assets already discovered in USM Anywhere. When you select the **Merge Duplicate Assets** checkbox in the DDI Frontline VM configuration menu, USM Anywhere merges the information from the DDI Frontline VM scan with the existing asset. Assets are matched by comparing the unique DDI ID, MAC address, IP address, and host name from the DDI Frontline VM scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the DDI Frontline VM configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for DDI Frontline VM page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the DDI Frontline VM scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the DDI Frontline VM scan.
- **Merge:** Merge the information from the DDI Frontline VM scan with the matching asset details in USM Anywhere.
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a DDI Frontline VM asset profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window opens showing the existing asset and the new asset that will be created once the two are split.
4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for DDI Frontline VM Orchestration

The BlueApp for DDI Frontline VM provides a set of orchestration actions that you can use to identify vulnerabilities and manage assets in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for DDI Frontline VM

Action	Description
Run Scan	Use DDI Frontline VM to scan asset for vulnerabilities. Scanner, scan policies, business groups and asset groups can all be specified here. Scans can also be scheduled for a specific date and time.
Run Scan by Label	Use DDI Frontline VM to scan asset for vulnerabilities based on a specific DDI label. Scanner, scan policies, business groups, and asset groups can all be specified here.

Actions for the BlueApp for DDI Frontline VM (Continued)

Action	Description
Add Asset to Static Asset Group	Add asset to a static DDI Frontline VM asset group.
Add Label to Asset	Add a DDI label and, optionally, label color to an IP range.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

Digital Defense Incorporated (DDI) Frontline Vulnerability Manager (VM) scans can be performed from the app's Action page (**AlienApps DDI Frontline VM > Actions**) by clicking **Run** next to the action. Alternately, you can run DDI Frontline VM actions from the Vulnerabilities or Assets pages.

To launch a DDI Frontline VM action from a vulnerability

1. Go to **Environment > Vulnerabilities**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **DDI Frontline VM** tile.
5. For the App Action, select the action you want to run.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Fill out the details for the scan action you selected.
7. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

To launch a DDI Frontline VM scan for an asset

1. Go to **Environment > Assets**.
2. Do one of the following:
   - Next to the asset name that you want to scan, click the icon and select **Full Details**, and then select **Actions > Scan with BlueApp**.
   - Next to the asset name that you want to scan, click the icon that you want to scan and select **Scan with BlueApp**.
3. For the App Action, select the action you want to run.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
4. Fill out the details for the scan action you selected.
5. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

BlueApp for Fortinet FortiGate

The BlueApp for Fortinet FortiGate enables you to automate threat detection and response activities between USM Anywhere and the Fortinet FortiGate Next-Generation Firewall (NGFW). The BlueApp for Fortinet FortiGate enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from your FortiGate firewall and provides orchestration actions to streamline incident response activities based on risk identified in USM Anywhere.

Edition: The BlueApp for Fortinet FortiGate is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Fortinet FortiGate

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the BlueApp for Fortinet FortiGate in USM Anywhere, you first need to log in to FortiGate to create and obtain the API token.

To generate the API token in FortiGate

1. Log in to the FortiGate graphical user interface (GUI).
2. From the Status dashboard, click the Administrators widget.
3. Click your user ID and select **Show active administrator sessions**.
4. Write down or copy the source address of the user ID.

   This will be used for the API's Trusted Host field in step 8.
5. Go to **System > Admin Profiles > Create New** to create a new administrator profile.
6. Enter a name and change the Firewall and Security Profile access permissions to **Read/Write** (the other permissions can remain set to **Read**), and then click **OK**.
7. Go to **System > Administrators > Create New > REST API Admin**.
8. Enter all required values and use the source address you copied previously for the Trusted Host field.
9. Click **OK** to generate the API token.

   Write down or copy the API token to use later when configuring the BlueApp in USM Anywhere.

Connecting the BlueApp for Fortinet FortiGate in USM Anywhere

After obtaining the credentials, you must configure the connection within USM Anywhere.

To enable the BlueApp for Fortinet FortiGate

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.

5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter your information into the following fields:

   - FortiGate Firewall IP Address/Host Name
   - Port (must be port 443)
   - FortiGate Access Token

7. (Optional) Select **Validate HTTPS host name** and **Require CA certificate** checkboxes and enter the certificate authority (CA) certificate if you want to use this option.

8. Click **Save**.

9. Verify the connection.

   After USM Anywhere completes a successful connection to the FortiGate APIs, a  icon displays in the Health column.

   If the  icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your FortiGate connection.

Uploading a CA Certificate (Optional)

If you leave the Require CA Certificate checkbox deselected, the BlueApp uses the browser's default trust store. When you select the Require CA Certificate checkbox, the certificate entered in the CA Certificate field takes precedence and is the only certificate trusted by the client.

There are two major use cases that might require you to upload your own certificate in the CA Certificate field:

- The firewall was deployed with a self-signed Secure Sockets Layer (SSL) certificate. A certificate like this is typically generated on the firewall at the time of deployment. In this case, you need to export that self-signed certificate from the firewall and paste it into the CA Certificate field.

- You have deployed the firewall with a SSL certificate signed by your own CA. In this case, you need to import the root and intermediate certificates, if any, from your CA. This way, the BlueApp has the same trusted certificate chain that are deployed on your firewall.

Forwarding FortiGate Syslog Messages to USM Anywhere

To collect logs from Fortinet FortiGate, you can configure logging in Log & Report > Log Settings and send all the syslog messages to the USM Anywhere Sensor IP address. See Configure logging to other syslog servers for detailed instructions from the vendor.

Forwarding FortiAnalyzer Syslog Messages to USM Anywhere

If you use FortiGate FortiAnalyzer, you can also configure FortiAnalyzer to forward logs to the USM Anywhere Sensor IP address. See the FortiAnalyzer log forwarding guide for detailed instructions from the vendor.

BlueApp for Fortinet FortiGate Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use FortiGate actions to respond to the events in your environment. Rather than manually adding addresses in the FortiGate user interface (UI) and entering the relevant information, you can use the BlueApp for Fortinet FortiGate response actions to automatically manage your FortiGate firewall using information from your USM Anywhere environment. The table below shows the actions.

Actions for the BlueApp for Fortinet FortiGate

Action	Description
Add Source Address to Address Group	Run this action to add the source address to a group in your FortiGate environment. If the group doesn't exist in FortiGate, it will be created by the action from USM Anywhere
Add Destination Address to Address Group	Run this action to add the destination address to a group in your FortiGate environment. If the group doesn't exist in FortiGate, it will be created by the action from USM Anywhere
Add to Custom Category	Run this action to add the source address to a group in your FortiGate environment
Add to Custom Category	Run this action to include the source address, destination address, or both to a custom group in your FortiGate environment

Actions for the BlueApp for Fortinet FortiGate (Continued)

Action	Description
Add to Custom Category	Run this action to assign an asset, object, or item to a custom category
Add Address to Address Group	Run this action to add an IP address to a predefined address group
Add Address to Address Group Using Rule	Run this action to add IP address to a predefined address group based on a specified rule
Add Address to Static URL Filter	Run this action to assign an address or URL to a predefined static URL filter
Add Address to Static URL Filter Using Rule	Run this action to assign an address or URL to a predefined static URL filter using a specified rule

Note: Before launching a FortiGate response action or creating a FortiGate response action rule, the BlueApp for Fortinet FortiGate must be enabled and connected to your FortiGate instance. See Configuring the BlueApp for Fortinet FortiGate for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to send a request to your connected FortiGate instance to add source or destination IP address information to an existing FortiGate group. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch a FortiGate response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run FortiGate Action**.
5. Select the app action and fill out the fields that are populated in the window.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating FortiGate Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a FortiGate response action when events, alarms, or vulnerabilities match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically creates a new FortiGate incident when malware is detected so that a member of your response team can manage and address the issue. FortiGate events are updated on an hourly basis.

After you create a rule, new events, alarms, or vulnerabilities that match the rule, conditions will trigger the FortiGate response action to create a new incident. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about

managing orchestration rules.

Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new FortiGate response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the FortiGate incident.

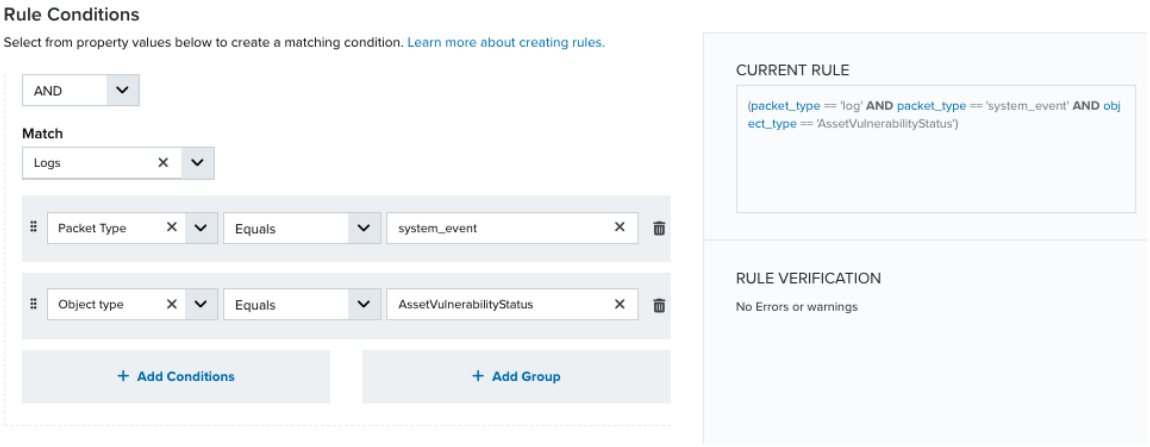
   The FortiGate parameters that you set will depend on the action that you select.

   - Create a New Incident from a Vulnerability Status Update

     This is the default action if you create the rule after applying a FortiGate response action to a vulnerability. Use this action to open a new incident when a status change occurs for a vulnerability that satisfies the matching criteria.

     Important: To match vulnerability status updates, your rule must include the following criteria: `(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus')`.

     However, it is important to be aware that this will return all vulnerability status changes matching these rules. It is advisable to narrow the rule with further conditions. Additionally, you can create a similar alarm rule first to test the amount of responses it would generate when active before you use the rule with FortiGate..



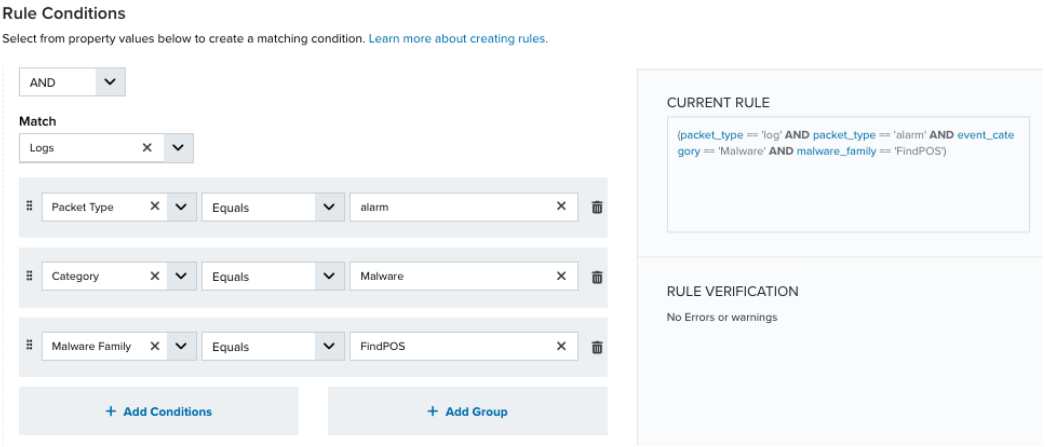
- Create a New Incident from an Alarm

  This is the default action if you create the rule after applying a FortiGate response action to an alarm. Use this action to open a new FortiGate incident for a new alarm that satisfies the matching criteria.

- Create a New Issue from Event-Based Orchestration

  Use this action to open a new FortiGate incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red

border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Fortinet FortiManager

The BlueApp for Fortinet FortiManager enables you to automate threat detection and response activities between USM Anywhere and the Fortinet FortiManager. The BlueApp for Fortinet FortiManager enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from your Fortinet ADOMs (Administration Units) and provides orchestration actions to streamline incident response activities based on risk identified in USM Anywhere.

Edition: The BlueApp for Fortinet FortiGate is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Fortinet FortiManager

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the Fortinet FortiManager App in USM Anywhere, you first need to log in to FortiManager to create an administrator account for connection with USM Anywhere.

To create the administrator account in FortiManager

1. Log in to the FortiManager graphical user interface (GUI).
2. Go to **System Settings > System Settings**.
3. On the dashboard panel, go to **Admin > Administrators** and click **Create New**.
4. In the New Administrator window, enter a name and password for the new account and enable the following settings:
   - **Admin Profile**: Super_User
   - **Administrative Domain**: All ADOMs
   - **Policy Package Access**: All Packages

- **JSON API Access**: Read-Write

5. Click **OK** to save the new administrator profile.

Connecting the BlueApp for Fortinet FortiManager in USM Anywhere

After you obtain the credentials, you must configure the connection within USM Anywhere.

To enable the BlueApp for Fortinet FortiManager

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the IP Address or FQDN.
7. Enter the username for the account you created in the FortiManager GUI.
8. (Optional) Select Validate HTTPS host name and Require CA certificate checkboxes and enter the certificate authority (CA) certificate if you want to use this option.
9. (Optional) Create a name and password for the external block list.
10. Click **Save**.

Create and Link Credentials for the External Block Lists (Optional)

The BlueApp for Fortinet FortiManager can utilize USM Anywhere to populate and manage external block lists for IP addresses, domains, and FortiGuard categories. To use the external block lists feature in USM Anywhere, you need to create a name and password in the BlueApp for Fortinet FortiManager API configurations page and enter it into your FortiManager instance. See the Fortinet documentation on Threat Feed configuration for further details.

To configure the external block list connection in FortiManager

1. Log in to the FortiManager graphical user interface (GUI).
2. Go to **Policy & Objects > Threat Feeds**.
3. Click **Create New**.
4. Select either **FortiGuard Category**, **IP Addresses**, or **Domain Name** to create a connected block list for the selected item.
5. Enter a name for the new threat feed.
6. In the URI of external resource field, your URI will be populated as follows:

   `http://192.168.1.1:0/apps/apiActions/fortiGate/getblocklist?`

   Following the question mark, you need to enter either `type=ipaddress`, `type=domain`, or `type=category`, depending on which you are creating a threat feed for.
7. Enter the username and password you created previously in the BlueApp for Fortinet FortiManager Configure API page in LevelBlue.
8. (Optional) Enter the Category ID, Refresh Rate, and Comments.
9. Click **OK** to save the new Threat Feed.
10. Repeat steps 3-9 for each block list (Category, IP Addresses, and Domain Name).

Uploading a CA Certificate (Optional)

If you leave the Require CA Certificate checkbox deselected, the BlueApp uses the browser's default trust store. When you select the Require CA Certificate checkbox, the certificate entered in the CA Certificate field takes precedence and is the only certificate trusted by the client.

There are two major use cases that might require you to upload your own certificate in the CA Certificate field:

- The firewall was deployed with a self-signed Secure Sockets Layer (SSL) certificate. A certificate like this is typically generated on the firewall at the time of deployment. In this case, you need to export that self-signed certificate from the firewall and paste it into the CA Certificate field.
- You have deployed the firewall with a SSL certificate signed by your own CA. In this case, you need to import the root and intermediate certificates, if any, from your CA. This way, the BlueApp has the same trusted certificate chain that are deployed on your firewall.

BlueApp for Fortinet FortiManager Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use Fortinet FortiManager actions to respond to the events in your environment. Rather than manually adding addresses in the FortiManager user interface (UI) and entering the relevant information, you can use the BlueApp for Fortinet FortiManager response actions to automatically manage your FortiManager firewall using information from your USM Anywhere environment. The table below shows these actions.

Example of Alarms Generated from the Fortigate AlienApp

Action	Description
Add Address to Static URL Filter	Run this action to add the source or destination address to a static URL filter in your FortiManager environment
Add Address to Address Group	Run this action to add the destination address to a group in your FortiManager environment. If the group entered doesn't exist in FortiManager, it will be created by the action from USM Anywhere
Add to Custom Category	Run this action to add an address to a group in your FortiManager environment
Add Category to External Block List	Run this action to add items to an external block list using a custom category as a filter
Add Category to External Block List	Run this action to add a category to an external block list to restrict its access
Add Domain to External Block List	Run this action to add a domain to an external block list to restrict its access
Add IP Address to External Block List	Run this action to add an IP address into an external block list to restrict its access
Add IP Address to External Block List	Run this action to add an IP address to an external block using a predefined rule to restrict its access
Get External Block List	Run this action to retrieve the external block list

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. From here, you can click one of the following tabs to display more information.
   - **Actions:**Displays information regarding the supported BlueApps actions.
   - **History:**Displays information about the executed actions.
   - **Block List-IP Address:** Displays the IP addresses in the external block list and enables you to modify them.
   - **Block List-Domain:** Displays the domains in the external block list and enables you to modify them.
   - **Block List-Category:** Displays the categories in the external block list and enables you to modify them.

Launch Actions from USM Anywhere

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to send a request to your connected FortiManager instance to add source or destination IP information from the event to existing FortiManager ADOMs. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch a FortiManager response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run FortiManager Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

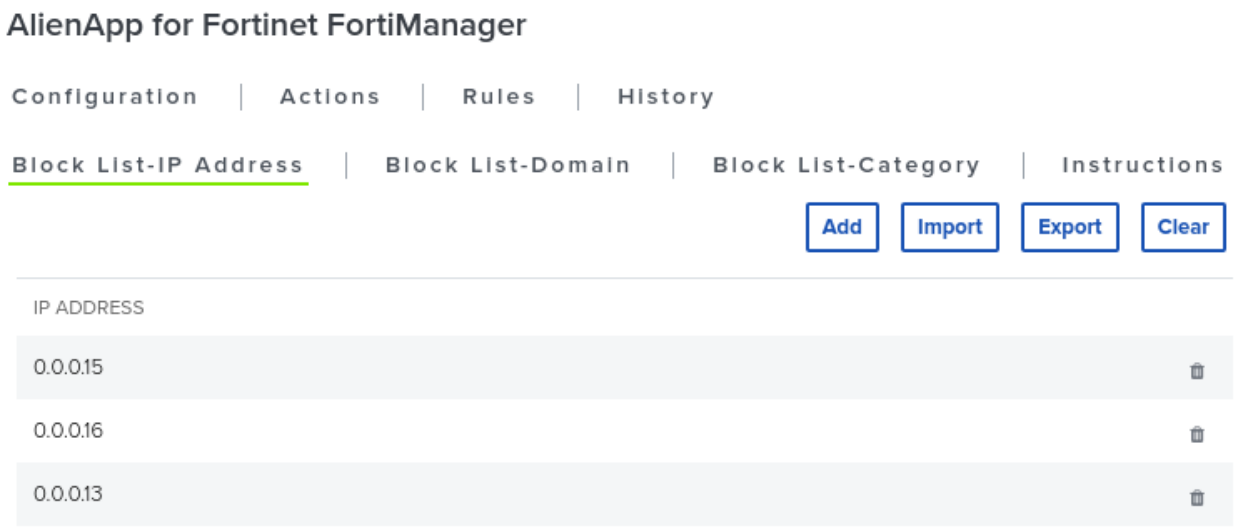
   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

External Block List

The external block lists for IP addresses, domains, and categories, are all contained in the BlueApp for Fortinet FortiManager page (**Data Sources > AlienApps > Fortinet FortiManager**). For each tab, you can see the list of all the items on the block list, and you can

remove individual items by clicking the icon next to the item. Each tab also contains three buttons above the list:

- **Add:** Opens a dialog box to add an IP address, domain, or category to the list.
- **Import:** Opens a dialog box to import a text file to import a list of IP addresses, domains, or categories to the list. This enables you to take your copied block list from another sensor and apply it to the current sensor.
- **Export:** Exports the entire IP address, domain, or category list as a downloadable .txt file. This enables you to copy your block list to another sensor.
- **Clear:** Clears the entire IP address, domain, or category list.



Creating FortiManager Response Action Rules

Role Availability | Read-Only | Investigator | Analyst | Manager

You can create orchestration rules in USM Anywhere that automatically trigger a FortiManager response action when events, alarms, or vulnerabilities match the criteria that you specify. This way, you can automate the way you filter IP addresses into the policies within the FortiManager UI.

After you create a rule, new events, alarms, or vulnerabilities that match the rule conditions will trigger the FortiManager response action to create a new incident. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new FortiManager response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the FortiManager incident.

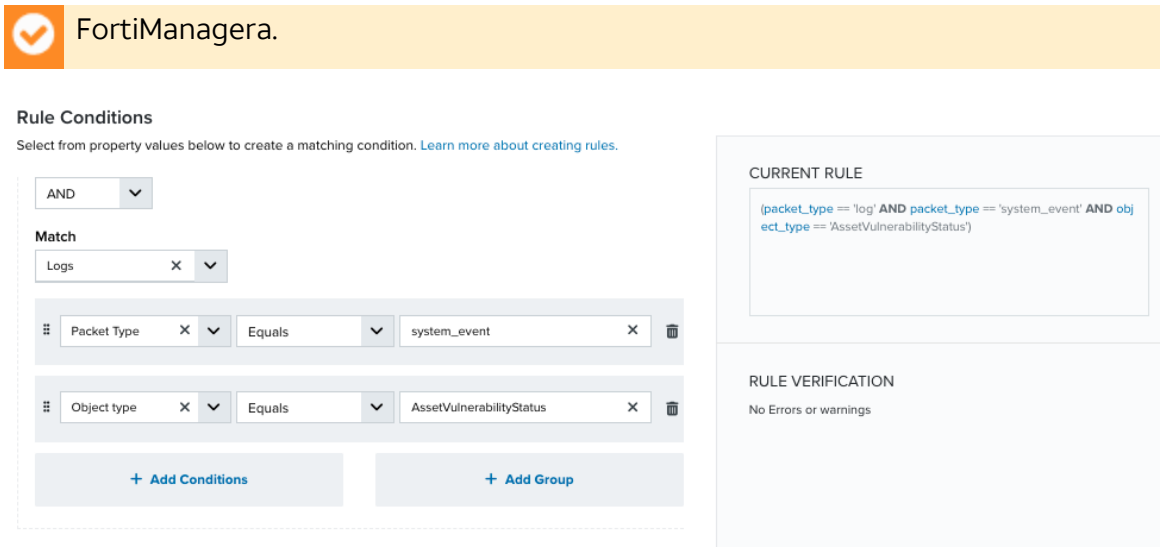
   The FortiManager parameters that you set will depend on the action that you select.

   - Create a New Incident from a Vulnerability Status Update

     This is the default action if you create the rule after applying a FortiManager response action to a vulnerability. Use this action to open a new incident when a status change occurs for vulnerabilities that satisfy the matching criteria.

     Important: To match vulnerability status updates, your rule must include the following criteria: `(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus')`.

     However, it is important to be aware that this will return all vulnerability status changes matching these rules. It is advisable to narrow the rule with further conditions. Additionally, you can create a similar alarm rule first to test the amount of responses it would generate when active before you use the rule with



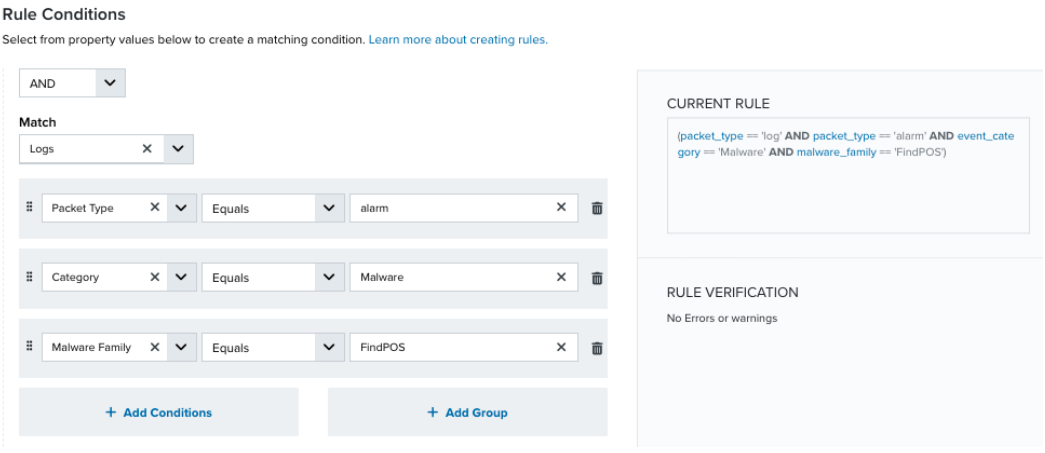
- Create a New Incident from an Alarm

  This is the default action if you create the rule after applying a FortiManager response action to an alarm. Use this action to run a new FortiManager rule for the addresses of a new alarm that satisfies the matching criteria.

- Create a New Issue from Event-Based Orchestration

  Use this action to add information to the designated FortiManager groups based on an incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the  icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for G Suite

With the BlueApp for G Suite, you can monitor your Google G Suite (formerly known as Google Apps) activity and detect threats directly from USM Anywhere, providing a single pane of glass for all your security monitoring and compliance needs. This integration gives you the ability to collect this information, extending USM Anywhere threat detection capabilities to Google Gmail, Google Calendar, and Google Drive (Google Docs, Google Sheets, Google Slides, and Google Forms).

- Predefined log collection jobs perform scheduled API queries for G Suite logs and USM Anywhere produces normalized events from this data.
- The out-of-the-box correlation rules for G Suite events enable USM Anywhere to automatically create alarms, notifying you about suspicious activity in your environment.
- The BlueApp for G Suite includes predefined dashboards that give an overview of G Suite Audit and G Suite Drive to streamline your investigation and incident response processes.

Important: All G Suite environments include access to the Google Drive Activity API, which provides the basic G Suite audit log data. However, only G Suite Enterprise or G Suite Business include access to the Reports API, which provides to the advanced G Suite log data. If you are a G Suite Basic customer, you cannot collect log data for Google Drive.

See their Google Support site for more information about the differences between the G Suite editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for G Suite

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

After you configure the connection between the BlueApp for G Suite for a deployed USM Anywhere Sensor and your Google G Suite environment, the predefined log collection jobs perform scheduled queries for events. When USM Anywhere collects and analyzes the first of these events, the G Suite Audit and G Suite Drive dashboards are available in the Dashboard menu (according to the types of collected events).

Note: Currently, the BlueApp for G Suite supports the connection of one G Suite account per USM Anywhere Sensor. If you have more than one G Suite account that you want to monitor in USM Anywhere, you must configure each for a different sensor.

When configuring your BlueApp for G Suite, you have the option of configuring it to collect logs through BigQuery as well. Adding this additional log collection can provide you enhanced insight into your security posture with visibility into things like phishing attacks.

Important: If you choose to enable BigQuery log collection, you must complete all of the following BigQuery configuration steps. If you do not wish to enable BigQuery log collection, none of the BigQuery-related steps are necessary to configure your BlueApp for G Suite.

Set Up the Google Service Account

As a Google administrator, you must create a new project in your Google Developers Console and create a service account in the Google API Console to support server-to-server interactions. See Using OAuth 2.0 for Server to Server Applications for more information about server-to-server authentication in Google.

As you complete the following setup tasks, you must collect these items to complete the integration with the BlueApp for G Suite:

- Client identification (Unique ID) for the service account
- G Suite admin user email address
- Private key file, which is saved to your computer when you create the service account and the key

Important: You must have administrative privileges to configure G Suite for integration with the BlueApp for G Suite. Ask your Google administrator for these privileges.

Service Account Creation

Create a service account according to the instructions in the G Suite Administrator Help page. Pay attention to these specifics:

- In *Step 2: Enable the APIs*, enable the following:
  - Admin SDK
  - (BigQuery.) Gmail API
  - (BigQuery.) Groups Migration API
  - (BigQuery.) BigQuery API
  - (BigQuery.) BigQuery Connections API
  - (BigQuery.) BigQuery Data Transfer API
- *Step 3: Set up the OAuth consent screen* is optional.
- In *Step 4: Create the service account*, do the following:
  1. For key type, select **P12** and then click **Create** (item 8 in the article).

     A dialog box opens informing you that the private key has been saved to your computer. It also displays the password for the private key.
  2. Copy the password and store it in a secure location.

Note: The following two steps are optional because this information will be configured automatically as you complete your BigQuery setup.

3. (BigQuery.)In the *Select a role* section, select **BigQuery** from the drop-down list and then **BigQuery Admin**.
4. (BigQuery.) In the *Grant users access to this service account* section, add **gapps-reports@system.gserviceaccount.com**.

Domain-Wide Authority Delegation

Follow the steps listed in the *Delegating domain-wide authority to the service account* section of Using OAuth 2.0 for Server to Server Applications.

In Step 5, enter the following OAuth scopes:

```
https://www.googleapis.com/auth/admin.reports.audit.readonly
https://www.googleapis.com/auth/admin.directory.domain.readonly
https://www.googleapis.com/auth/admin.directory.user.readonly
https://www.googleapis.com/auth/bigquery
```

Warning: Whether you are configuring BigQuery log collection or not, the BigQuery OAuth scope is required for your app to function.

Important: Adding the client and scopes in the G Suite console can be subject to a propagation time, which could be up to two hours. If you use the Check Connections tool for your G Suite platform in CloudMigrator, it may not be successful immediately.

Complete Your BigQuery Setup

If you are completing the optional BigQuery log collection enhancement to your BlueApp for G Suite, complete the following two tasks before proceeding with your AlienApp configuration.

Note: See Google's documentation for further details about the instructions below.

To create a dataset for your BigQuery log collection

1. Navigate to **BigQuery** in your Google Cloud Platform (GCP) console, and then select **SQL Workspace**.
2. Select the project you intend to use for this log collection, and then click **Actions >**

Create Dataset.

3. When prompted, enter a unique dataset ID.
4. Click **Save**.

Grant Google Gmail access to your BigQuery log collection

1. Navigate to **Apps** in your GCP console, and then go to **Google Workspace > Settings for Gmail > Setup**.
2. Click **Enable Email Logs in BigQuery**.
3. Use the drop-down list to select your project.
4. Specify a unique name for your dataset.
5. Click **Save**.

Connecting the BlueApp for G Suite

After you create the new service account in Google G Suite and enable the Admin Software Development Kit (SDK), you must configure the connection within USM Anywhere.

Important: Adding the client and scopes in the G Suite console can be subject to a propagation time, which could be up to two hours. The BlueApp for G Suite connection configuration might not be successful immediately if these resources are not yet accessible.

To enable the BlueApp for G Suite

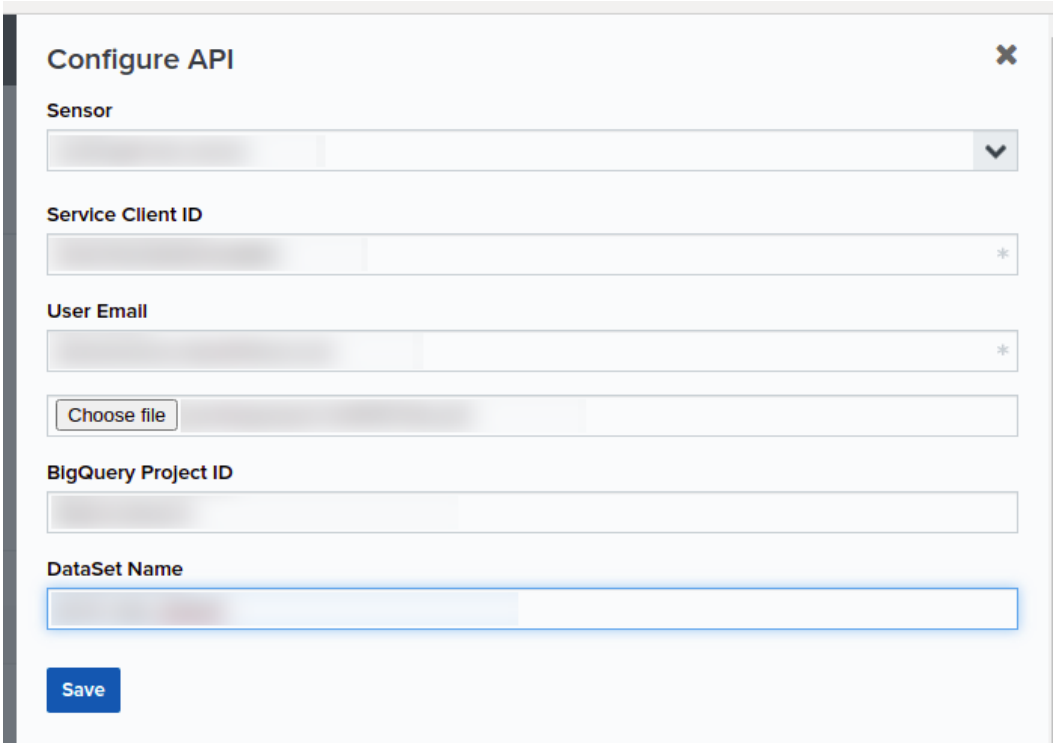
1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. In the Service Client ID field, enter the unique identification (ID) for the Google service account you created.
7. In the User Email field, enter the G Suite admin user email address.

   Note: The G Suite admin user is the account you use to sign in to your Google Admin console. You cannot use the email address of the service account created for this integration.

8. (BigQuery.) Under *BigQuery Project ID*, enter the ID of the Google Cloud Platform (GCP) project you used to configure BigQuery.
9. (BigQuery.) Under *DataSet Name*, enter the unique name you specified in Complete Your BigQuery Setup.
10. (Optional.) Click **Choose File** to upload the P12 private key file for the Google service account you created.



11. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Jira

The BlueApp for Jira streamlines incident response activities by automatically opening Atlassian Jira issues in response to threats detected by USM Anywhere. Upon execution of the action, USM Anywhere generates the Jira issue and populates the subject and description fields with details from an alarm, event or vulnerability.

Important: The BlueApp for Jira integration works with the Cloud deployment of Jira Service Desk and Jira Software. The Server deployment (self-managed) is not currently supported.

With a configured BlueApp for Jira connection to your Jira instance, you can simplify the response execution process for threats identified in USM Anywhere.

Edition: The BlueApp for Jira is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Jira

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

When the BlueApp for Jira is enabled and connected to your Atlassian Jira Service Desk or Jira Software instance, you can launch response actions and create response action rules to send data from USM Anywhere to the instance and create new issues. See BlueApp for Jira Actions for more information about the response actions supported by the BlueApp for Jira.

Important: The BlueApp for Jira integration works with the Cloud deployment of Jira Service Desk and Jira Software. The Server deployment (self-managed) is not currently supported.

BlueApp for Jira Requirements

Before you configure the BlueApp for Jira, make sure you have these integration requirements.

- Fully-qualified domain name (FQDN) for your Jira instance
- User account that USM Anywhere will use to access the Jira instance

  This user account must have access to the projects where you want to create issues from threats detected by USM Anywhere and rights to create an API token.

Note: Depending on the way that you want the BlueApp for Jira to fit into your processes, you should determine if you want to use an existing user account or create a new user account in your Jira instance to be used exclusively for USM Anywhere.

If you are an analyst and you are manually opening issues in response to alarms and vulnerabilities, it may be appropriate to use the same account that you use to manage issues in the Jira user interface (UI). However, if you plan to use rules primarily to generate issues automatically, a user account that is specific to USM Anywhere works well and makes it easy to filter these issues in Jira dashboards.

Get Your API Token in Jira

Before you can use the BlueApp for Jira to collect and analyze Jira log data within USM Anywhere, you must have an API token that can be used to connect to the Jira APIs. Jira issues an API token for a specific user account and all requests with that token act on behalf of that user.

To acquire an API token for Jira

1. Go to the Manage API tokens for your Atlassian account page and follow the vendor instructions to generate the token.
2. Copy the token to be entered in USM Anywhere.

Important: If you generate a new API token or key at some point in the future, it will revoke the existing token making the connection unauthorized. Therefore, you must update the token in USM Anywhere accordingly.

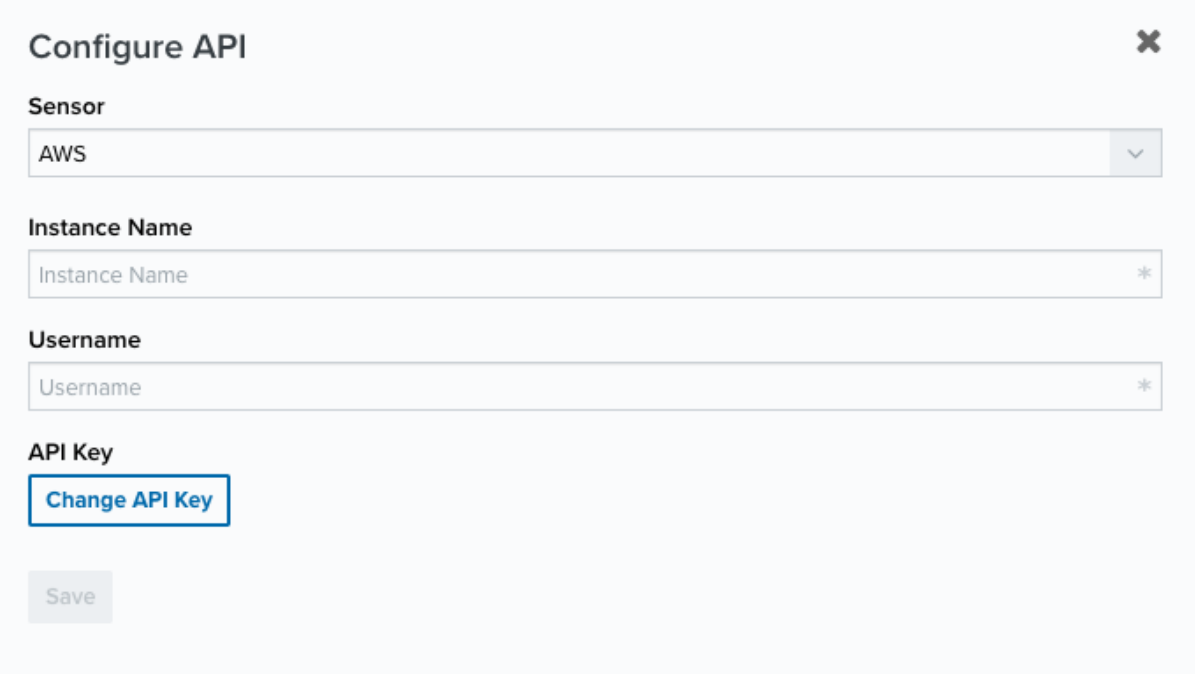
Configure the Jira Connection in USM Anywhere

To support the response actions in USM Anywhere, you must configure a connection with the Jira instance. This connection enables the BlueApp to perform operations using the Jira Representational State Transfer (REST) APIs. The user account that you use for the connection requires Create and Read permissions for one or more Jira projects where you want to create new issues from USM Anywhere.

To configure the Jira connection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Specify the connection information for Jira:

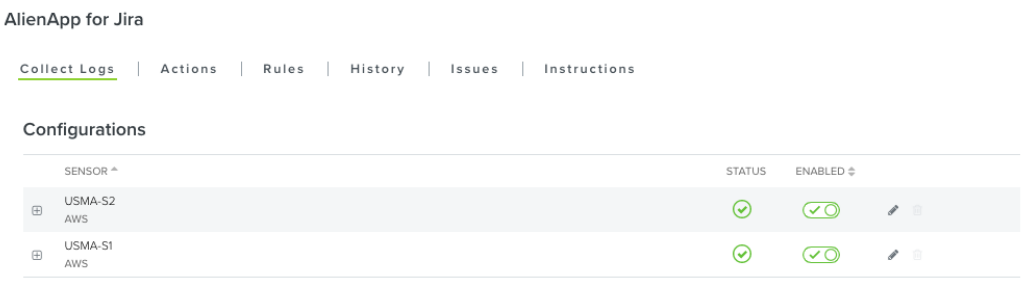


- **Instance Name**: Enter the FQDN for your cloud-based instance. For example, if you access your cloud-based instance at https://mycorp.atlassian.net, you must enter **mycorp.atlassian.net** in this field.
- **Username**: Enter the email address for the account you used to create the API token. USM Anywhere uses this as the username to access your cloud-based instance.
- **API Key**: Click **Change API Key** and enter the API token created with the account.

In the Set Available USM Anywhere Attributes section, select the checkboxes for the options you want to make available for populating the ticket information in Jira when you create a response action rule.

7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Jira instance and the APIs, a icon displays in the Health column.



If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Jira connection.

BlueApp for Jira Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, your team determines which items require the opening of a new Atlassian Jira issue. Rather than manually opening each issue in the Jira user interface (UI) and entering the relevant alarm, event, or vulnerability information, you can use the BlueApp for Jira response actions to automatically create the Jira issue with the subject and description fields pre-populated with content from your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Jira

Action	Description
Create New Issue from Alarm	Run this action to generate a new Jira issue directly from an alarm This action is available when you launch a response action directly from an alarm or a response action in an orchestration rule
Create New Issue from Vulnerability	Run this action to generate a new Jira issue or task directly from a vulnerability This action is available when you launch a response action directly from a vulnerability

Actions for the BlueApp for Jira (Continued)

Action	Description
Create New Issue from Event	Run this action to generate a new Jira issue directly from an event This action is available when you launch a response action directly from an event
Create New Issue from Event Based Orchestration Rule	Run this action to generate a new Jira issue directly from an orchestration rule that triggers from a matching event This action is available when you launch a response action in an orchestration rule
Create New Issue	Run this action to initiate the creation of a new issue for tracking and managing a specific item
Create New Issue from Vulnerability Status Update	Run this action to initiate the creation of a new issue based on a status update from a vulnerability assessment

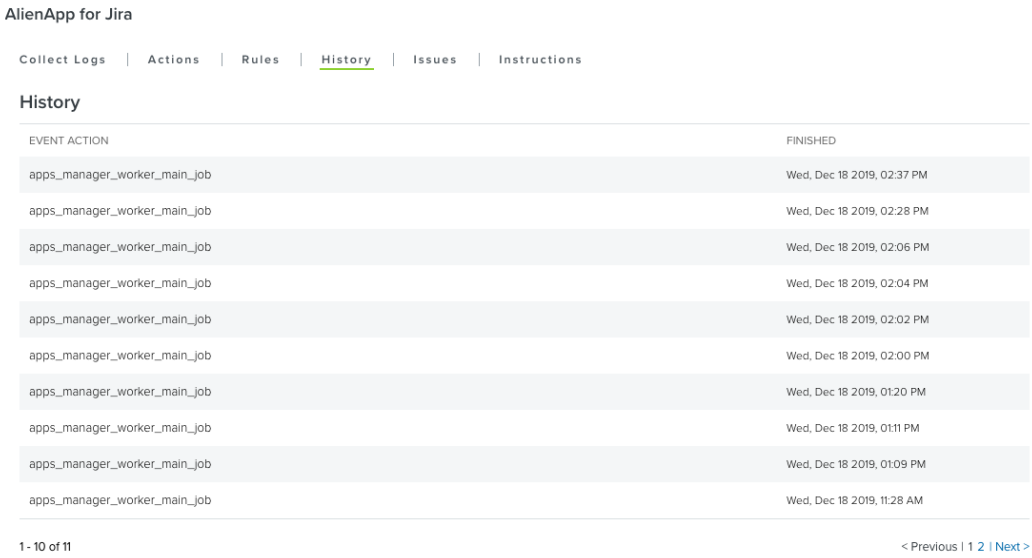
Upon execution of a response action, USM Anywhere generates the Jira issue and passes the associated information to that new issue.

Note: Before launching a Jira response action or creating a Jira response action rule, the BlueApp for Jira must be enabled and connected to your cloud-based Jira instance. See Configuring the BlueApp for Jira for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.

4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed actions.



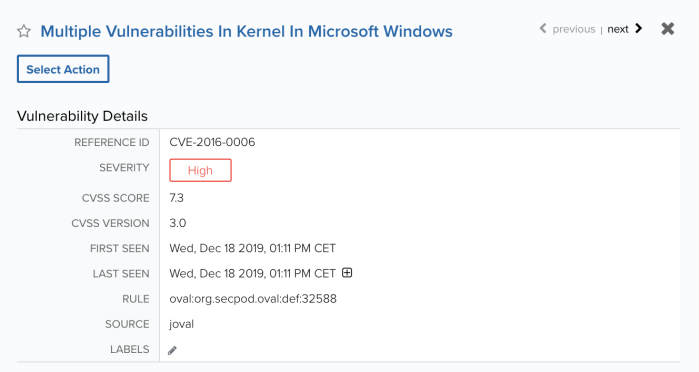
Launch Actions from USM Anywhere

You can launch an action directly from alarms, events, or vulnerabilities. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm, event, or vulnerability.

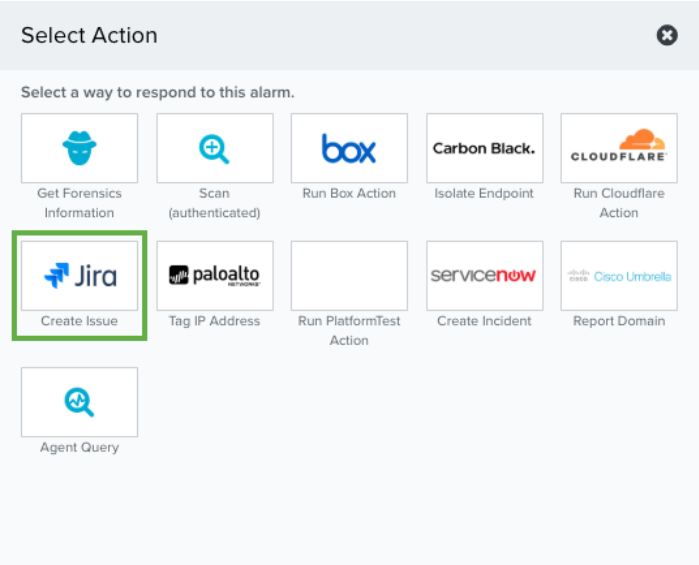
Note: Before launching a Jira response action, the BlueApp for Jira must be enabled and connected to your Jira instance. See Configuring the BlueApp for Jira for more information.

To launch a Jira response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.



4. In the Select Action dialog box, select the **Jira** tile.



This displays the options for the selected response app.

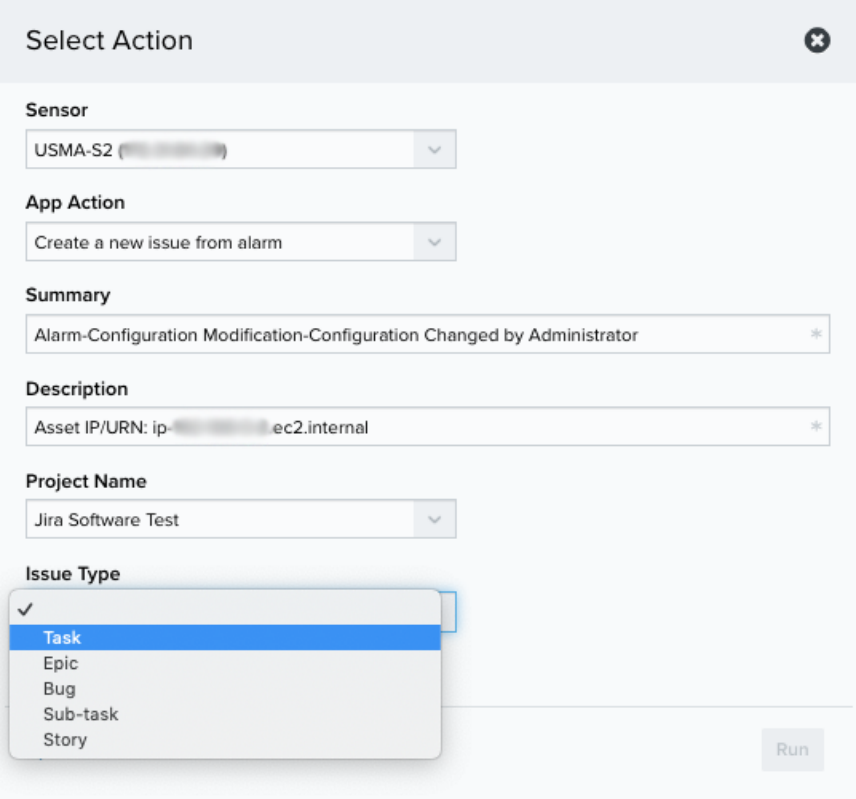
5. (Optional.) If you have more than one USM Anywhere Sensor configured for the BlueApp for Jira, use the Select Sensor option to set the sensor that you want to use for the rule.
6. Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
7. Define the information included in the new Jira issue:

- **Project Name**: Select the name of the Jira project for ticket to be created in.
- **Issue Type**: Select the issue type of the ticket.
- **Short Description**: By default, this field contains the name of the alarm, event, or vulnerability. This is the text that populates the summary (heading) for the new Jira issue. You can change the text in this field before you run the action, if needed.
- **Description**: Enter information in this field to populate description field for the Jira issue. Typically, this information describes what needs to be done to complete the open issue.
- **Priority**: Assign the priority for the ticket created.
- **Components**: Enter the component to be listed on the ticket. (Only available if the Jira Project is selected.)
- **Assignee**: Enter the name of the user the ticket will be assigned to, or enter part of the name and select the user from the auto-complete list. (Only available if the Jira Project is selected.)

8. Set the Project Key for the project where you want to create the new issue.

   The projects that are available for selection will depend on the projects that are permitted for the user account configured for the BlueApp for Jira.

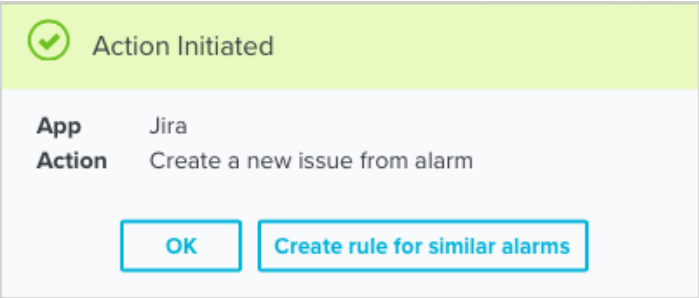
9. Set the Issue Type for the new issue.



The issue types that are available for selection will depend on the types configured in your Jira instance for the selected project

10. Click **Run**.

    After USM Anywhere initiates the action, it displays a confirmation dialog box.



    If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Jira Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Jira response action when events match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically creates a new Jira task when malware is detected so that a member of your response team can manage and address the issue. Response Action rules can also be configured to populate Jira tickets with information from USM Anywhere.

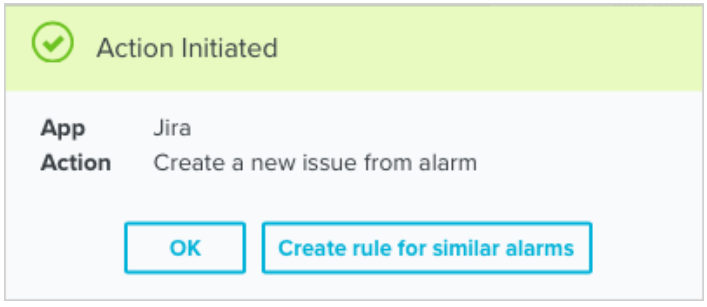
After you create a rule, new alarms or events that match the rule conditions will trigger the Jira response action to create a new issue. The rule does *not* trigger for your existing alarms or events.

Note: Before launching a Jira response action or creating a Jira orchestration rule, the BlueApp for Jira must be enabled and connected to your cloud-based Jira instance. For more information, see Configuring the BlueApp for Jira.

You can create a new rule in one of two ways:

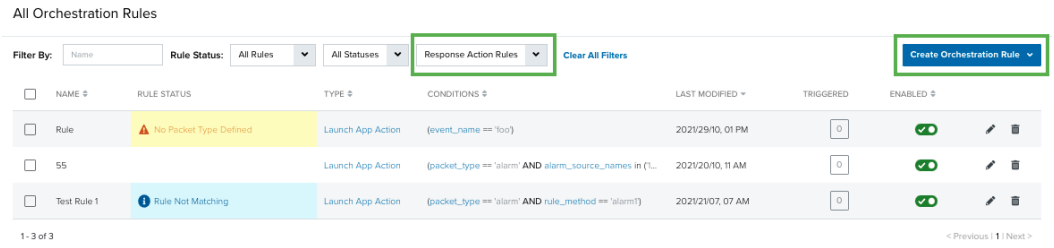
- **From an Applied Response Action**: You can automatically create a rule using the response action that you apply to an existing alarm. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

  In the confirmation dialog box, click **Create rule for similar alarms** or **Create rule for similar events**.



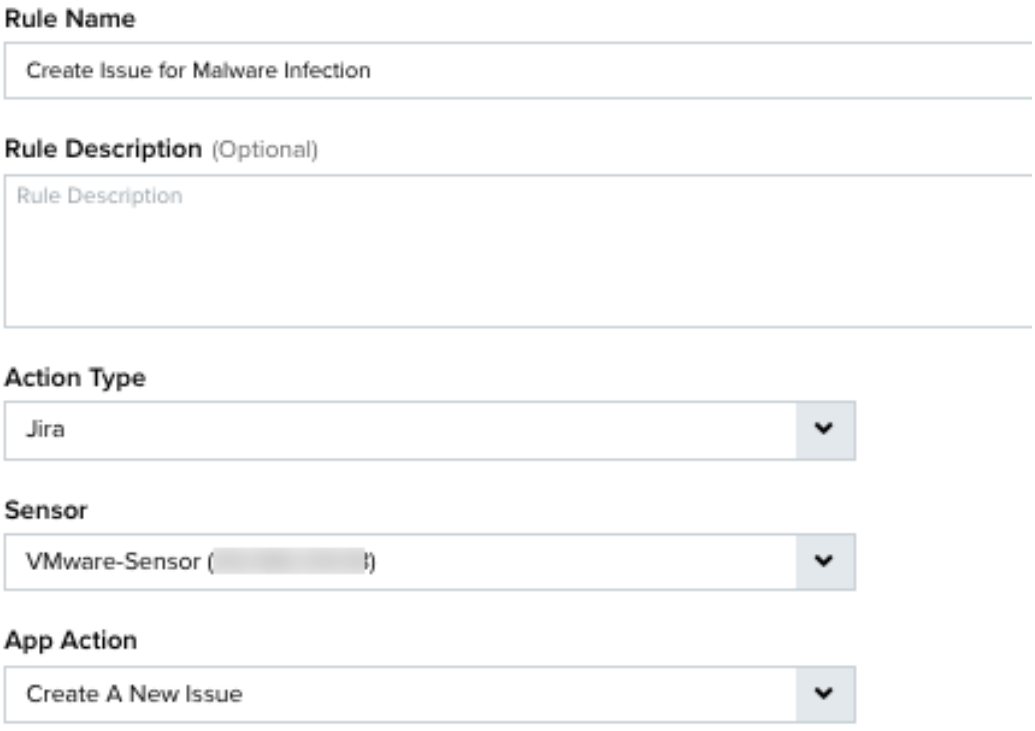
- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click **Create Orchestration Rule > Response Action Rule** to define the new rule.



To define a new Jira response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the Jira issue.



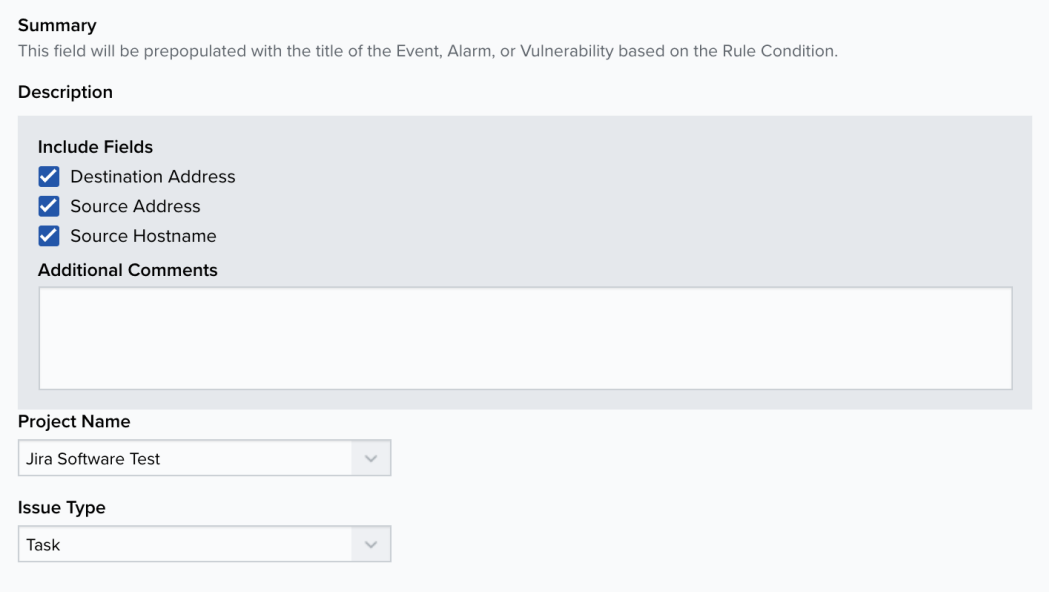
The Jira Parameters that you set will depend on the action that you select:

Create a new issue from alarm

This is the default action. Use this action to trigger the rule for alarms that satisfy the matching criteria. For this response action, the information fields contain default values that will automatically generate information based on the alarm that triggers the rule.

The Summary field generates the Jira issue summary text using the strategy and method identified in the alarm.

The Description field generates the Jira issue description text using the identified source for the alarm.

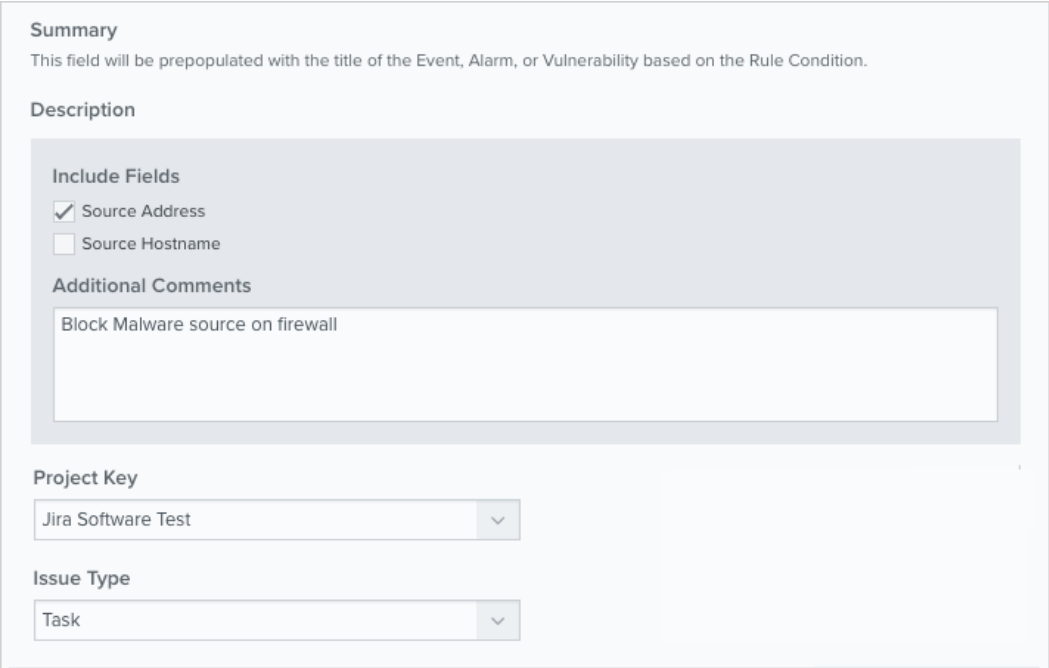


Create a new issue from event based orchestration

Use this action to trigger the rule for any event that satisfies the matching criteria. It uses the title of the alarm, event, or vulnerability that triggers the rule to populate the summary text for the Jira issue.

Set the Description options to define the information populated in the description field of the Jira issues:

- **Source Address**: Select this checkbox to include the source address for the event.
- **Source Hostname**: Select this checkbox to include the source hostname for the event.
- **Additional Comments**: Enter any additional information that you want to include in the description field of the Jira issue.



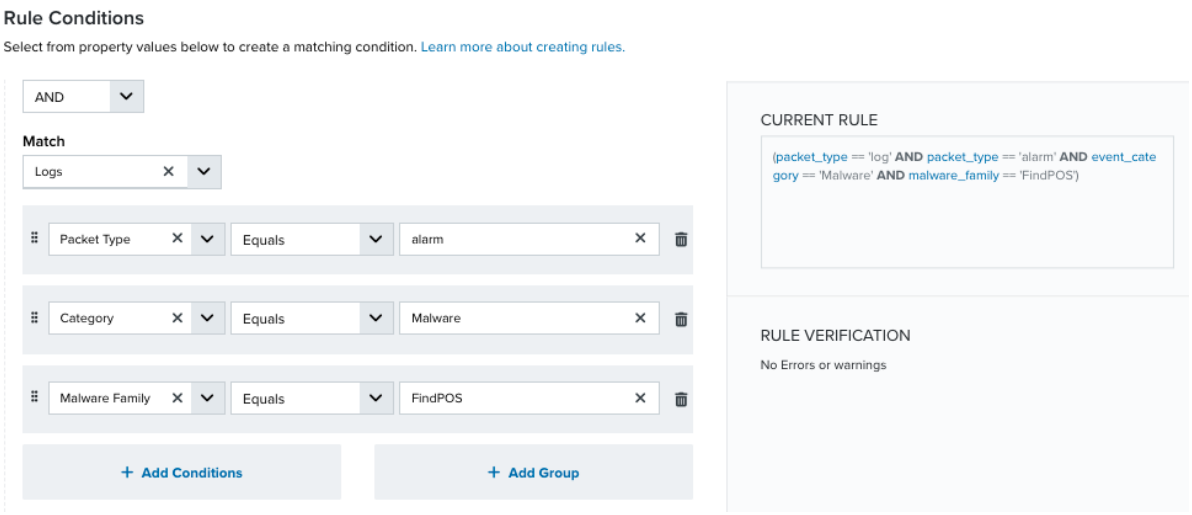
3. Set the Project Name for the project where you want to create the new issue.

   The projects that are available for selection will depend on the projects that are permitted for the user account configured for the BlueApp for Jira.

4. Set the Issue Type for the new issue.

   The issue types that are available for selection will depend on the types configured in your Jira instance for the selected project

5. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

6. Click **Save Rule**.
7. Click **OK** in the confirmation dialog box.

Managing Your Jira Issues

Role Availability ✔ Read-Only ✔ Investigator ✔ Analyst ✔ Manager

After the BlueApp for Jira is configured and users execute the supported actions directly or through an orchestration rule, you can easily view a list of the Jira issues created by USM Anywhere and look at the events, alarms, and vulnerabilities related to the executed actions.

Viewing Jira Issues Created by USM Anywhere

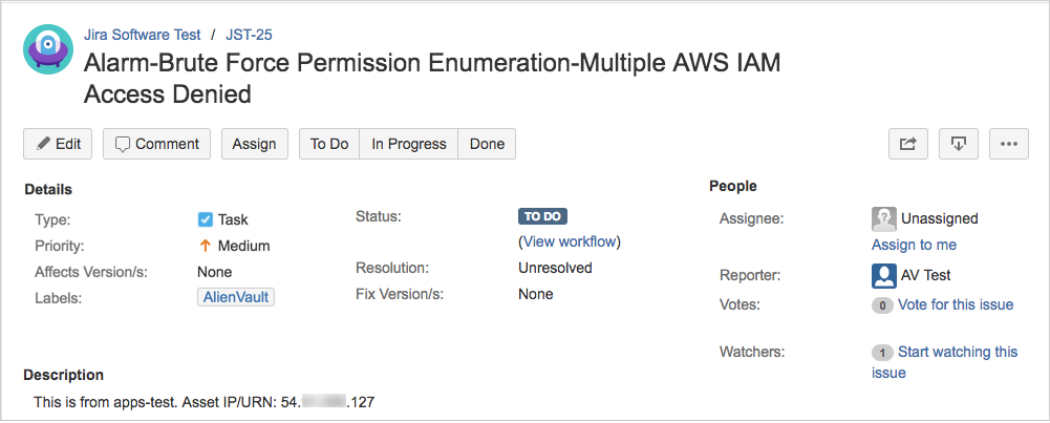
The Issues list includes all issues created by an action applied directly to an alarm, event, or vulnerability, as well as any from actions that were triggered by an orchestration rule. From this list, you can open the issue in your cloud-based Jira instance to view additional information about the issue or make updates to the issue, such as assigning the item to a team member or changing the priority.

To access the Jira issues

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Issues** tab.

   The displayed list includes all Jira issues generated by USM Anywhere, with the most recently opened issues at the top. Here you can view the status and assignment for the issue as reported by your Jira instance.

5. Click **View** to open the incident in the Jira user interface (UI).



In Jira, you can assign the issue, change its status, or perform any of the functions supported in the Jira project.

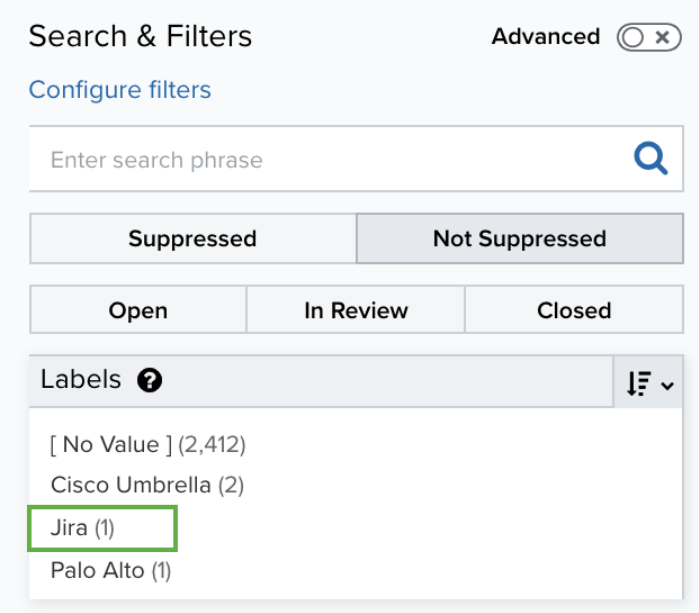
Filtering the Labeled Alarms and Vulnerabilities

USM Anywhere uses labels as a mechanism to classify alarms and vulnerabilities. These labels make it easy to filter items by label so that you can locate them easily and track their status. When the BlueApp for Jira executes a response action for an alarm or vulnerability, it automatically applies the *Jira* label to it. You can use this label as a filter so that a page displays data for only those items related to an BlueApp for Jira response action.

To view Jira action alarms or vulnerabilities

1. Open the Alarms page or Vulnerabilities page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

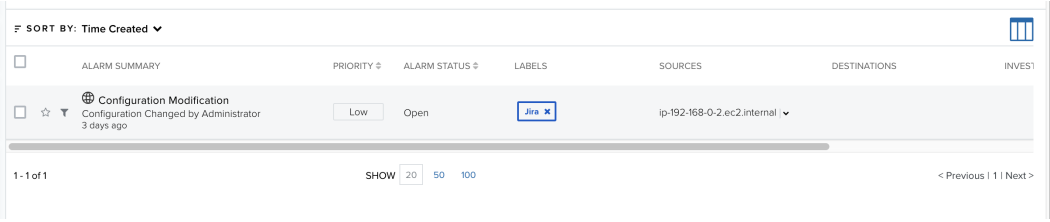
   USM Anywhere includes several filters displayed by default.
3. Locate the Labels filter and select **Jira**.



If the Labels filter is not displayed, click **Configure Filters** at the bottom of the Search & Filters pane to configure filters for the page. See Managing Filters in the *USM Anywhere*

User Guide for more information about configuring filters for the page display.

In the displayed list, you can scroll the list to the right and view the Labels column.



BlueApp for Lookout

Lookout is one of the leaders in mobile threat defense. The BlueApp for Lookout enhances the threat detection capabilities of USM Anywhere by collecting and analyzing log data from the Lookout console to provide a single-pane-of-glass experience for the mobile space.

Edition: The BlueApp for Lookout is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Lookout

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

To configure the BlueApp for Lookout in USM Anywhere, you need to have an API key to authenticate communication with Lookout.

Set up the Lookout API

Before you can use the BlueApp for Lookout with USM Anywhere, you must have an API token that USM Anywhere can use to connect to your Lookout server. Lookout generates this token for use by your user account.

To acquire the API token for Lookout

1. Log in to the Lookout console as an administrator.
2. In the left navigation menu, go to **System > Application Keys**.

> **Note:** If you do not see the Application Keys tab, contact Lookout Enterprise Support to enable this feature on your application.

3. Click **Generate Key**.
4. Enter a label name, and then click **Next**.
5. Copy the generated key by clicking **Click to Copy Application Key to Clipboard**.

> **Warning:** Copy the generated key to your application immediately or save it locally as you cannot access the key again after this procedure.

> **Important:** If you generate a new API key at some point in the future, it will revoke the existing token making the connection unauthorized. Therefore, you must update the token in the BlueApp for Lookout accordingly.

Configure the BlueApp for Lookout in USM Anywhere

After you generate a Lookout API token and copy the value, you're ready to enable the BlueApp for Lookout in USM Anywhere.

To enable the BlueApp for Lookout

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is

important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the API token you acquired from Lookout.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for McAfee ePO

The BlueApp for McAfee ePO provides functional support to monitor your McAfee ePolicy Orchestrator (ePO) activities directly in USM Anywhere. This integration analyzes log data from ePO and provides alerts for intrusions, malicious IPs, suspicious activities, and more.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for McAfee ePO

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

The BlueApp for McAfee ePO connects to the Microsoft SQL database within your McAfee ePolicy Orchestrator (ePO) to retrieve and ingest data for analysis in USM Anywhere. After USM Anywhere analyzes the first of these events, the McAfee ePO dashboard is available.

Requirements

To configure the BlueApp for McAfee ePO, you must add a scheduled job in USM Anywhere that collects data directly from the SQL database in your McAfee ePO. Before you do this, there is information about your database that is required to make the connection:

- Hostname or IP address of the SQL database
- Port number (usually 1433) that is open for the connection
- The database name
- Username and password used to log in to the SQL database

> **Important:** This is the Microsoft SQL Server account and not the Microsoft Windows user account. The BlueApp for McAfee ePO uses SQL Server authentication over Windows Authentication.

- User account has read permission for the EPOEvents table

Creating a Scheduler Job for McAfee ePO

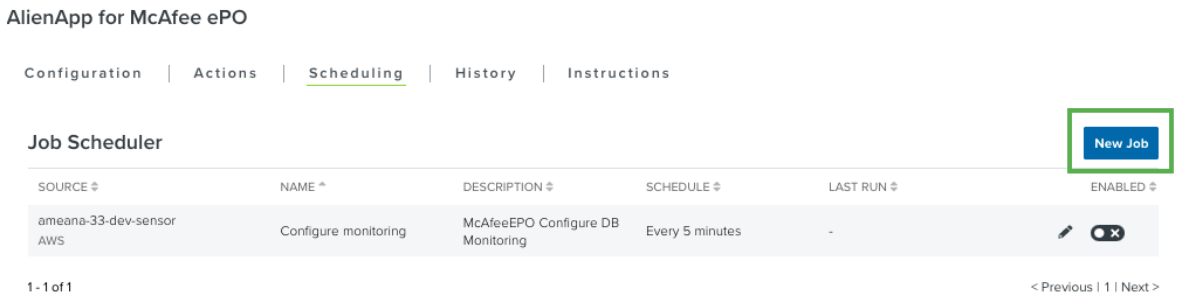
The BlueApp for McAfee ePO page provides easy access to define a new log collection job to retrieve your McAfee ePO event data. After you create the new job, you can make changes to the parameters for the scheduled job or review its history in the Scheduler page. See USM Anywhere Scheduler in the *USM Anywhere User Guide* for more information about working with scheduled jobs.

> **Note:** Unlike other apps, the McAfee ePO app allows multiple scheduler jobs to be configured to run against the same sensor.

To schedule a McAfee ePO job

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Scheduling** tab.

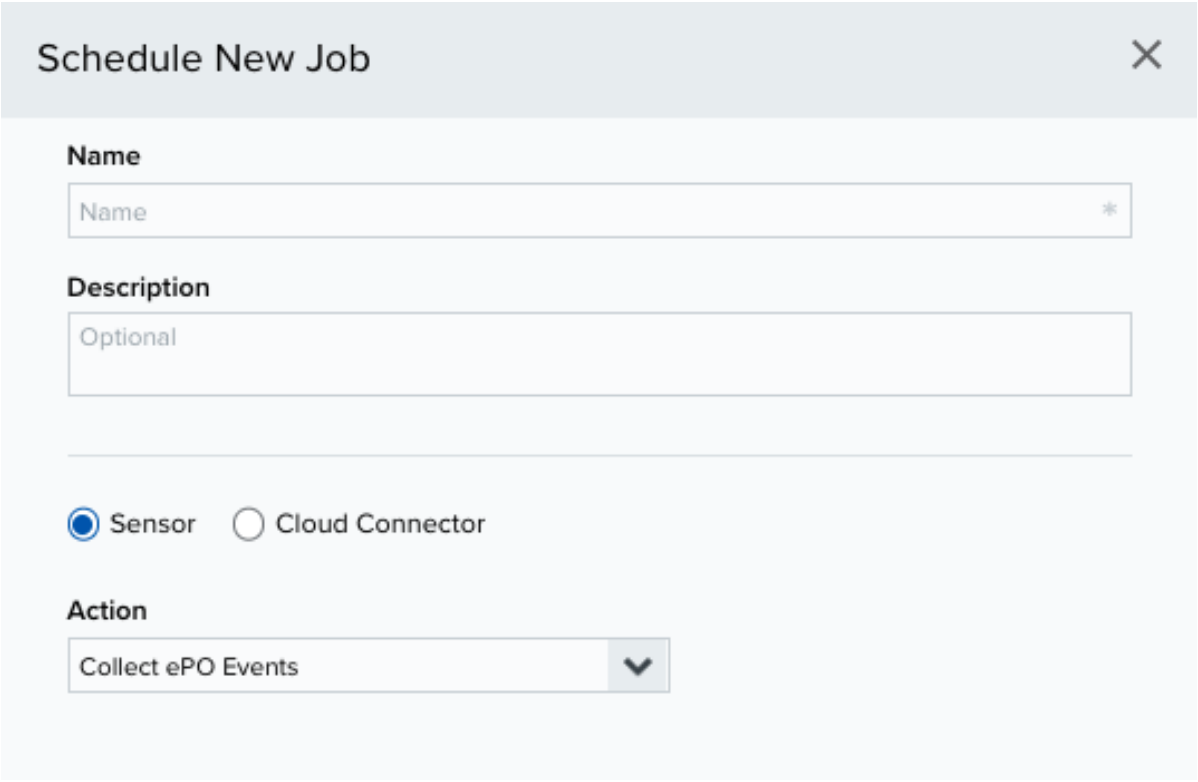
5. Enable an existing job or click **New Job**.



If you click **New Job**, the Schedule New Job dialog box opens with the options defined for an BlueApp for McAfee ePO job.

6. Enter the name and description for the job.

   The description is optional, but it is a best practice to provide this information so that others can easily understand what it does.



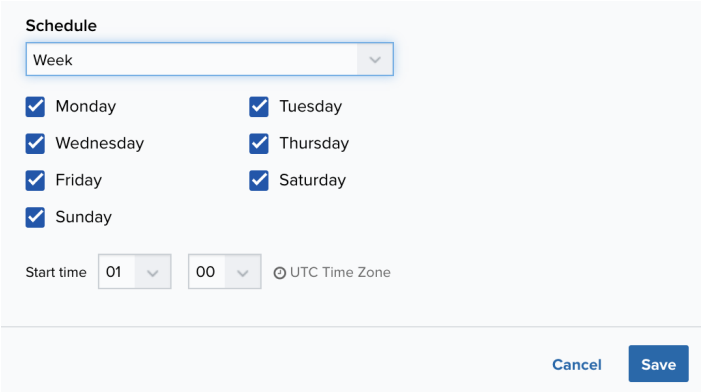
7. Select **Sensor** as the source for your new job.

8. Select an Action from the dropdown menu.
   - **Collect ePO Events**: Schedules one job to collect ePO events from the sensor.
   - **Configure monitoring (not encrypted)**: Schedules multiple jobs each monitoring one database.
9. If you selected *Collect ePO Events*, complete the following configuration steps:
   1. In the Schedule section, specify when USM Anywhere runs the job:
      a. Select the increment as **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

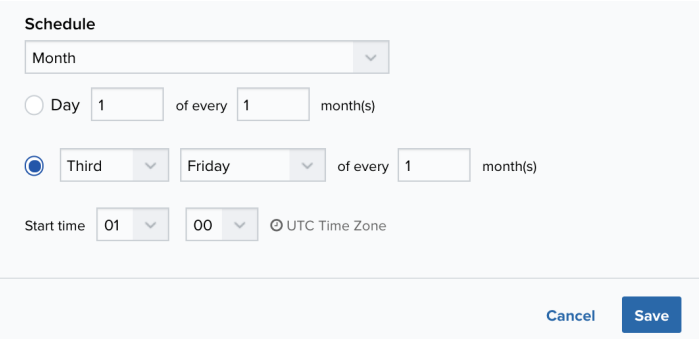
      Warning: After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See USM Anywhere System Monitor for more information.

      b. Set the interval options for the increment.

      The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.



Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.



Important: USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

c. Set the start time.

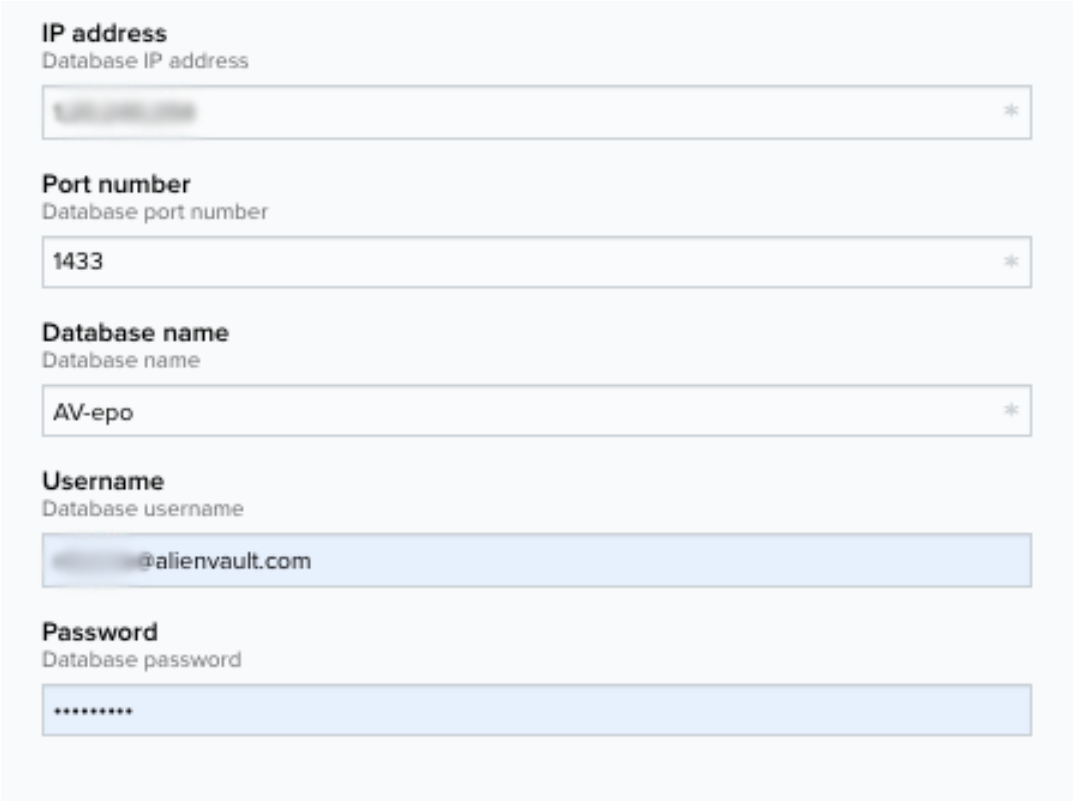
   This is the time that the job starts at the specified interval. It uses the time zone configured for your USM Anywhere instance (the default is Coordinated Universal Time [UTC]).

2. Click **Save** to save your new scheduled job.

10. If you selected *Configure Monitoring*, complete the following configuration steps for each individual database you wish to monitor:

Warning: If you select this action, the username and password you configure for the database will be stored and passed unencrypted.

1. Enter the McAfee ePO database connection information:



   - In the IP address field, enter the IP address of the ePO server SQL database.
   - In the Port number field, enter the port number on which the ePO server SQL database listens.
   - In the Database name field, enter the name of the ePO server SQL database.
   - In the Username and Password fields, enter the credentials you use to access the ePO server SQL database.

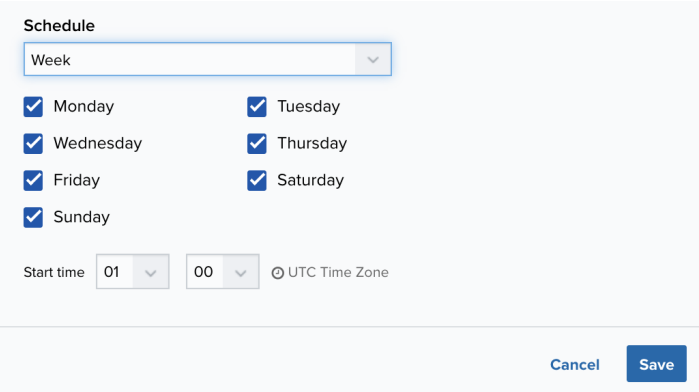
2. In the Schedule section, specify when USM Anywhere runs the job:

   a. Select the increment as **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

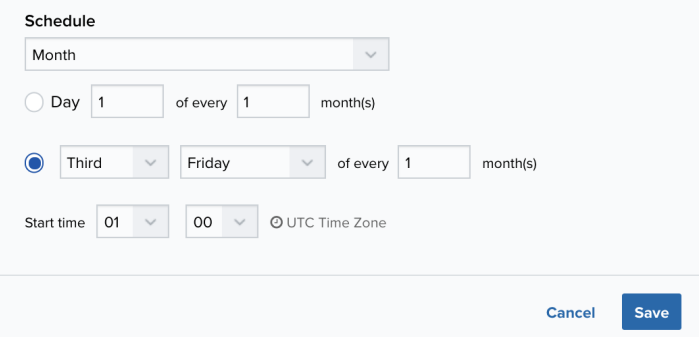
   Warning: After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See USM Anywhere System Monitor for more information.

   b. Set the interval options for the increment.

The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.



Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.



Important: USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

c. Set the start time.

   This is the time that the job starts at the specified interval. It uses the time zone configured for your USM Anywhere instance (the default is Coordinated Universal Time [UTC]).

3. Click **Save**.

After the scheduled job runs, you should start seeing new events in USM Anywhere originating from the ePO server SQL database.

BlueApp for Microsoft Defender ATP

The AlienApp for Microsoft Defender Advanced Threat Protection (ATP) enables you to leverage your Microsoft Azure logs to prevent, detect, investigate, and respond to advanced threats in your USM Anywhere environment. The BlueApp generates events by querying the Microsoft Defender for Endpoint APIs or receiving events from the Azure Event Hubs.

Edition: The BlueApp for Microsoft Defender ATP is available in the Standard and Premium editions of USM Anywhere.

See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Microsoft Defender ATP

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

Before you configure the BlueApp for Microsoft Defender Advanced Threat Protection (ATP), you must have the following information from your Microsoft Azure account:

- Defender Tenant ID
- Application ID
- Scope
- Client Secret

See the Microsoft Defender ATP setup documentation for full details on creating an app to retrieve the aforementioned information.

To ensure successful configuration, you must select the following permissions for your app:

- Alert.Read.All
- Machine.Isolate
- Machine.StopandQuarantine
- Ti.ReadWrite.All
- Machine.Read.All

- Machine.Scan
- SecurityAlert.Read.All
- SecurityIncident.Read.All

BlueApp for Microsoft Defender ATP Configurations

To set up the BlueApp for Microsoft Defender ATP, you first need to create an Azure Active Directory (Azure AD) application and record your Tenant ID, Application ID, Scope, and Client Secret during that process.

To enable the BlueApp for Microsoft Defender ATP

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the following items:
   - Application ID
   - Tenant ID
   - Scope
   - Client Secret
7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Microsoft Defender ATP APIs, a  icon displays in the Health column.

If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Microsoft Defender ATP connection.

Collect Logs from Microsoft Defender ATP

There are two ways to collect logs from Microsoft Defender ATP:

- Through the Microsoft Defender for Endpoints API
- From Azure Event Hubs.

Important: Do not configure both methods because it will create duplicate events.

The API Method

For the API method, since you've already connected to the API when configuring the BlueApp for Microsoft Defender ATP, the remaining task is to enable the log collection scheduler job in USM Anywhere.

To collect logs using the API

1. In the USM Anywhere main menu, go to **Settings > Scheduler** and search for the collection job for the BlueApp.
2. Enable the job if it is not already enabled. To customize the log collection rate, click the edit icon and set the desired interval for log collection.

The Azure Event Hubs Method

If you want to use Azure Event Hubs instead, you must first stream the logs from Microsoft Defender ATP to Azure Event Hubs, and then enable the Event Hubs log collection on your Azure Sensor.

To stream logs from Azure Event Hubs

1. Log in to the Azure portal.
2. Create an event hub. See Microsoft Azure Quickstart: Create an event hub using Azure portal for instructions.
3. Go to the event hub you just created and click **Shared access policies** in the sidebar.
4. Create or edit a policy, and then select **Manage**, **Send**, and **Listen**. Streaming to Event Hubs requires these permissions.
5. Copy the connection string listed in the policy under *Connection string-primary key*.

You need to enter this string when configuring the Event Hubs connection in USM Anywhere.

6. Configure streaming for Microsoft Defender ATP logs. See Configure Microsoft Defender ATP to stream Advanced Hunting events to your Azure Event Hubs for instructions from Microsoft.

> **Note:** Make sure to enable *Stream to an event hub* and select the Event Hub you just created as the destination.

To configure Event Hubs in USM Anywhere

1. Go to **Data Sources > Sensors** and open the Azure Sensor.
2. Click the **Configurations** tab.
3. Complete the three fields:
   - **Event Hub Name**: The name of the event hub created during initial setup.
   - **Event Hub Connection String**: A string containing unique configuration data about your Azure Event Hubs implementation. This string was discovered during the previous procedure.
   - **Event Hub Consumer Group**: The name of your Event Hubs consumer group. You can locate this name by opening your Event Hubs overview in the Azure portal and scrolling to the bottom of the page.
4. (Optional.) Select **Process generic events?** to collect events for which USM Anywhere currently does not have a parser. These events will display as "GENERIC event" under Activity > Events.
5. Click **Save**.
6. Click the **Event Hub** tab to check the connection status and the number of events processed by each data source.

BlueApp for Microsoft Defender ATP Actions

The BlueApp for Microsoft Defender Advanced Threat Protection (ATP) provides a set of orchestration actions that you can use to respond to threats forwarded from your Microsoft Azure Events Hub.

As USM Anywhere surfaces events, vulnerabilities, and alarms, your team determines which items require a response action. Rather than manually tagging threats, you can use the BlueApp for Microsoft Defender ATP orchestration actions to enforce protection based on the information associated with the event or alarm. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Microsoft Defender ATP

Action	Description
Collect Alert from Microsoft Defender ATP	Run this action to collect Microsoft Defender ATP alerts
Initiate Remote Scan	Run this action to initiate a Remote Scan for Microsoft Defender ATP
Start Remote Scan	Run this action to start a full scan on the host
Start Remote Scan	Run this action to start a remote scan from an orchestration rule
Set Indicator of Compromise	Run this action to create a policy for an Indicator of Compromise (IOC) in response to File, URL, or IP address. You can target your response to the IOC and create a rule to Allow, Block, or Report instances of the IOC. An IOC event or alarm generated by BlueApp for Microsoft Defender ATP will also contain a link to get statistics on the details of the IOC.
Isolate Machine	Run this action to cut off network traffic (except for the agent) based on the details of the event or rule conditions
Isolate a Machine using Rule	Run this action to isolate a machine using a rule
Release a Machine	Run this action to unisolates the machine based on the details of the event, alarm, or rule conditions

Actions for the BlueApp for Microsoft Defender ATP (Continued)

Action	Description
Release a Machine	Run this action to release a machine from an event or alarm
Quarantine a File	Run this action to quarantine the file that appears and delete it from the machine The file name, file path, and the SHA1 of the file are displayed when this action is selected
Quarantine a File	Run this action to quarantine a file from an event, alarm, or rule

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

To launch a Microsoft Defender ATP orchestration action for an alarm

1. Go to **Activity > Alarms** or **Acitvity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **Microsoft Defender ATP** tile.
5. For the App Action, select the action you want to launch.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

   You can launch an action to tag the alarm destination host or source host.

6. Enter the Microsoft Defender ATP name that you want applied.
7. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Microsoft Defender ATP Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

Use the BlueApp for Microsoft Defender Advanced Threat Protection (ATP) to access the Microsoft Defender ATP response actions, which enable you to quickly respond to threats identified by USM Anywhere. You can create response action rules in USM Anywhere that automatically trigger when alarms or events match the criteria that you specify.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

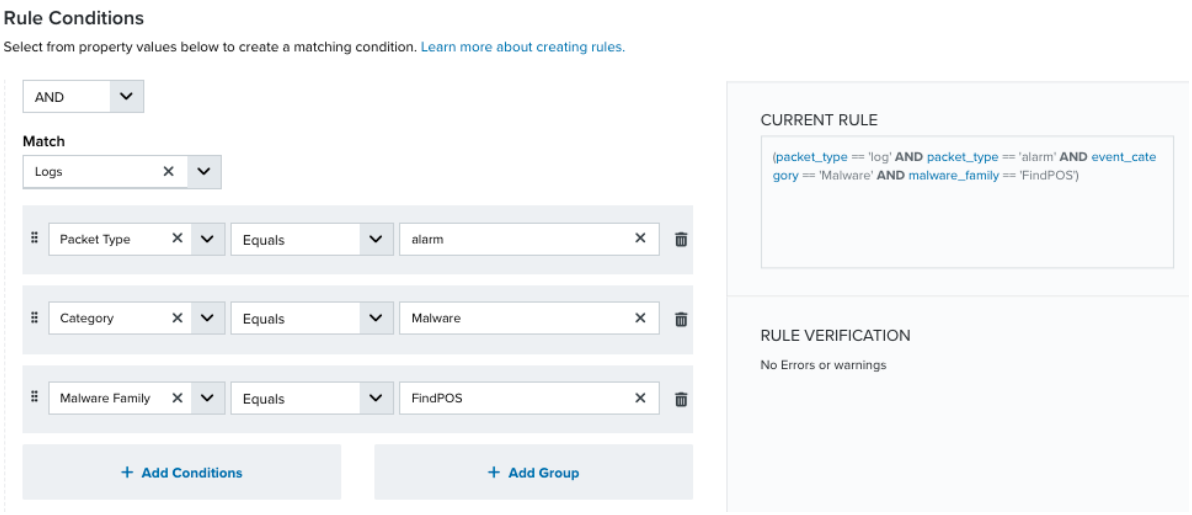
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation pane. Then click **Create Response Action Rule** to define the new rule.

To define a new Microsoft Defender ATP response action rule

1. Enter a name for the rule.
2. Select the action you want to launch from the **Action** drop-down menu.

   You can launch an action to tag the destination host or source for an alarm or an event.

3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. Click **OK** in the confirmation dialog box.

BlueApp for Mimecast Events Collection

The BlueApp for Mimecast Events Collection enables you to collect and normalize your logs from Mimecast. The BlueApp for Mimecast Events Collection collects logs from the Mimecast cloud, normalizes the events into the USM platform, and includes alarm rules to alert you to any Mimecast issues.

Edition: The BlueApp for Mimecast Events Collection is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Mimecast Events Collection

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To configure the BlueApp for Mimecast Events Collection in USM Anywhere, you need to have a Mimecast account with the appropriate authorization, as well as an API access token and secret key.

Set up the Mimecast API

Follow the instructions listed in the Mimecast user documentation. Here are the instructions on how to generate the API access token and secret key for USM Appliance.

To set up Mimecast to enable the BlueApp for Mimecast Events Collection

1. Create a new user within the Mimecast Administration Console whose authentication token will never expire.
   i. Assign your new user to the Basic Administrator role under **Administration > Account > Roles**.
   ii. Create a new group under **Administration > Directories > Profile Groups** and add your user to it.
   iii. Create a new authentication profile under **Administration > Services > Applications**, ensuring that you set the Authentication TTL to **Never Expires**.

Note: If you do not select Never Expires, you will have to generate a new API token and secret key and reconfigure your AlienApp every time this expires, or your AlienApp will not be able to collect data.

iv. Still in **Administration > Services > Applications**, create a new application setting and add the group you created in step 3 and the authentication profile you created in step 4.

2. Generate an API token and secret key under Services > API Applications > Create Keys.

Important: Be sure to save the API token and secret key, which you will need to configure the BlueApp for Mimecast Events Collection.

Configure BlueApp for Mimecast Events Collection in USM Anywhere

To enable the BlueApp for Mimecast Events Collection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the required information to configure the API.
   - **Email Address:** the email address of your credentialed Mimecast user
   - **Access Key:** the API token you generated previously
   - **Secret Key:** the secret key you generated previously
   - **App ID:** the ID assigned to your Mimecast application when you registered your app
   - **App Key:** the app key assigned to your Mimecast application when you registered your app
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for MobileIron Threat Defense

The advanced BlueApp for MobileIron Threat Defense provides mobile detection and response capabilities together with USM Anywhere and extends your visibility into malicious activity on the mobile devices. With BlueApp for MobileIron Threat Defense, USM Anywhere can discover mobile assets with MobileIron Go installed on them and ingest logs from them.

The BlueApp for MobileIron Threat Defense orchestration actions allow you to invoke remote actions on connected mobile devices. You can lock the device, reset the device or the password on it, send push notifications, and more. The BlueApp for MobileIron Threat Defense is also capable of pulling user records to enrich USM Anywhere user behavior analytics (UBA) data.

Edition: The BlueApp for MobileIron Threat Defense is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for MobileIron Threat Defense

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

Mobile Iron Configuration

To configure the BlueApp for MobileIron Threat Defense in USM Anywhere, you need the following:

- Your MobileIron zConsole API key
- Your MobileIron zConsole host URL
- Your MobleIron Cloud host URL
- A MobileIron Cloud user account with full role permissions.

Note: The BlueApp for MobileIron Threat Defense only processes events generated from devices that have the MobileIron Go app installed. Events generated from the Zimperium zIPS app will cause duplicated events in USM Anywhere, but because these events do not contain a Mobile Iron Threat Defense identifier, the BlueApp for MobileIron Threat Defense cannot process these events.

Obtain a MobileIron zConsole API Key

To obtain an API key for MobileIron Threat Defense, you need to log into the MobileIron Technical Support page and create an API key request. It will be mailed to you.

Create a New User in MobileIron Cloud

You need a user with full role permissions to connect the BlueApp for MobileIron Threat Defense to your USM Anywhere instance.

To set up your MobileIron Cloud user account with full role permissions

1. Log in to MobileIron Cloud.
2. Click the **Users** tab to open the Users page.
3. Click **Add** and select **Single User** from the dropdown menu.
4. Enter a name and email address for the new account and click **Done**.
5. On the Users page, click the checkbox next to the new user you created.
6. Click **Actions** and select **Assign Roles** from the dropdown menu to grant permissions to the new role.
7. In the Assign section of the window, select the **All** checkbox to allow the user full role permissions.

To enable the BlueApp for MobileIron Threat Defense

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Management URL, Username, and API Token.
7. Check **Allow Creation of New Assets** to allow Mobile Iron scans to create new assets in USM Anywhere.

   Check **Allow Merging of Existing Assets** to allow USM Anywhere to run a match against the Mobile Iron identification to merge the assets found with existing USM Anywhere assets.

   See BlueApp for MobileIron Threat Defense Asset Discovery and Management for more details on the asset creation and merging processes.
8. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for MobileIron Threat Defense Actions

The BlueApp for MobileIron Threat Defense provides a set of orchestration actions that you can use to identify and manage assets in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for MobileIron Threat Defense

Action	Description
Wipe Device	Run this action to remotely wipe the contents of a user's device. You can enter a message that will be displayed on the device before it is wiped. Once the device is wiped, it returns to factory default settings.
Change Password	Run this action to remotely issue a new password for a user's device. The password must have at least 12 characters, including at least 1 special character, 1 uppercase character, 1 lowercase character, and 1 number
Send Message	Run this action to send a message directly to a user You can choose to send a message either though the email registered to the phone, by push notification, or both
Delete User	Run this action to delete a user
Retrieve Events	Run this action to retrieve events from zConsole
Retrieve Matched Assets	Run this action to retrieve matched assets from MobileIron Cloud
Scan MobileIron Users	Run this action to scan the users from MobileIron
Send Message	Run this action to send a message to the selected device from a user
Send Message	Run this action to send a message to the selected device from an alarm
Send Message	Run this action to send a message to the selected device from EV
Change Password from Alarm	Run this action to change the password for a user from an alarm
Change Password from Event	Run this action to change the password for a user from an event
Change Password	Run this action to change the password for a user
Wipe Device from Alarm	Run this action to wipe a device from an alarm

Actions for the BlueApp for MobileIron Threat Defense (Continued)

Action	Description
Configure to Device/Device Group from Alarm	Run this action to configure the device or device group from an alarm
Configure Device/Device Group from Event	Run this action to configure the device or device group from an event
Configure Device/Device Group from User	Run this action to configure the device or device group from the user
Create or assign a Device to a Device Group	Run this action to create or add an existing device to the MobileIron Device Group Click **Associated User Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device
Create or Assign a User to a User Group	Run this action to create or add an existing user to a User Group Click **Associated User Groups** to see details on the device's current group associations
Assign a Policy to a Device Group	Run this action to assign a policy to the selected device group Click **Device Details**, **Associated Device Groups**, **Associated Configurations**, or **Associated Policies** to see more details related to the device Click **Available Configurations** or **Available Policies** to see a list of all configurations and policies available Click **Associated Policies** in the action window, and select a dynamically generated list of policies from the All Policies drop-down list
Assign a Configuration to a Device or Device Group	Run this action to assign a user configuration to the selected device group Click **Associated Configurations** to see a list of the current configurations for the device
Lock Device	Run this action to remotely lock a user's device Click **Device Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device

Actions for the BlueApp for MobileIron Threat Defense (Continued)

Action	Description
Unlock Device	Remotely unlock a user's device Click **Device Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device
Restart Device	Run this action to remotely restart a user's device. Click **Device Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device Click **Device Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device
Retire Device	Run this action to remotely retire a user's device Click **Device Details**, **Device Application List**, or **Device Compliance Status** to see more details on the device When you retire a device, all management features are removed. This also deletes documents, configurations, and profiles If the device is registered as a corporate-owned device, it reverts to factory default settings

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **MobileIron** tile.
5. For the App Action, select the action you want to launch.
6. Enter the name of the category you want the IP address added to, if applicable.
7. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating MobileIron Threat Defense Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ **Analyst** ✓ **Manager**

You can create orchestration rules in USM Anywhere that automatically trigger a MobileIron Threat Defense response action when events or alarms match the criteria that you specify.

After you create a rule, new events or alarms that match the rule will trigger the MobileIron Thread Defense response action to create a new incident. The rule does *not* trigger for existing events or alarms.

You can create a new rule as follows:

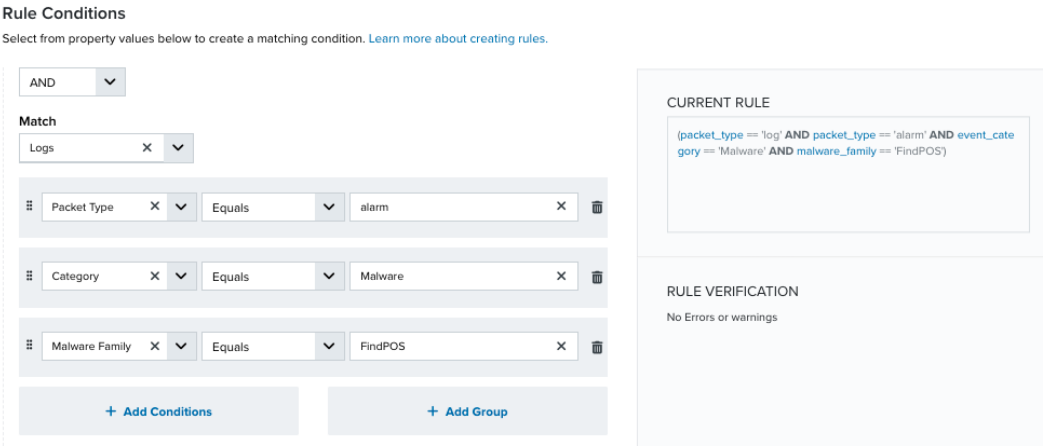
- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new MobileIron Threat Defense response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the MobileIron Threat Defense incident.

   The MobileIron Threat Defense parameters that you set will depend on the action that you select.
3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is

required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for MobileIron Threat Defense Asset Discovery and Management

The BlueApp for MobileIron Threat Defense features powerful device management capabilities than can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow MobileIron Threat Defense to create assets that are linked to devices in USM Anywhere.

Asset Creation from BlueApp for MobileIron Threat Defense

When MobileIron Threat Defense runs a scan, it identifies all assets in the scan and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in the app's configuration menu. Assets created from a MobileIron Threat Defense scan will include the information ported from MobileIron Threat Defense in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in MobileIron Threat Defense scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the MobileIron Threat Defense configuration menu, USM Anywhere will merge the information from the MobileIron Threat Defense scan with the existing asset. Assets are matched by comparing the media access control (MAC) address, IP address, and hostname from the MobileIron Threat Defense scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the MobileIron Threat Defense configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for MobileIron Threat Defense page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the MobileIron Threat Defense scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the MobileIron Threat Defense scan.
- **Merge:** Merge the information from the MobileIron Threat Defense scan with the matching asset details in USM Anywhere
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a MobileIron Threat Defense profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window displays showing the existing asset and the new asset that will be created once the two are split.
4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for MobileIron Threat Defense User Behavior Analytics (UBA)

The BlueApp for MobileIron Threat Defense can pull user records to enrich USM Anywhere user behavior analytics (UBA). When MobileIron users are detected by the BlueApp for MobileIron Threat Defense, their data will be used to enrich related events and alarms. In addition, you can configure orchestration rules and take actions based on these users and their activity.

To view information about these users in USM Anywhere

1. In USM Anywhere, go to **Environment > Users**.
2. Click the carrot next to any username and select **Full User Details** to view that user's information.
   The Full User Details page opens, displaying all of the accounts, alarms, and events related to this user.
3. Under the Accounts tab, click the button to view the device details for all devices associated with a particular user account.
4. Click the **Actions** button, and then **Advanced AlienApp Actions** to run available orchestration actions directly from this user's page.

See User Behavior Analytics (UBA) to read more about USM Anywhere UBA functionality.

BlueApp for Office 365

With the BlueApp for Office 365, you can monitor all of your Microsoft Office 365 cloud applications, track user activity, and receive alerts in USM Anywhere for suspicious and malicious activity in your environment. This integration gives you the ability to collect additional information about your environment and what your users are doing, which drives investigation and incident response processes.

The BlueApp for Office 365 supports the following features:

- Out-of-the-box correlation rules for Office 365 events, enabling USM Anywhere to automatically create alarms to notify you about suspicious activity in your environment.
- Predefined dashboards that give an overview of Microsoft OneDrive, Microsoft SharePoint, and Microsoft Azure Active Directory (AD) activity and provide quick visibility into Office 365 events to streamline your investigation and incident response processes.
- Direct access to the Microsoft Office 365 Management Activity API, giving you comprehensive visibility, a richer data set, and greater control over your cloud security, with information about your user, administration, system, and policy actions and events from Office 365 and Azure AD activity logs.

Note: If you're a Microsoft Windows user and want to include Office 365 logs in your USM Anywhere environment but don't yet use Azure, you'll need to sign up for an Azure subscription. The subscription is required to connect to the APIs that access your Office 365 environment.

It is *not* required that you deploy the USM Anywhere Azure Sensor to use the BlueApp for Office 365. You can use any deployed sensor for the BlueApp connection.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

BlueApp for Office 365 Requirements

Before you can configure and use the BlueApp for Office 365, you must make sure that your network and your Microsoft Office 365 environment are set up to support the API calls through Microsoft Azure Active Directory (AD) and audit log search.

Firewall Permissions

This integration requires connectivity between your USM Anywhere Sensor and the Microsoft APIs. If you have an Azure Sensor deployed in your Azure subscription, you should use this sensor to configure the BlueApp because you don't need to configure additional permissions.

If you use a *non-Azure Sensor*, you must set your firewall permissions based on the following table to allow inbound and outbound connections for the sensor.

Firewall Permissions for the USM Anywhere Sensor

Type	Port	Endpoint	Purpose
TCP	443	https://login.windows.net	Authentication for your Office 365 account
TCP	443	https://graph.microsoft.com	Queries to retrieve log data from the Microsoft Graph APIs
TCP	443	https://manage.office.com	Queries to retrieve log data from the Office 365 Management APIs

Note: To access Office 365 US Government, allow connections to `graph.microsoft.us` instead of graph.microsoft.com and `manage.office365.us` instead of manage.office.com.

Office 365 Account Privileges

To access Office 365 Management APIs (such as mail, contacts, calendar, and files), you must have an Office 365 Business account with global administrator privileges. See the Microsoft Support article to determine which Office 365 Business products you have.

Note: If you have multiple Office 365 accounts, you must deploy a USM Anywhere Sensor in *each* Office 365 account from which you want to collect events.

Azure AD Registration

BlueApp for Office 365 configuration includes creating an application in Azure AD. This application securely authenticates the BlueApp for Office 365 so that it can access and collect data according to the services and permission levels you define. This function requires that your Office 365 account is associated with an Azure subscription.

Important: If you do not already have an Azure subscription, you must create one. The subscription is required to register an app in Azure AD for your Office 365 account.

Before registering the application, you must first save a certificate from the BlueApp for Office 365.

To obtain the certificate

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Enter **Office 365** in the Search field, and then click the tile.
4. Click the **Instructions** tab.

   The page contains a manifest for the BlueApp and an abbreviated version of the following procedure.

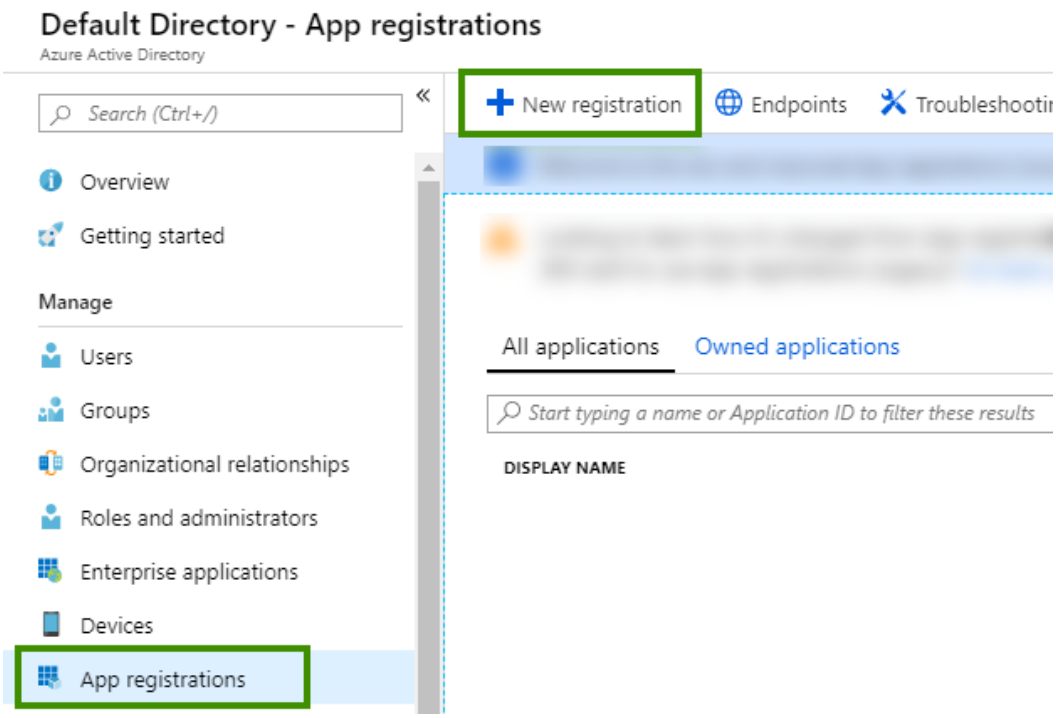
5. Save the content of the *value* field within the manifest in a file named `cert.pem`.

To register USM Anywhere in Azure

1. Save the content of your **value** field in a file named `cert.pem`. Do not include quotation marks:


```
{
  "customKeyIdentifier": "4txq5dVWNEUi0h6H3Co0B5j52qU=",
  "keyId": "ebbaf7db-b6f1-4b9c-8bc1-8bef075ab9dc",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": MIIEzTCCArUCBNEuR+AwDQYJKoZIhvcNAQENBQAwKjEoMCYGA1UEAwwfb2ZmaWNlMzY1LmFwcHMuYWxpZW52YXVsdC5jbG91ZDAgFw0yMjEwMTEyMDU3NTVaGA8yMTIyMTAxMTIwNTc1NVowKjEoMCYGA1UEAwwfb2Z
maWNlMzY1LmFwcHMuYWxpZW52YXVsdC5jbG91ZDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAPw8aWzQzX/SQM49O8zbLA7lwFJZzo0rSuqJEWixI62eYX+zziZuqnjmMfExagRlOVT90fsnTkA+Wu84rX0F4/vIFhYvZH
wpv9GuLnkW3SgXIpA5lK6xMuJYvn2ta01Lnx+4bRpiZgfJbg2pF9OgU1BruOH7q3bzTIfETAytn42YiIUkChS/8/U804Idrw+2Ni/TdDepaL3YNABgKOGqIH1JD86Po1SLYsIMt2fdKwvfgZDHC+a/urGU3AHFq5cpOjQq22nQSHl1
T/w3XudO64GmgtifRgHK4SRMsG/rlzpHrlDy4woL+rGKkaSBOPXCNGAC1XJwV9cAIkctNJO74rFgbfr+9+GBLr1oS5rG3RBPv9/Lgn0WZEJu31DTVt1A4xQCeOjn6Cywf23k56Bdrl/8MEFSTKGkk1TJKmrRtcHJgMhgX2qS1FzzOpz
xy+p/Gjo7yBO1DK3hQEjAEe2rxKN2UcHjPQbFXySARMFQxWlfbmGOigHVgYu0uhXCItaSqQWPfzFv1+0yTe1J/zHnz1PMd8o9xt+C06sWkavRUkLgmsxFR52k4J+QHBaFaBnTMoeA2HbrJiZtxALuHRAmq0sOZ0dFo5/HSkq7d9wyex
IU1sNG5IX5ZSmp6HijrqzPfFxL3vSrIX0K1EYHl2S8lLliHTn6LUrMfZdJqVtoV7LBAgMBAAEwDQYJKoZIhvcNAQENBQADggIBAFHkc3f6vJoA31aWZW4ojOLzlFSp4Z427DGXToloPOVU4Cn1JehGtJSn2eznACCshDw66yxygdAsr
AFJfiLjstxMfmpibsCuSVx219IhZjFZWhmKo+4vym4TnM9vX8+/Hsv3NQ8tzjPVZwA/28LI1jpWGffKHSJwlyNIFzYjjQiFTFGpIUbSCA6M/ASKYGLhGmjWgnC3lkcoJxA751vaCU9SM9FzXb7l9hAyIW2X6SUjO+330oRv0UYkRbfA
ORW/PQV046tX63zy0HJTxTj4X/E7p1Mx8Pt8D1HzZnFw2NCZiXy0I2bqGGVv5oEP2vfS6auCrxPqBmnG5fZD3ofWm3UwW84/lQa8/YQJA1Vn19/NW947lgJ49GGejnmcD9wlvyDxkMhyMNNvnW5RDYwoT6AOTHyn1I7PkvJNItA0+yZL
OA3GoL5SOQ2qISKtbmee4QbCuuzrSlVgFq61vw4x+K6omOkEv50Wi1+DEM3V/JbGmItk5qpsn73lkFaOBGBUlSCzUQt2HOJLTVvrM5QsFR/3yYkWjqikN8li86yNIYpMMRg/gwNtMLMtuFAlc53fBg3SXdngBmio7E3pptcXwZbc5Ds
it0AytxTBJvLl/zYl6C7ueEH77tMubnFWSn6ZzSDtW6elNlw65PHUDLBcWc9gga9xV4c0DORTBoAKz9sC6
}
```


2. Log in to the Azure portal and click **Azure Active Directory**.
3. Go to **App Registrations**, and then click **New Registration**.



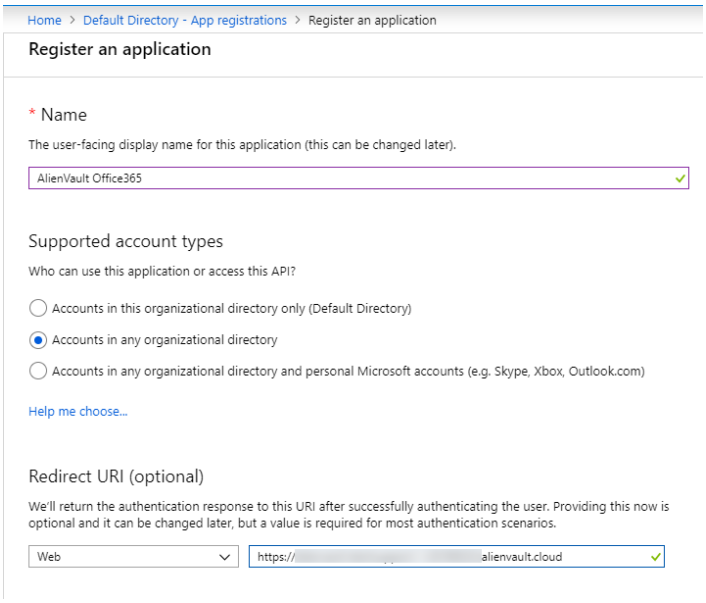
4. Register the application:

   a. Enter a name for the application.

   b. In Supported Account Types, select who can use this application.

      Your selection decides if this application is single-tenant or multi-tenant in the Microsoft identity platform. See Microsoft Documentation for the description of each type.

   c. In Redirect URI, enter your USM Anywhere login URL (for example, *https://acmecompany.alienvault.cloud*).



d. Click **Register**.

   The application is created and the overview page displays.

5. Add permissions for accessing Office 365 Management APIs:

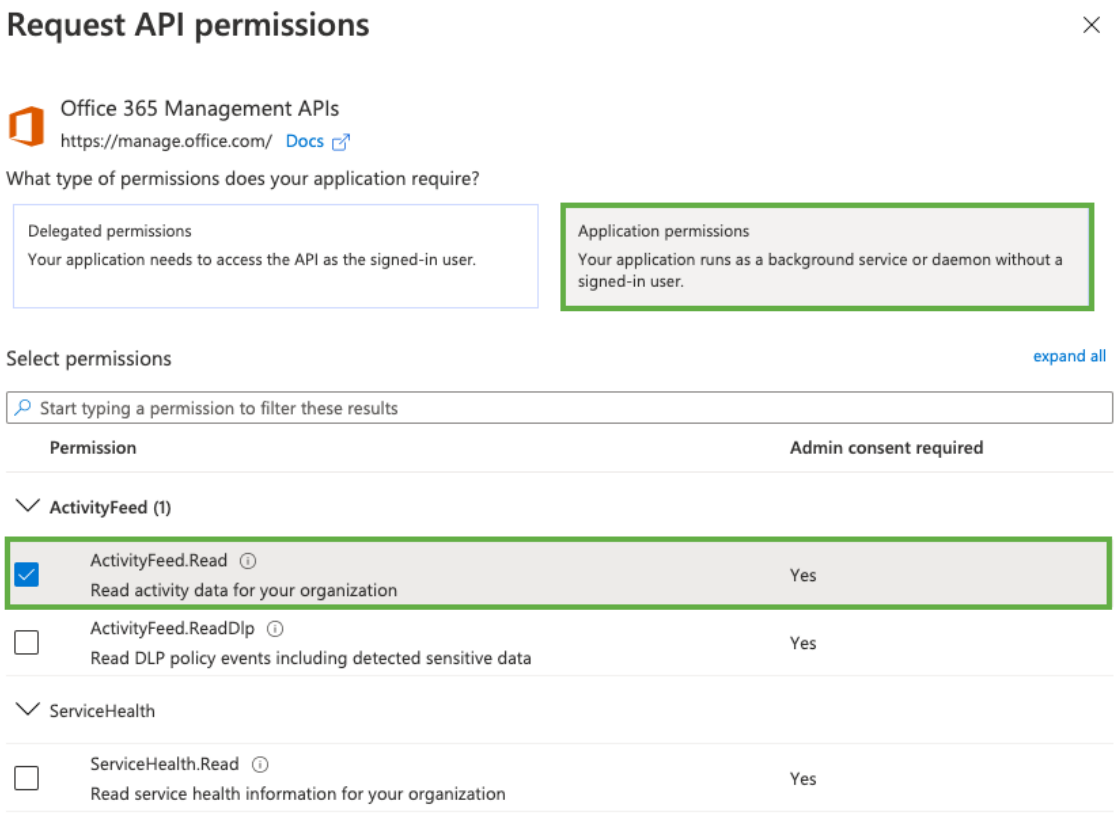
   a. Go to **API Permissions**, and then click **Add a Permission**.

   b. Under Request API Permissions, click **Office 365 Management APIs**.

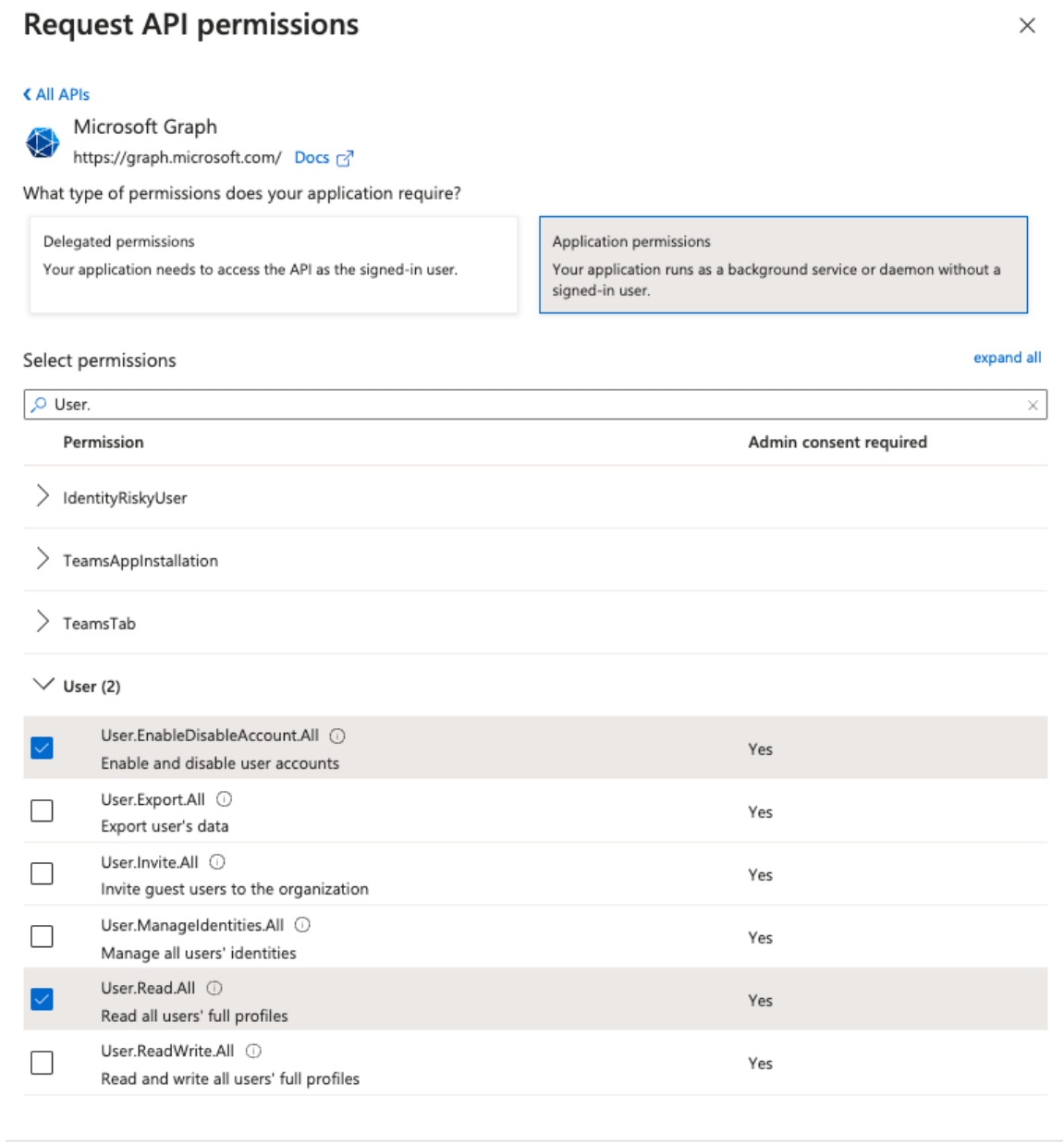
   c. Click **Application Permissions**.

   d. Expand the groups to select **ActivityFeed.Read** permissions, and then click **Add Per-**

missions.

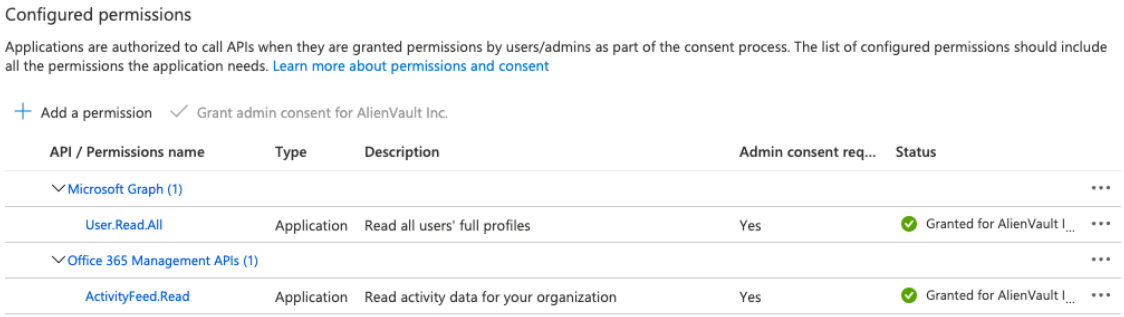


6. Add permissions for pulling Azure AD users:
   a. Go to **API Permissions**, and then click **Add a Permission**.
   b. Under Request API Permissions, click **Microsoft Graph**.
   c. Click **Application Permissions**.
   d. Expand User to select **User.Read.All** and **Users.EnableDisableAccount.All** permissions, and then click **Add Permissions**.



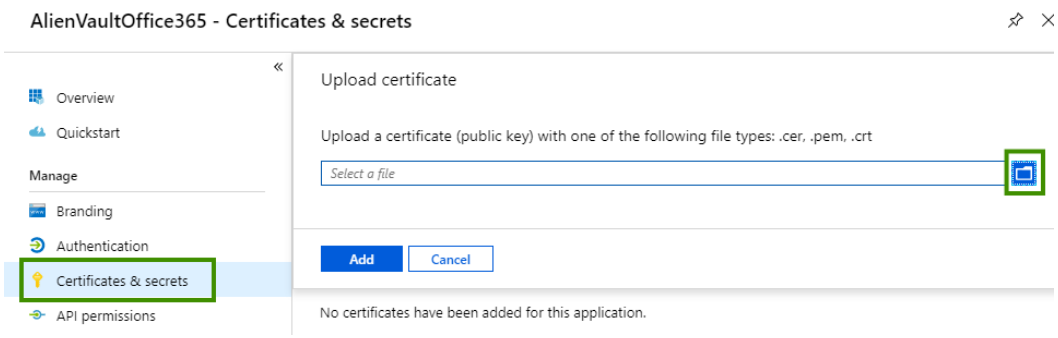
e. Click **Grant Admin Consent for Default Directory**, and then click **Yes** when prompted.

Important: You must grant permissions for the application to work. You must have the global administrator privileges to successfully grant permissions.



7. Update the credentials of the application:

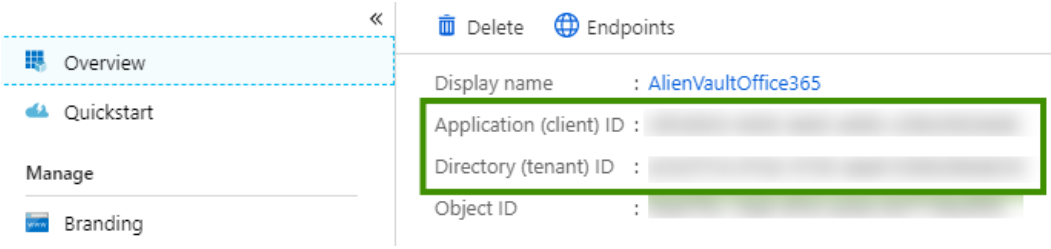
   a. Go to **Certificates & Secrets**.



   b. Select the `cert.pem` file created in the previous procedure, and then click **Add**.

      The credentials of the application are updated.

8. Return to the overview page of the application and copy the **Application (Client) ID** and **Directory (Tenant) ID** to your clipboard.



Return to USM Anywhere to finish setting up the BlueApp for Office 365. See Configuring the BlueApp for Office 365 for more information.

Audit Log Search

Office 365 audit logging records almost every significant action, including Office 365 logins, viewing documents, downloading documents, sharing documents, setting changes, and password resets. Office 365 includes the Security & Compliance Center to support search capabilities for these logs. You can use the search capabilities to compare events generated by the BlueApp for Office 365 with the information logged in the Office 365 environment.

This feature is required for logs to be collected and is enabled by default as of January 2019. See the Microsoft Support article for more detailed information.

Mailbox Auditing

To collect additional mailbox access activity in your Office 365 environment, you must enable mailbox audit logging. Microsoft mailbox auditing records actions performed by mailbox owners, delegates, and administrators. Mailbox auditing in Office 365 is not mandatory for log collection using the BlueApp for Office 365, but it is turned on by default starting as of January 2019. See the Microsoft Support article for detailed information.

Note: Enabling mailbox auditing requires that you can connect to the Microsoft Exchange Online PowerShell. See Using PowerShell with Exchange Online on the Microsoft site for more information.

It is a best practice to enable global audit logging, including non-owner mailbox access on every mailbox in your tenancy. You can use the following command to enable this auditing:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq
"UserMailbox" -or RecipientTypeDetails -eq "SharedMailbox" -or
RecipientTypeDetails -eq "RoomMailbox" -or RecipientTypeDetails -eq
"DiscoveryMailbox"}| Set-Mailbox -AuditEnabled $true -AuditLogAgeLimit 365 -
AuditOwner
Create,HardDelete,MailboxLogin,MoveToDeletedItems,SoftDelete,Update,UpdateInb
oxRules
```

Configuring the BlueApp for Office 365

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

The Microsoft Office 365 Management Activity API provides information about various user, admin, system, and policy actions and events from Office 365. After you configure the connection between the BlueApp for Office 365 and the Office 365 Management Activity API, the predefined log collection job performs a query for Office 365 events. When USM Anywhere collects and analyzes the first of these events, the Office 365 Azure Active Directory dashboard, Office 365 OneDrive dashboard, and Office 365 SharePoint dashboard become available in the Dashboards menu (according to the type of events that it collects).

Warning: Due to the design of the Office 365 Management Activity API, you may see events being delayed or received out of order. See Office 365 Event Latency for more information.

Before you configure the BlueApp for Office 365, make sure that you have fulfilled the firewall permissions and requirements in your Office 365 account for this integration.

To configure the BlueApp for Office 365

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Follow the instructions on the page to register the BlueApp for Office 365 in Azure, and then copy the Application (client) ID and Directory (tenant) ID.

   Note: This step is better conducted in a different browser.
7. Enter the copied IDs in the Tenant ID and Application ID fields.
8. Select the endpoint for Office 365 Management Activity API:

- Office 365: `https://manage.office.com`
- Office 365 US Government: `https://manage.office365.us`

9. Click **Save**.
10. Verify the connection.

    After USM Anywhere completes a successful connection to the Office 365 APIs, a icon displays in the Health column.

    If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Office 365 connection.

11. In the USM Anywhere main menu, go to **Settings > Scheduler** and search for the collection job for Office 365.
12. Enable the job if it is not already enabled.

    Important: The BlueApp will not work if the scheduler job is not enabled.

    When this job runs for the first time after the connection, it collects Office 365 events from the previous hour. On subsequent runs (every 20 minutes), it only collects new events since the last check. In the unlikely event that the AlienApp stops working after it is enabled, Microsoft Azure keeps Office 365 events for 7 days. The AlienApp will resume collecting events after it recovers.

Office 365 Event Latency

Because the BlueApp for Office 365 data queries must rely on information as provided by the Microsoft Office 365 Management Activity API, you may see non-sequential events as well as delayed timestamps for retrieved events and generated alarms. This is beyond the control of LevelBlue. You can observe the latency by comparing the Time Received ISO8601 and Time Created ISO8601 fields of an Office 365 event in USM Anywhere.

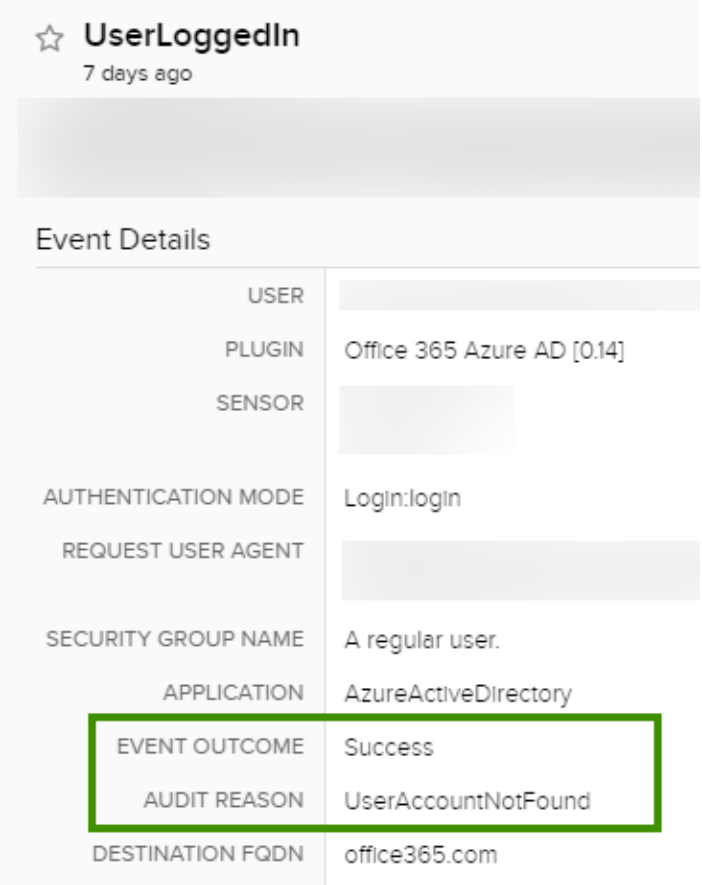
APP ID	office-365
WAS FUZZIED	false
CLOUD APP	office-365
TIME RECEIVED	Wed, Sep 05 2018, 11:20 AM AEST
WAS GUESSED	false
HAS ALARM	true
EVENT HASH	[redacted]
DATA SOURCE	Exchange
TIME RECEIVED ISO8601	2018-09-05T01:20:01.541Z
APP NAME	office-365
USED HINT	false
PACKET TYPE	log
SUPPRESSED	false
USER RESOURCE	[redacted]
REPORTING DEVICE VERSION	1
TRANSIENT	false
TIME CREATED ISO8601	2018-09-04T12:49:58.000Z
DATA SOURCE TYPE	Mail Server
NEEDS ENRICHMENT	true
IN ALARMS	[redacted]

The Office 365 Management Activity API aggregates actions and events into tenant-specific content binary large objects (BLOBs). It creates these BLOBs by collecting and aggregating actions and events across multiple servers and data centers. Because of this distributed process, the actions and events contained in the BLOBs do not necessarily appear in the order in which they occur. Also, the timestamp for logs stored in these BLOBs are based on the BLOB creation, not the events. See the Working with the Office 365 Management Activity API page for more information about log collection and aggregation by the Microsoft Activity API.

Additionally, the Management Activity API incorporates mechanisms designed to ensure that customers have access to logs through service interruptions. This can result in a time delay of up to 30 minutes, and sometimes 24 hours or more, after an event occurs for the corresponding audit log entry to be collected and provided by the API. See the Search the audit log in the compliance center page for a table listing the time delays of different services in Office 365. However, if you observe delays to be more than 5 days, it could indicate a potential issue. On the Office 365 Management Activity API FAQs and troubleshooting page, Microsoft advises to check the Service Health Dashboard or open a ticket with Microsoft support.

Office 365 UserLoggedIn Event Discrepancy

When using the BlueApp for Office 365, you may see successful login events when the user actually fails to log in. For example:



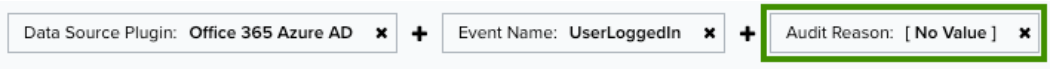
This is not a mistake in the BlueApp, but rather the data USM Anywhere receives from Microsoft Office 365, which appears to be by design. When examining the raw log for this event, notice that the ResultStatusDetail (mapped to Event Outcome) shows Success while the LogonError (mapped to Audit Reason) shows UserAccountNotFound:

```
{
  "CreationTime": "2020-01-03T04:20:32",
  "Operation": "UserLoggedIn",
  "ResultStatus": "Succeeded",
  "ExtendedProperties": {
     "FlowTokenScenario": "Login",
     "RequestType": "Login:login",
     "ResultStatusDetail": "Success"
  },
  "Target": [
    {
      "ID": "Unknown",
      "Type": 0
    }
  ],
  "TargetContextId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
```

```
  "LogonError": "UserAccountNotFound"
}
```

LevelBlue has seen similar issues reported in different communities, including the Microsoft community. Unfortunately, there is no clear answer on what has caused the discrepancy. Since Office 365 uses Microsoft Azure Active Directory (AD) to authenticate users, a possible explanation exists that the user accounts are not synchronized. See the Microsoft documentation to understand the relationship between Office 365 and Azure AD.

Because of this discrepancy, to construct a list of truly successful login events in USM Anywhere, you need to filter for UserLoggedIn events with an empty Audit Reason field. For example:



BlueApp for Office 365 Actions

The BlueApp for Office 365 provides a set of orchestration actions that you can use to integrate your BlueApp for Office 365 in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Office 365

Action	Description
Scan Audit. General Events	Run this action to scan Audit.General content from events
Disable User Account from Event/Alarm/Investigation	Run this action to disable a user account from an event, alarm, or investigation
Disable User Account from Rule	Run this action to disable a user account from a rule
Enable User Account	Run this action to enable a user account from a rule, event, alarm, or investigation

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.

3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms, Events, or Investigations

You can launch an action directly from alarms, events, or investigations. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm, event, or investigation.

To launch an BlueApp for Office 365 response action for an alarm, event, or investigation

1. Go to **Activity > Alarms**, **Activity > Events**, or **Investigations**.
2. Click the alarm, event, or investigation to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run BlueApp for Office 365 Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar investigations**, **Create rule for similar alarms**, or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Office 365 Response Action Rules

Role Availability | ✗ Read-Only | ✗ Investigator | ✓ Analyst | ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger an Office 365 response action when alarms, events, and investigations match the criteria that you specify. After you create a rule, new alarms, events, and investigations that match the rule conditions trigger the Office 365 response action to create a new incident. The rule does *not* trigger for existing alarms, events, or investigations.

You can create a new rule as follows:

- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

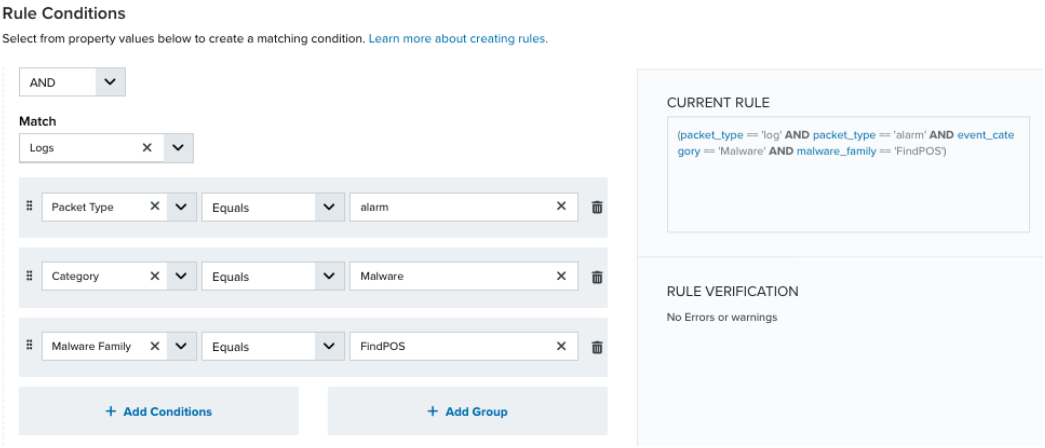
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the app:** Go to the BlueApp for Office 365 page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new BlueApp for Office 365 response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the BlueApp for Office 365 incident.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

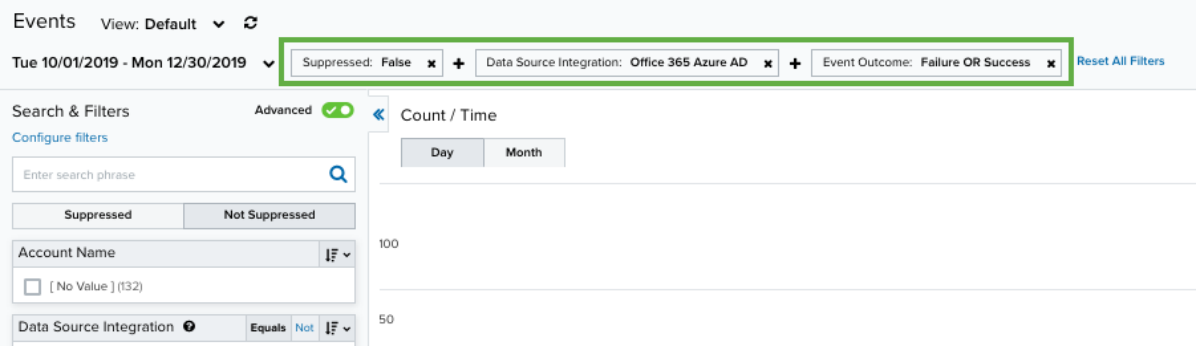
Tutorial: Create a Notification Rule for Office 365 Users Logged In from a Different Location than Assigned

As a cloud-based subscription service, Microsoft Office 365 enables users to create and share from anywhere on any device. This can be problematic for some organizations so Microsoft also provides Conditional Access policies to limit user access based on their locations. With a configured BlueApp for Office 365 and a notification rule, you can let USM Anywhere inform you when a user logs into Office 365 from a location other than the one to which they are assigned. This tutorial provides step-by-step instructions on how to create such a rule in USM Anywhere.

To create a notification rule for Office 365 user logged in events

1. If not done already, enable and configure the BlueApp for Office 365.
2. Go to the Office 365 Azure Active Directory Dashboard and under Login Activity, click the graph where the event count is not zero.

   This takes you to the Events page showing Office 365 Azure Active Directory (AD) login failure or success events. You can also directly go to the Events page and search for these events.

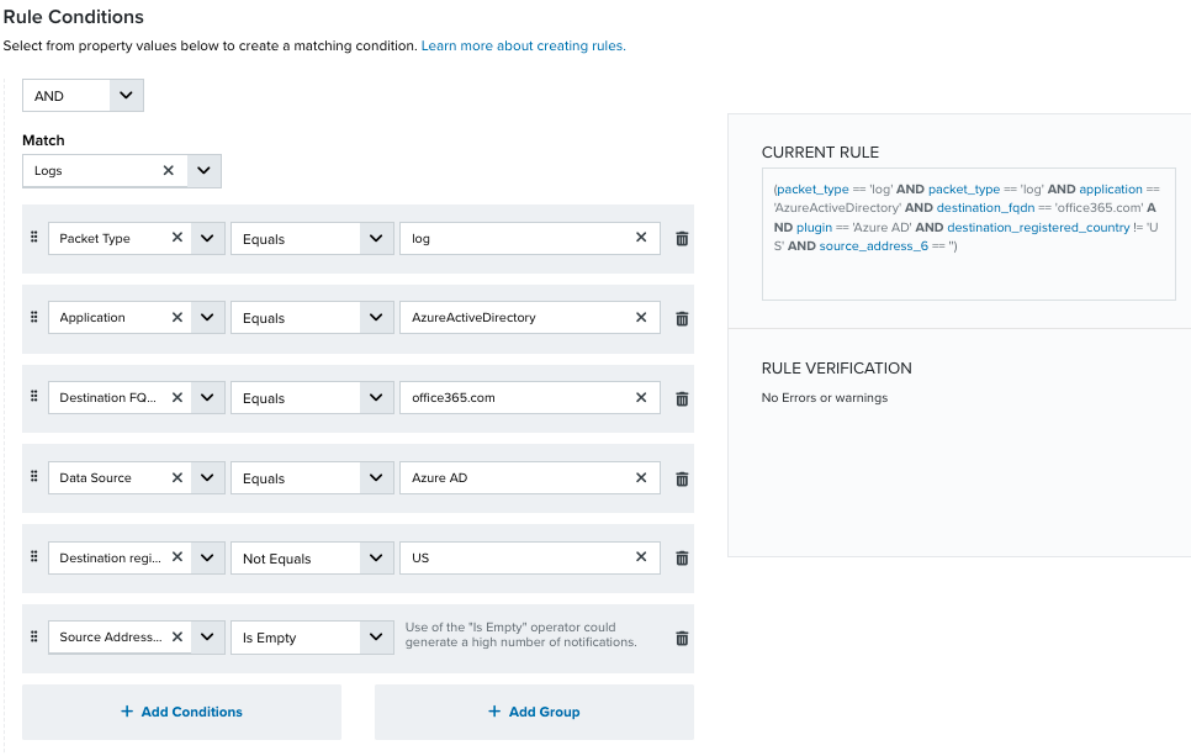


3. Click one of the events to open event details on the right.
4. Select **Create Rule > Create Notification Rule**.
5. Type a name for the rule and select a notification method of your preference.
6. USM Anywhere prepopulates the rule conditions based on the event. You can delete some conditions to make the rule more generic.
7. To match a user logging in from a location other than the one they are assigned to, you need to add the following conditions

```
Source Registered Country != <user assigned location>
Source Address 6 == ""
```

> **Note:** The "Source Address 6 is empty" condition prevents any device with an IPv6 address from triggering this rule. LevelBlue recommends adding this condition because IPv6 geolocation is relatively new and its current database is incomplete.

8. To match all login events, make sure that you include every condition shown in this screenshot.



Note: If you want the rule to only match successful login events or failed login events, you can add the Event Name condition and set it equal to UserLoggedIn or UserLoginFailed respectively.

9. Save the rule.

BlueApp for Okta

The BlueApp for Okta provides deep security monitoring for single sign-on (SSO) and multifactor authentication (MFA) activities, helping you safeguard user credentials through early threat detection and rapid response. It enhances the threat detection capabilities of USM Anywhere by collecting and analyzing log data from your Okta environment to help you detect user credential theft, abuse, policy violations, and other threats to your Okta account.

The BlueApp for Okta supports the following features:

- It regularly queries the Okta API for information, such as authentication events, user profile updates, user state changes, application and group assignment, and Okta platform changes.

- The out-of-the-box correlation rules for Okta events enable USM Anywhere to automatically create alarms, notifying you about suspicious activity in your Okta environment.
- It includes a predefined dashboard that provides an overview of Okta activity so that you have quick visibility to streamline your investigation and incident response processes.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Okta

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

After you configure the connection between the BlueApp for Okta and the Okta API, the predefined, scheduled job collects event logs from Okta every 20 minutes. After USM Anywhere collects and analyzes the first of these events, the Okta dashboard is available in the Dashboards menu.

Create an Okta API Token

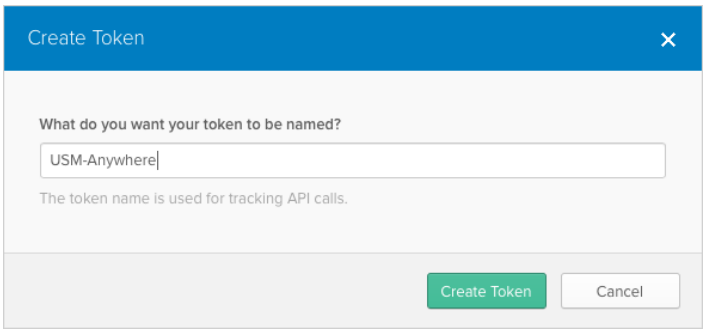
Before you can collect and analyze Okta log data within USM Anywhere, you must have an API token that USM Anywhere can use to connect to your Okta environment. Okta issues an API token for a specific user and all requests with that token act on behalf of that user.

Important: You must have Okta Super Administrator or Org Administrator privileges to generate a valid API token for integration with the BlueApp for Okta. See their Administrators article for more information about administrator privileges in Okta.

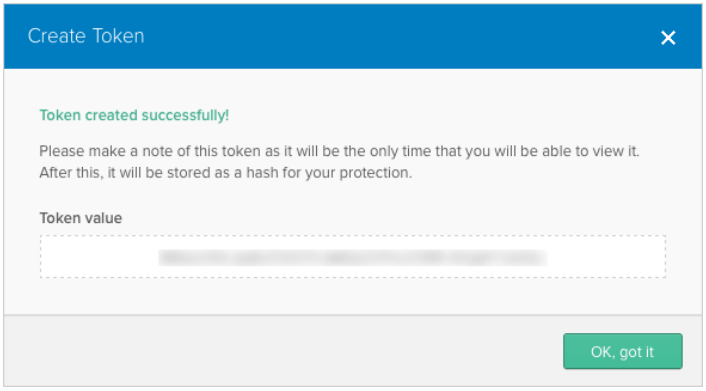
To acquire the API token for Okta

1. Open your Okta administration dashboard with your user login.
2. Select **Security > API**.
3. At the top of the page, click **Create Token**.
4. In the dialog box, enter a name for the token and click **Create Token**.

   The name should indicate the intended use for the token, such as *USM-Anywhere*.

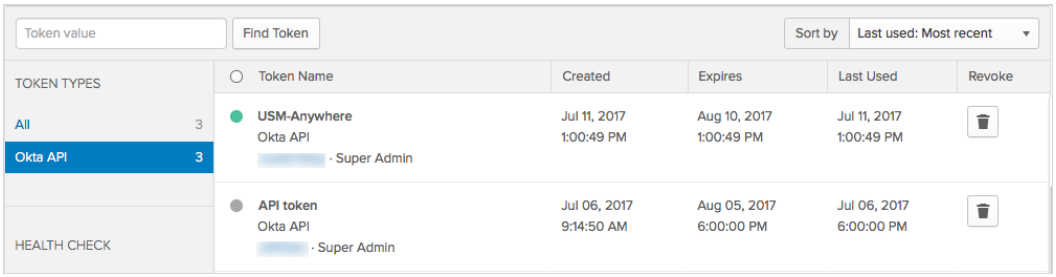


Okta generates the unique token and displays the value in the dialog box.



5. Copy the token to your clipboard or an encrypted text file and click **OK, got it**.

   The list in the page includes your new token.



Enable the BlueApp for Okta API Connection

After you generate an Okta API token and copy the value, you're ready to enable the BlueApp in USM Anywhere.

To enable the BlueApp for Okta

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the connection information to access the API for your Okta environment:

   - **Okta URL**: Enter the URL that you use to access your Okta environment.
   - **Okta API Token**: Click **Change Okta API Token** and enter the API token created with your user account.
7. Click **Save**.
8. Verify the connection.

After USM Anywhere completes a successful connection to the Okta APIs, a icon displays in the Health column.

If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Okta connection.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Oracle Database

The BlueApp for Oracle Database enables you to take log information from your Oracle Database Environment and feed it directly into your USM Anywhere environment.

Edition: The BlueApp for Oracle Database is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Oracle Database

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To use the BlueApp for Oracle Database in USM Anywhere, you need to enable the audit trail in Oracle Database and grant audit access to the Oracle Database user account that will be connected to USM Anywhere.

Set Up Oracle Audit Trail

To turn on the audit trail for Oracle Database, refer to the Oracle documentation Enabling or Disabling the Standard Audit Trail.

To grant audit access for the user account

1. Log into Oracle Database by entering the Oracle Service Identifier (SID) password with the following command:

   ```
   sqlplus system/<PASSWORD>@<SID>
   ```

2. Once you have logged in, enable audit access for the user with the following command:

   ```
   AUDIT ALL BY <USER> BY ACCESS
   ```

Connecting the BlueApp for Oracle Database in USM Anywhere

After obtaining the credentials, you must configure the connection within USM Anywhere.

To enable the BlueApp for Oracle Database

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter your Oracle information into the following fields:

- Database Host Name
- Port number
- Oracle Service Identifier (SID)
- Username
- Password

7. Click **Save**.
8. Verify the connection.

   After USM Anywhere completes a successful connection to the Oracle Database APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Oracle Database connection.

BlueApp for Palo Alto Networks PAN-OS

The BlueApp for Palo Alto Networks PAN-OS enables you to automate intrusion detection and response activities between USM Anywhere and Palo Alto Networks Next-Generation Firewall (NGFW) products. The BlueApp for Palo Alto Networks PAN-OS enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities from your Palo Alto Networks firewall, and provides orchestration actions to streamline incident response activities based on risks identified in USM Anywhere.

Edition: The BlueApp for Palo Alto Networks PAN-OS is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Palo Alto Networks PAN-OS

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

When the BlueApp for Palo Alto Networks PAN-OS is enabled and connected to your Palo Alto Networks environment, you can launch app actions and create orchestration rules to send data from USM Anywhere to your Palo Alto device. For more information about the orchestration actions supported by the BlueApp for Palo Alto Networks PAN-OS, see BlueApp for Palo Alto Networks PAN-OS Actions.

Note: To fully integrate USM Anywhere with your Palo Alto Networks device, you should also have the Palo Alto Networks PAN-OS log collection enabled so that USM Anywhere can retrieve and normalize the raw log data. See Collecting Logs from Palo Alto Networks for details.

Note: The BlueApp for Palo Alto Networks PAN-OS is designed for use with single firewalls, and does not integrate with the Palo Alto Panorama software for managing multiple firewalls.

BlueApp for Palo Alto Networks PAN-OS Requirements

Before you can begin configuration, you must have the following information from the PAN-OS and, if desired, from a Certificate Authority (CA):

- An API key
- The IP address or hostname of the Palo Alto Networks PAN-OS
- A dedicated admin account
- (Optional) A Secure Socket Layer (SSL) certificate, either self-signed or from a CA. See Uploading a CA Certificate for more information.

To acquire an API key for PAN-OS

1. Go to https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/get-your-api-key.html and follow the vendor instructions to generate the key.
2. Copy the token to be entered in USM Anywhere.

To create an admin account in Palo Alto Networks

1. Log in to your Palo Alto Networks account with an admin user profile.
2. Click the **Device** tab.
3. Select **Admin Roles** in the left pane and click **Add** to create a new administrator profile.

4. In the Admin Role Profile window, enter a name and description (optional) for the profile.
5. Click the **XML/REST API** tab and click each of the items under that tab to enable them all.
6. Click **OK** to create the profile.
7. Now select **Administrators** from the left panel and click **Add**.
8. In the Administrator window:
    a. Enter a name for the account, a password, and select **Role Based** for the Administrator Type.
    b. For Profile, enter the name of the profile you previously created in the Admin Roles section.
9. Click **OK** to create the admin account.

Configure the BlueApp for Palo Alto Networks PAN-OS Connection

To support the orchestration actions in USM Anywhere, you must configure a connection with the PAN-OS firewall. This connection enables the BlueApp to send a request to the PAN-OS API.

Important: USM Anywhere can only communicate with one PAN-OS instance per sensor. If you have multiple PAN-OS instances in your network, contact LevelBlue Technical Support for assistance.

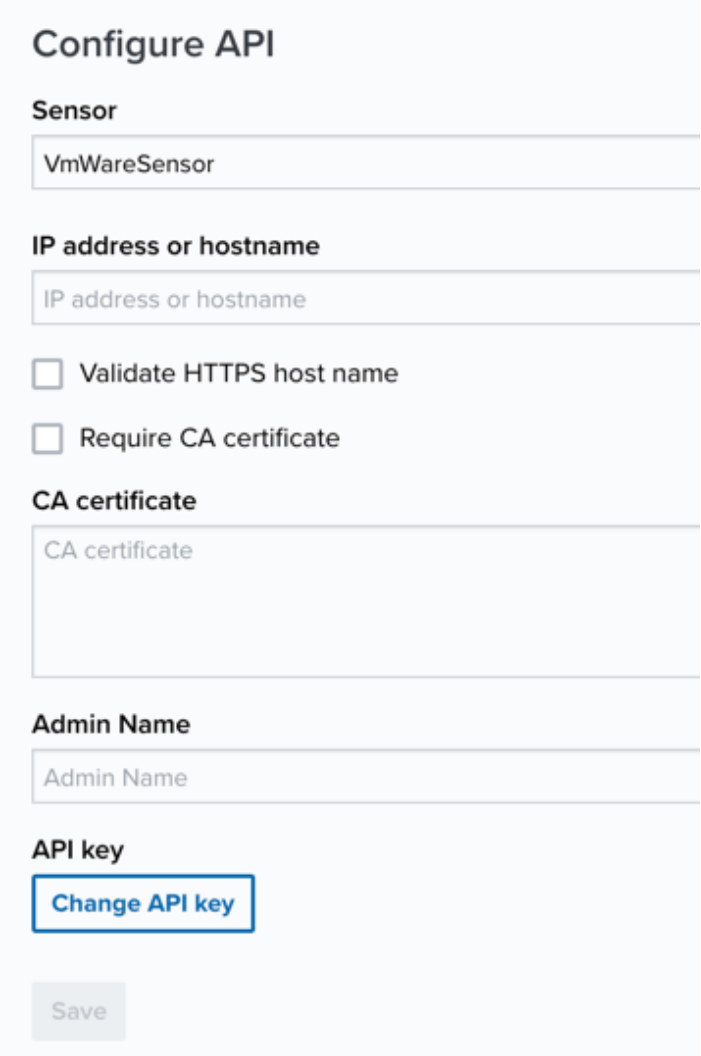
To configure the connection for PAN-OS

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

    BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Specify the connection information for Palo Alto Networks:

   - **IP address or hostname**: Enter the IP address or hostname of your PAN-OS instance.
   - (Optional) **Validate HTTPS host name**: Select this option if you want USM Anywhere to validate the hostname against its SSL certificate.
   - (Optional) **Require CA certificate**: Select this option if you prefer to use a security certificate to establish a trusted SSL connection between PAN-OS and USM Anywhere.
   - (Optional) **CA certificate**: Enter your certificate for the connection.
   - **Admin Name**: Enter the name of the admin account you created.
   - **API key**: Enter the API key that you generated in PAN-OS.



7. Click **Save**.

Uploading a CA Certificate

If you leave the Require CA Certificate checkbox deselected, the BlueApp uses the browser's default trust store. When you select the Require CA Certificate checkbox, the certificate entered in the CA Certificate field takes precedence and is the only certificate trusted by the client.

There are two major use cases that might require you to upload your own certificate in the CA Certificate field:

- The firewall was deployed with a self-signed Secure Sockets Layer (SSL) certificate. A certificate like this is typically generated on the firewall at the time of deployment. In this case, you need to export that self-signed certificate from the firewall and paste it into the CA Certificate field.
- You have deployed the firewall with a SSL certificate signed by your own CA. In this case, you need to import the root and intermediate certificates, if any, from your CA. This way, the BlueApp has the same trusted certificate chain that are deployed on your firewall.

See the Palo Alto Networks PAN-OS documentation for further information on exporting a certificate to use with the BlueApp.

BlueApp for Palo Alto Networks PAN-OS Actions

The BlueApp for Palo Alto Networks PAN-OS provides a set of orchestration actions that you can use to quickly send IP addresses to the firewall as a response to threats identified by USM Anywhere. You can also send IP addresses to Palo Alto Dynamic Address Groups. The BlueApp sends standard HTTP requests to the Palo Alto Networks PAN-OS APIs to register tags. Each such tag contains the source or destination address (*or* the fully qualified domain name [FQDN]) of the event or alarm that triggered the action or orchestration rule.

Important: Using the BlueApp for Palo Alto Networks PAN-OS orchestration actions requires that the BlueApp is enabled on a deployed USM Anywhere Sensor with configured integration to your Palo Alto Networks product. See Configuring the BlueApp for Palo Alto Networks PAN-OS for more information.

As USM Anywhere surfaces events and alarms, your team determines which items require a response action. Rather than manually tagging source and destination hosts in the Palo Alto Networks firewall for enforcement purposes, you can use the BlueApp for Palo Alto Networks PAN-OS orchestration actions to enforce protection based on the information associated with the event or alarm. The following table lists the available actions from the BlueApp.

Actions for BlueApp for Palo Alto Networks PAN-OS

Action	Description
Tag Source IP Address from Event	Run this action to tag a source IP address to a dynamic address group from an event
Tag Source IP Address from Rule	Run this action to tag source IP address and add it to a Dynamic Address Group in the connected Palo Alto Networks device from a rule
Tag Source IP Address from Alarm	Run this action to tag a source IP address to a dynamic address group from an alarm
Tag Source Address from Rule	Run this action to tag a source address from a rule
Tag Destination IP Address from Event	Run this action to tag a destination IP address to a dynamic address group from an event
Tag Destination IP Address from Rule	Run this action to tag destination IP Address and add it to a Dynamic Address Group in the connected Palo Alto Networks device from a rule
Tag Destination IP Address from Alarm	Run this action to tag a destination IP address to a dynamic group address from an alarm
Tag Destination Address from Rule	Run this action to tag a destination address from a rule
Remove Tag from Source Address	Run this action to remove a tag from the source address
Remove Tag from Address Group	Run this action to remove a tag from the address group
Remove Tag from Destination Address	Run this action to remove a tag from a destination address
Add Tag to Address Group	Run this action to add a tag to an address group

Actions for BlueApp for Palo Alto Networks PAN-OS (Continued)

Action	Description
Add Tag to Destination Address	Run this action to add a tag to a destination address
Add Tag to Source Address	Run this action to add a tag to a source address

Upon launch of the action, USM Anywhere sends a request to the Palo Alto Networks PAN-OS API to add one of the following identifiers to its Object database and to tag it according to the value specified in the action or rule.

- IPv4 address
- IPv6 address
- FQDN

Important: By default, changes affecting PAN-OS firewall configurations require activation through a *commit*. The object (host) tag requests sent by BlueApp for Palo Alto Networks PAN-OS are not activated until you or another Palo Alto administrator commits them. In the PAN-OS web UI, you can filter pending changes by user account or location and then preview, validate, or commit only those changes. For more information about committing these changes, refer to the PAN-OS documentation.

If a specified tag does not already exist in the Palo Alto Networks device, the action also creates the new tag. The tag creation does not require a commit in the Palo Alto Networks environment.

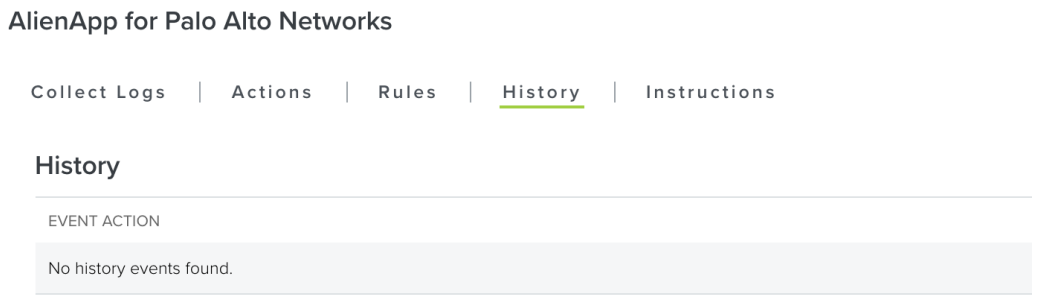
To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.

Note: To use the Dynamic Address Group actions, you first need to configure

Dynamic Address Groups in your policy within PAN-OS.

5. Click the **History** tab to display information about the executed orchestration actions.



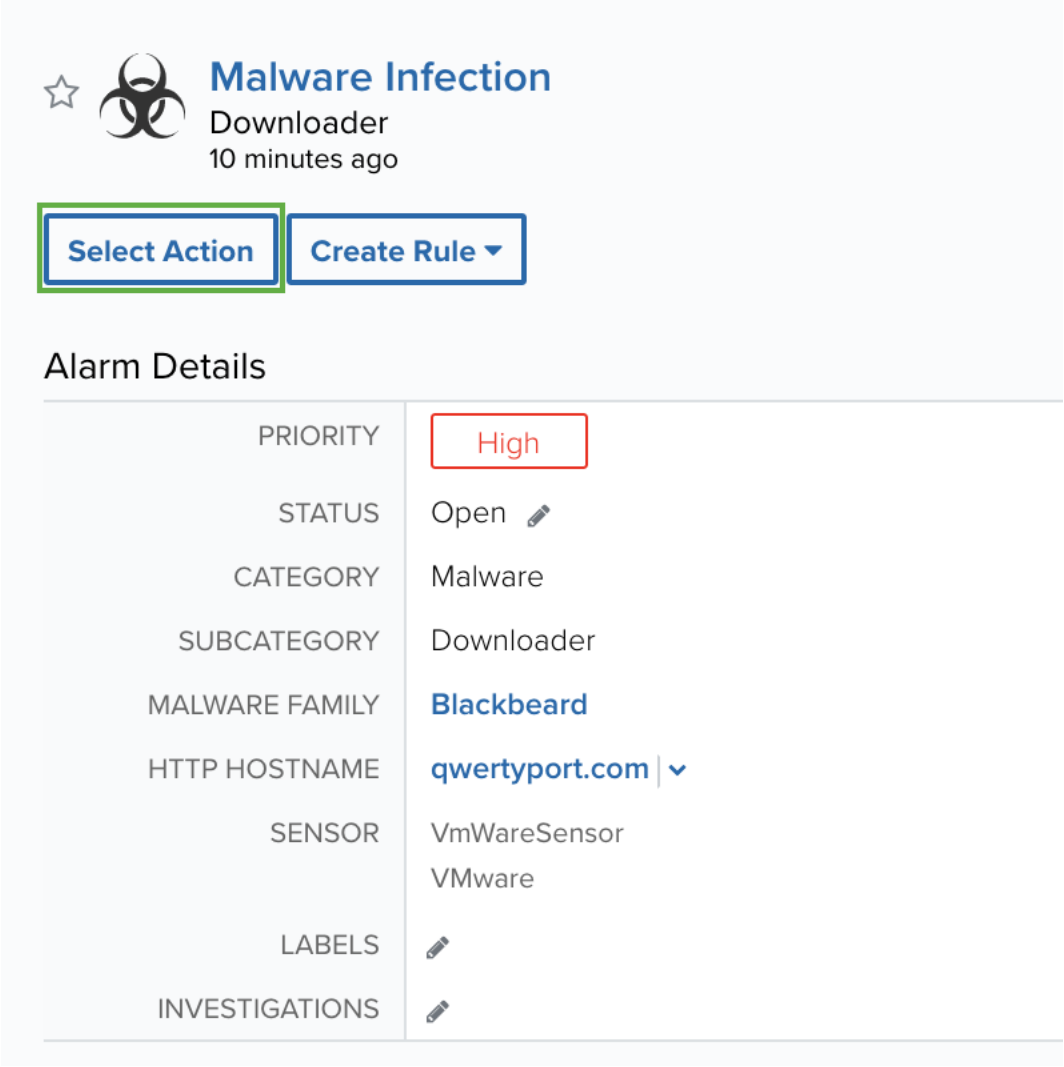
Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

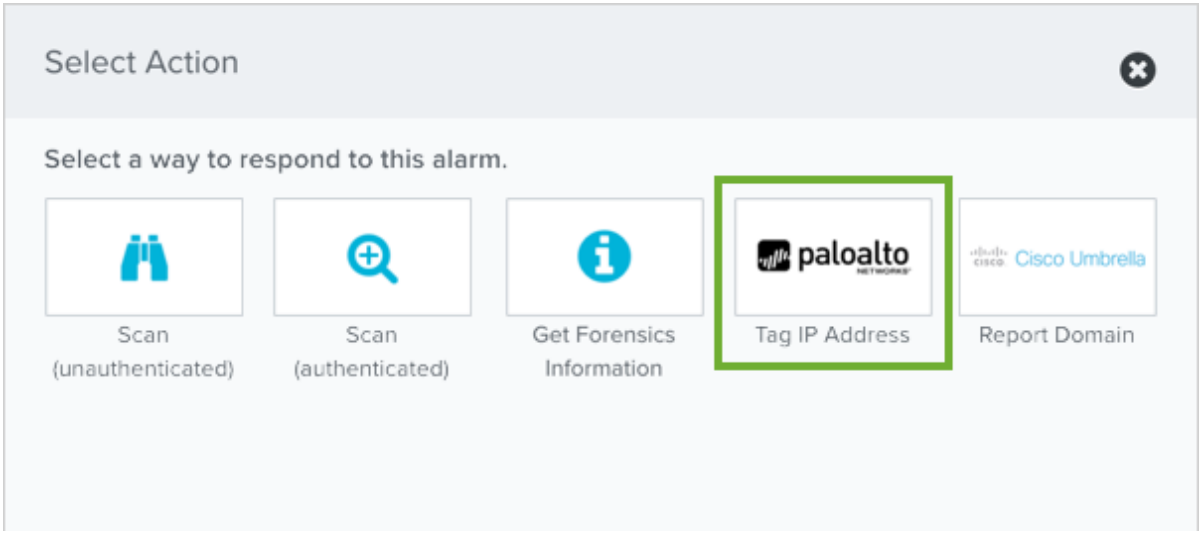
Note: All Group and Tag names will default to lowercase in USM Anywhere to avoid any potential confusion over letter casing.

To launch a Palo Alto Networks orchestration action for an alarm

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.


Malware Infection
Downloader
10 minutes ago
Select Action
Create Rule
Alarm Details
PRIORITY
High
STATUS
Open
CATEGORY
Malware
SUBCATEGORY
Downloader
MALWARE FAMILY
Blackbeard
HTTP HOSTNAME
qwertyport.com
SENSOR
VmWareSensor
VMware
LABELS
INVESTIGATIONS

4. In the Select Action dialog box, select the **Palo Alto** tile.

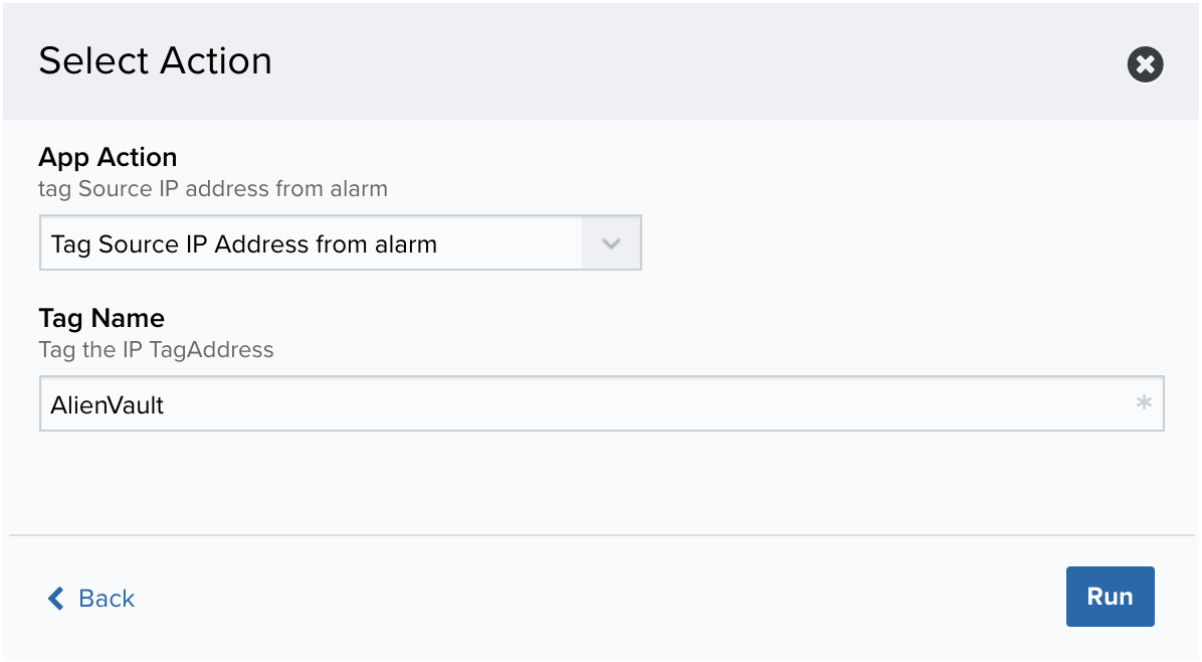


5. For the App Action, select the action you want to launch.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.

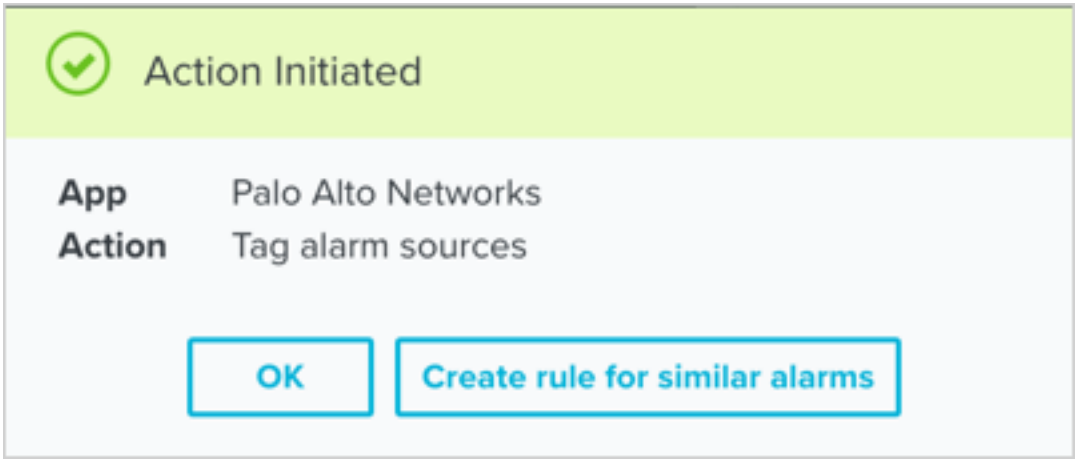
   You can launch an action to tag the alarm destination host or source host.

6. Enter the Palo Alto Networks Tag Name that you want to apply to the host.



7. Click **Run**.

After USM Anywhere initiates the action, it displays a confirmation dialog box.



If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Palo Alto Networks Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

Use the BlueApp for Palo Alto Networks PAN-OS to access the Palo Alto Networks response actions, which enable you to quickly respond to threats identified by USM Anywhere. You can create response action rules in USM Anywhere that automatically trigger when alarms or events match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically sends the host information for malware infections that it identifies to the connected Palo Alto Networks device as a request to tag the host for policy enforcement.

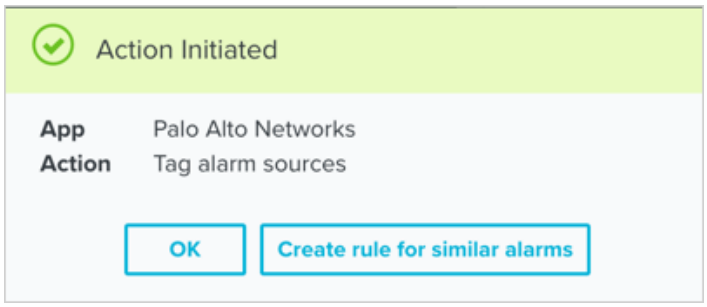
Note: All Group and Tag names will default to lowercase in USM Anywhere to avoid any potential confusion over letter casing.

After you create a rule, new events or alarms that match the rule will trigger the Palo Alto Networks action to tag to the associated source or the destination host. The rule does **not** trigger for your existing alarms or events.

You can create a new rule in one of two ways:

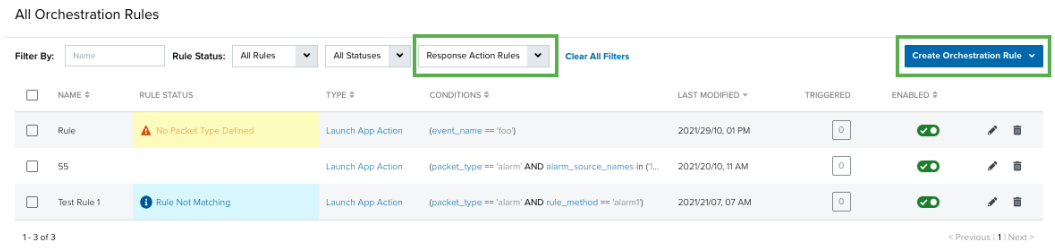
- **From an Applied Response Action:** You can automatically create a rule using the response action that you apply to an existing alarm or event. This makes it easy to set the matching conditions for the rule based on the existing item and use the same settings that you applied to that item.

  In the confirmation dialog box, click **Create rule for similar alarms** or **Create rule for similar events**.



- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click **Create Orchestration Rule > Response Action Rule** to define the new rule.

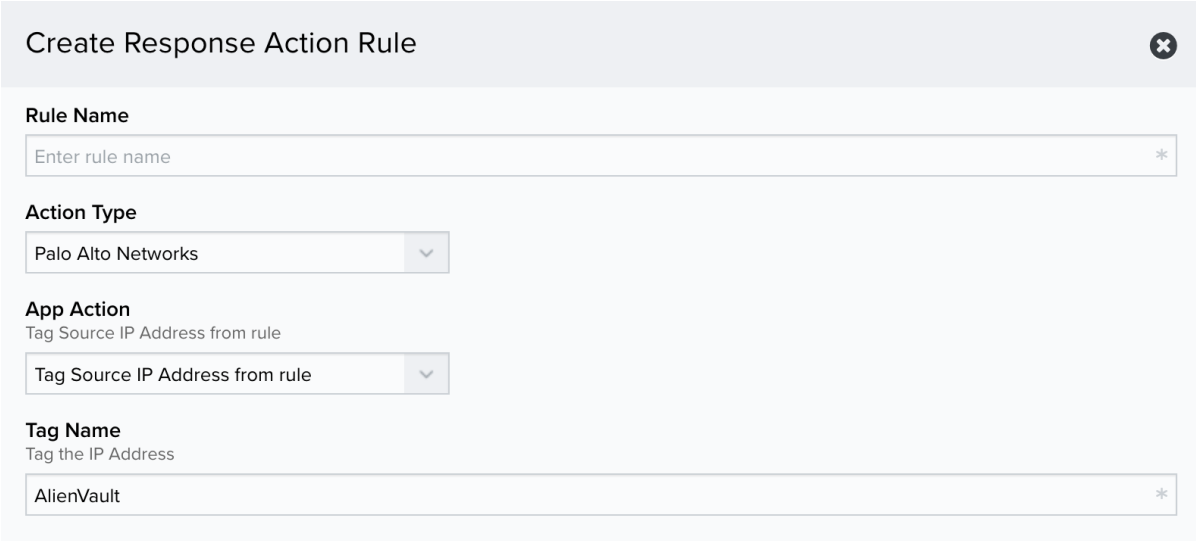


To define a new Palo Alto Networks response action rule

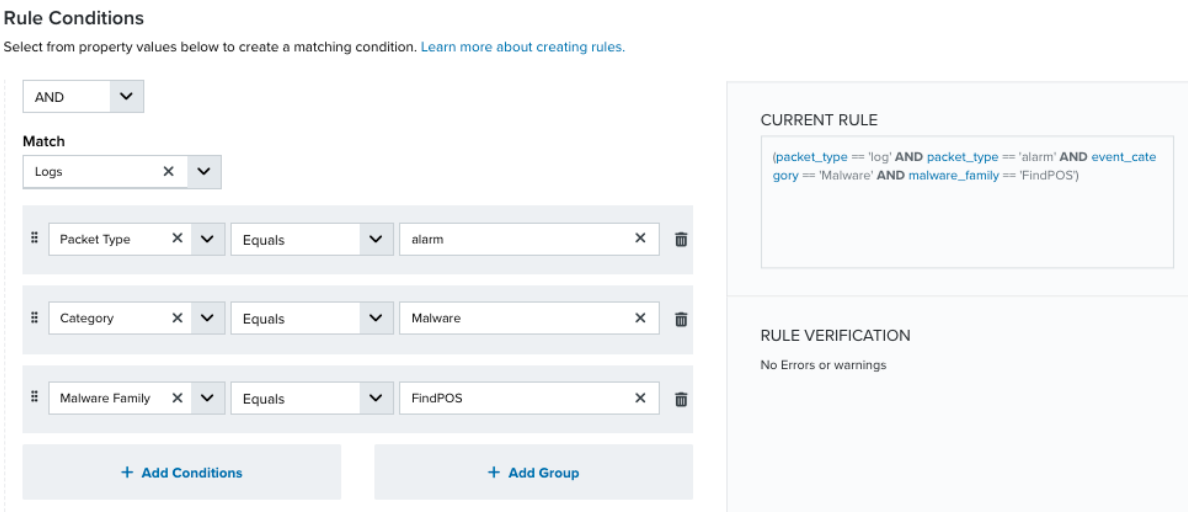
1. Enter a name for the rule.
2. For the Action, select the action you want to launch.

   You can launch an action to tag the destination host or source for an alarm or an event.

3. Enter the Palo Alto Networks Tag Name that you want to apply to the host.



4. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.

- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

5. Click **Save Rule**.

Collecting Logs from Palo Alto Networks

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

To fully integrate USM Anywhere with your Palo Alto Networks firewall, you should configure log collection so that USM Anywhere can retrieve and normalize raw log data from the firewall. BlueApp for Palo Alto Networks PAN-OS provides data normalization and analysis for Palo Alto Networks PAN-OS logs.

Before configuring the Palo Alto Networks PAN-OS log collection, you must have the IP Address of the USM Anywhere Sensor.

To configure PAN-OS to send log data to USM Anywhere

1. Configure PAN-OS to output events in Common Event Format (CEF). See the PAN-OS CEF Configuration Guide for instructions.

   Note: The vendor documentation references ArcSight, but it applies to USM Anywhere as well.

2. Add a syslog server profile. See the PAN-OS Administrator's Guide on Configure Syslog Monitoring for instructions.

   - For Syslog Server, enter the IP address of the USM Anywhere Sensor.
   - Select the transport protocol you want to use. USM Anywhere supports UDP, TCP, and TLS.
   - The port number depends on the transport protocol you choose. Use **514** for UDP, **601** for TCP, or **6514** for TLS.

3. Configure syslog forwarding on PAN-OS. See the PAN-OS Administrator's Guide on Configure Log Forwarding for instructions.

Note: The syslog messages from PAN-OS do not include the time zone setting on the device, so USM Anywhere assumes that all time occurs in Coordinated Universal Time (UTC), which is used by most devices. If your Palo Alto Network device is using a different time zone than UTC, the time information in the events will appear wrong. To correct this, configure your Palo Alto Network device to use UTC instead. See PAN-OS Web Interface Reference on Device Management for instructions.

BlueApp for Palo Alto Networks Panorama

The BlueApp for Palo Alto Networks Panorama enables you to automate intrusion detection and response activities between USM Anywhere and Palo Alto Networks Panorama. The BlueApp for Palo Alto Networks Panorama enhances the threat detection capabilities of USM Anywhere by providing orchestration actions to streamline incident response activities based on risks identified in USM Anywhere.

Edition: The BlueApp for Palo Alto Networks Panorama is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Palo Alto Networks Panorama

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

When the BlueApp for Palo Alto Networks Panorama is enabled and connected to your Palo Alto Networks environment, you can launch app actions and create orchestration rules to send data from USM Anywhere to your Palo Alto device. See BlueApp for Palo Alto Networks Panorama Actions for more information about the orchestration actions supported by the BlueApp for Palo Alto Networks Panorama,

BlueApp for Palo Alto Networks Panorama Setup

Tto configure Palo Alto Networks Panorama in USM Anywhere, you need the following:

- A dedicated Palo Alto Networks Panorama admin account with the account password
- The IP address or hostname of the Panorama instance
- API access enabled in your Panorama account
- Syslog forwarding enabled in Panorama

To generate API access in Panorama

1. Go to the Palo Alto Networks Panorama documentation and follow the vendor instructions to enable API access.
2. Enable all XML API features.

To enable log forwarding in Panorama

1. Go to the Palo Alto Networks Panorama Log Forwarding documentation and follow the vendor instructions.
2. In step 2 of the instructions, follow the instructions to configure a syslog server profile.

Enable BlueApp for Palo Alto Networks Panorama in USM Anywhere

Once you have enabled API access and log forwarding in Panorama, you can enable the BlueApp for Palo Alto Networks Panorama in USM Anywhere.

To enable the BlueApp for Palo Alto Networks Panorama in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.

5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Specify the connection information for Palo Alto Networks:

   - **IP address or hostname**: Enter the IP address or hostname of your Panorama instance.
   - **User Name**: Enter the name of the admin account you created.
   - **Password**: Enter the password for the Palo Alto Panorama user account.
   - (Optional) **Validate HTTPS host name**: Select the checkbox to validate the HTTPS host-name.

7. Click **Save**.

BlueApp for Palo Alto Networks Panorama Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use Palo Alto Networks Panorama actions to respond to the events in your environment. Rather than manually adding addresses in the Panorama user interface (UI) and entering the relevant information, you can use the BlueApp for Palo Alto Networks Panorama response actions to automatically manage your Palo Alto Networks address groups using information from your USM Anywhere environment. The table below shows the actions.

Actions for the BlueApp for Palo Alto Networks Panorama

Action	Description
Add Address to Address Group	Run this action to add the source, destination, or custom address to a group in your Panorama environment. If the group doesn't exist in Panorama, it will be created by the action from USM Anywhere
Remove Address from Address Group	Run this action to remove the source, destination, or custom address to a group in your Panorama environment

Actions for the BlueApp for Palo Alto Networks Panorama (Continued)

Action	Description
Add Tag to Address	Run this action to add a Panorama tag to an address. You can select either an existing tag from Panorama, or create a new one
Add Tag to Address Group	Run this action to add a Panorama tag to an address group. You can select either an existing tag from Panorama, or create a new one
Add Address to URL Category	Run this action to add a source or destination address to a Palo Alto Networks Panorama URL category to allow, alert, or block the URL based on the selected existing profile You can include optional pre-rule or post-rule policies that are based on your Panorama policy profiles If you select an Associated Profile in the action, the user will receive an alert if the policy is violated
Add IP to External Block List	Run this action to add an IP address to the Palo Alto Networks Panorama external block list
Add Domain to External Block List from Event/Alarm	Run this action to add a domain to the Palo Alto Networks Panorama external block list from an event or alarm to restrict their access
Add Domain to External Block List	Run this action to add a domain to the Palo Alto Networks Panorama external block list to restrict their access
Add Domain to External Block List from Rule	Run this action to add a domain to the Palo Alto Networks Panorama external block list from a rule to restrict their access
Add Domain to External Block List from Orchestration Rule	Run this action to add a domain to the Palo Alto Networks Panorama external block list from an orchestration rule to restrict their access
Add IP Address to External Block List from Event/Alarm	Run this action to add an IP address to an external block list from an event or alarm to restrict their access

Actions for the BlueApp for Palo Alto Networks Panorama (Continued)

Action	Description
Add IP Address to External Block List from Orchestration Rule	Run this action to add an IP address to an external block list from an orchestration rule to restrict their access
Get External Block List	Run this action to retrieve the external block list
Add URL to External Block List	Run this action to add a URL to the Palo Alto Networks Panorama external block list

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to send a request to your connected Panorama instance to add source or destination IP address information to an existing Panorama group. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from an action applied to an alarm, event, or vulnerability.

To launch a Panorama response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Panorama Action**.
5. Select the app action and fill out the fields that are populated in the window.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

External Block List

The external block lists for IP addresses, domains, and URLs, are all contained in the BlueApp for Palo Alto Networks Panorama page (**Data Sources > AlienApps > Palo Alto Panorama**). For each tab, you can see the list of all the items on the block list, and you can remove individual items by clicking the icon next to the item. Each tab also contains these buttons above the list:

- **Add:** Opens a dialog box to add an IP address, domain, or URL to the list.
- **Import:** Opens a dialog box to import a text file to import a list of IP addresses, domains, or URLs to the list. This enables you to take your copied block list from another sensor and apply it to the current sensor.
- **Export:** Exports the entire IP address, domain, or URL list as a downloadable .txt file. This enables you to copy your block list to another sensor.
- **Clear:** Clears the entire IP address, domain, or URL list.

Creating Palo Alto Panorama Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Palo Alto Networks Panorama response action when events, alarms, or vulnerabilities match the criteria that you specify. After you create a rule, new events, alarms, or vulnerabilities that match the rule, conditions will trigger the Panorama response action to initiate the response action. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about

managing orchestration rules.

Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

To define a new Panorama response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the Panorama incident.

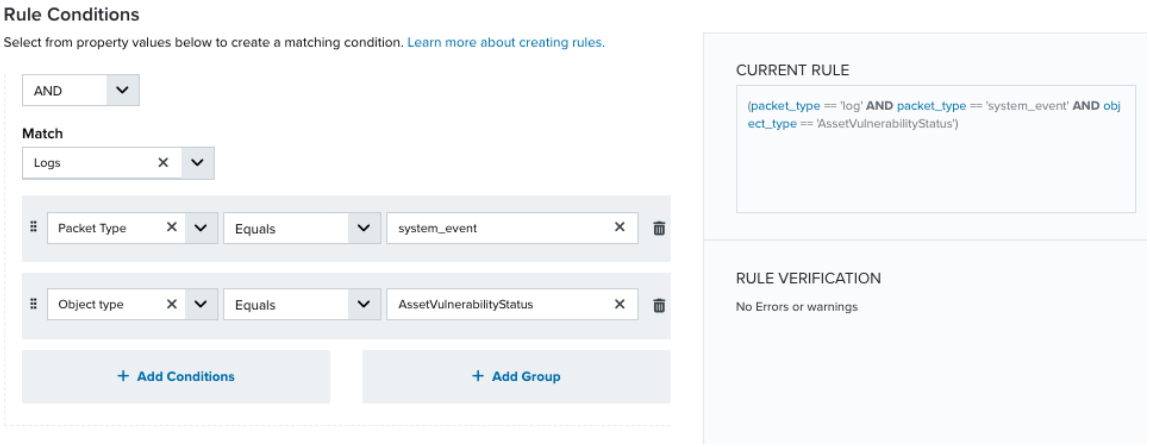
   The Panorama parameters that you set will depend on the action that you select.

   - Create a New Incident from a Vulnerability Status Update

     This is the default action if you create the rule after applying a Panorama response action to a vulnerability. Use this action to open a new incident when a status change occurs for a vulnerability that satisfies the matching criteria.

     Important: To match vulnerability status updates, your rule must include the following criteria: `(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus')`.

     However, it is important to be aware that this will return all vulnerability status changes matching these rules. It is advisable to narrow the rule with further conditions. Additionally, you can create a similar alarm rule first to test the amount of responses it would generate when active before you use the rule with Palo Alto Panorama..



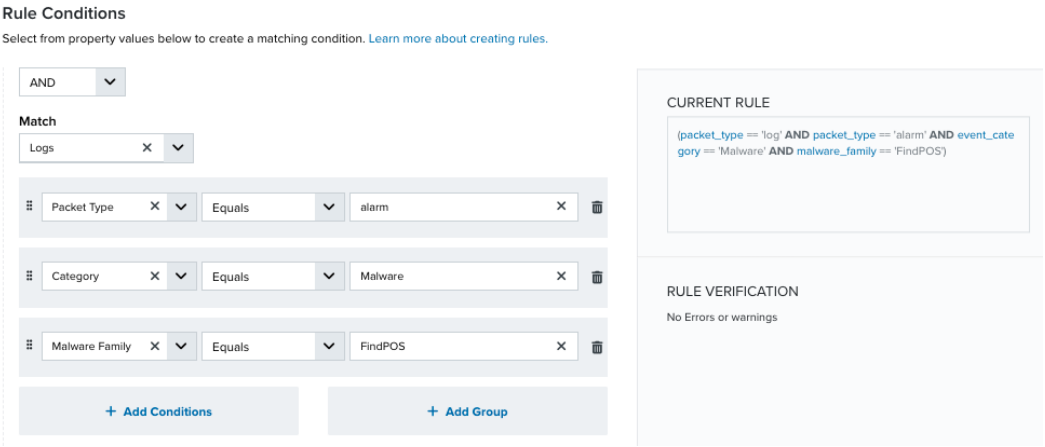
- Create a New Incident from an Alarm

  This is the default action if you create the rule after applying a Panorama response action to an alarm. Use this action to open a new Panorama incident for a new alarm that satisfies the matching criteria.

- Create a New Issue from Event-Based Orchestration

  Use this action to open a new Panorama incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red

border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Palo Alto Networks Prisma Access

The BlueApp for Palo Alto Networks Prisma Access integrates with the Prisma Access Cloud to give customers rich response actions to use in response to threats detected in the environment. It provides several different mechanisms to modify security policy and as well as the ability to block files and change alert statuses.

Important: Palo Alto Networks delivers logs for Prisma Access via their Cortex Data lake using Syslog. USM Anywhere supports this log source.

Edition: The BlueApp for Palo Alto Networks Prisma Access is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Palo Alto Networks Prisma Access

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

To configure the BlueApp for Palo Alto Networks Prisma Access in USM Anywhere, you need to have authentication credentials for Prisma Access with the appropriate permissions.

Set up the Prisma Access API

Follow the instructions listed in the Prisma Access documentation. Here are the instructions on how to generate the client ID and client secret for USM Appliance.

To generate the required credentials

1. Log into Palo Alto Prisma Access as an Admin user.
2. Navigate to **Settings > Identity & Access**.
3. Select **Add Identity**, then **Service Account**.
4. Configure a user with one of the following roles:

1. Superuser
2. Web Security Admin
3. Security Administrator

Configure the BlueApp for Palo Alto Networks Prisma Access in USM Anywhere

To enable the BlueApp for Palo Alto Networks Prisma Access

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the authentication credentials, including client ID and client secret.
7. Click **Save**.

BlueApp for Palo Alto Networks Prisma Access Actions

The BlueApp for Palo Alto Networks Prisma Access provides a set of orchestration actions that you can use to modify your security policy, block files, and change alert statuses in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Palo Alto Networks Prisma Access

Action	Description
Add Tag to Address	Add a tag to an address. If the tag does not already exist, a new tag will be created and added.
Remove tag from Address	Remove a tag from an address.

Actions for the BlueApp for Palo Alto Networks Prisma Access (Continued)

Action	Description
Add Tag to Address Group	Add a tag to an address group. If the tag does not already exist, a new tag will be created and added. If the address group does not already exist, a new address group will be created and tagged.
Remove Tag from Address Group	Remove a tag from an address group.
Add Address to Address Group	Add an address to an address group. If the address group does not already exist, a new address group will be created and the address added to it.
Remove Address from Address Group	Remove an address from an address group.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms, Events, Investigations, and Rules

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an Alarm, Event, Investigation, or Rule.

To launch a Prisma Access response action for an Alarm, Event, Investigation, or Rule

1. Go to **Activity > Alarms** or **Activity > Events**, **Investigations**, or **Settings > Rules**.
2. Click the Alarm, Event, Investigation, or Rule to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Palo Alto Prisma Access Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar investigations Create rule for similar alarms** or **Create rule for similar events** or **Create rule for similar rules** and define the new rule. If not, click **OK**.

BlueApp for Qualys

The BlueApp for Qualys enables you to integrate the Qualys threat protection and scanning capabilities with your USM Anywhere instance. The BlueApp for Qualys enhances the capabilities of your threat detection management by utilizing the Qualys asset scanning abilities. It takes the asset scan results (vulnerabilities) and asset management capabilities and merges them with USM Anywhere. The BlueApp for Qualys also adds unique threat collection, orchestration, and response capabilities to your workflow.

Note: The BlueApp for Qualys does not support Qualys's IP tracking feature. If you have enabled IP tracking in Qualys, asset filtering and orchestration rules will not be available in the AlienApp.

Edition: The BlueApp for Qualys is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for Qualys

Role Availability ✗ Read-Only ✗ Investigator ✗ Analyst ✓ **Manager**

To configure the BlueApp for Qualys, you need to enter your Qualys username, password, and API URL in USM Anywhere.

Qualys API Configuration

To enable Qualys in USM Anywhere, you need an admin user account and password, and you need to enter your API URL in USM Anywhere. See Qualys' Identify your Qualys Platform documentation to learn how to get your API URL.

Note: The BlueApp for Qualys does not support Qualys's IP tracking feature. If you have enabled IP tracking in Qualys, asset filtering and orchestration rules will not be available in the AlienApp.

Configure BlueApp for Qualys in USM Anywhere

To enable the BlueApp for Qualys

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Qualys Username and Password, and the API URL.
7. (Optional.) Use the checkboxes to enable the BlueApp for Qualys to create and merge assets:
   - Check **Allow Automatic Creation of New Assets** to enable Qualys scans to create new assets in USM Anywhere.
   - Check **Allow Automatic Merging of Existing Assets** to enable USM Anywhere to run a match against the Qualys identification to merge the assets found with existing USM Anywhere assets.

Important: If you want to create new assets, you need to select both options, **Allow Creation of New Assets** and **Allow Merging of Existing Assets**, to prevent the duplication of assets. USM Anywhere won't create new assets if you only select one of the options.

See BlueApp for Qualys Asset Discovery and Management for more details on the asset creation and merging processes.

8. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Qualys Asset Discovery and Management

The BlueApp for Qualys features powerful vulnerability assessment capabilities than can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow Qualys to create assets that are discovered in scans, as well as merge the asset information provided from the Qualys scan with the existing asset information in USM Anywhere.

Asset Creation from BlueApp for Qualys

When Qualys runs a scan, it identifies all assets in the scan and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in app's configuration menu. Assets created from a Qualys scan will include the information ported from Qualys in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in Qualys scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the Qualys configuration menu, USM Anywhere will merge the information from the Qualys scan with the existing asset. Assets are matched by comparing the ID, IP address, and host name (if valid) from the Qualys scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the Qualys configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for Qualys page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the Qualys scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the Qualys scan.
- **Merge:** Merge the information from the Qualys scan with the matching asset details in USM Anywhere.
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a Qualys profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

A window displays showing the existing asset and the new asset that will be created once the two are split.

4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for Qualys Actions

The BlueApp for Qualys provides a set of orchestration actions that you can use to identify threats and manage assets in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Qualys

Action	Description
Tag Asset	Run this action to add a Qualys tag to an asset
Scan IP From Rule	Run this action to scan a source or destination IP address from a rule
Single Asset Scan	Run this action to scan a single asset from a vulnerability
Asset Discovery	Qualys asset discovery feature
Collect Alert	Run this action to collect alert from Qualys scan from an asset
Vm Single Asset Scan	Run this action to scan a single asset for a vulnerability from a vulnerability
Vm Single Asset Scan	Run this action to scan a single asset for a vulnerability from an asset
Scan Destination IP from Rule	Run this action to scan a destination IP from a rule
Scan Source IP from Rule	Run this action to scan a source IP from a rule
Remove Asset Tag	Run this action to remove an asset tag from Qualys

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Vulnerabilities

You can launch an action directly from vulnerabilities. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to a vulnerability.

To launch a Qualys response action for an alarm or event

1. Go to **Activity > Vulnerabilities**.
2. Click the vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Qualys Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for the vulnerability, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar vulnerabilities** and define the new rule. If not, click **OK**.

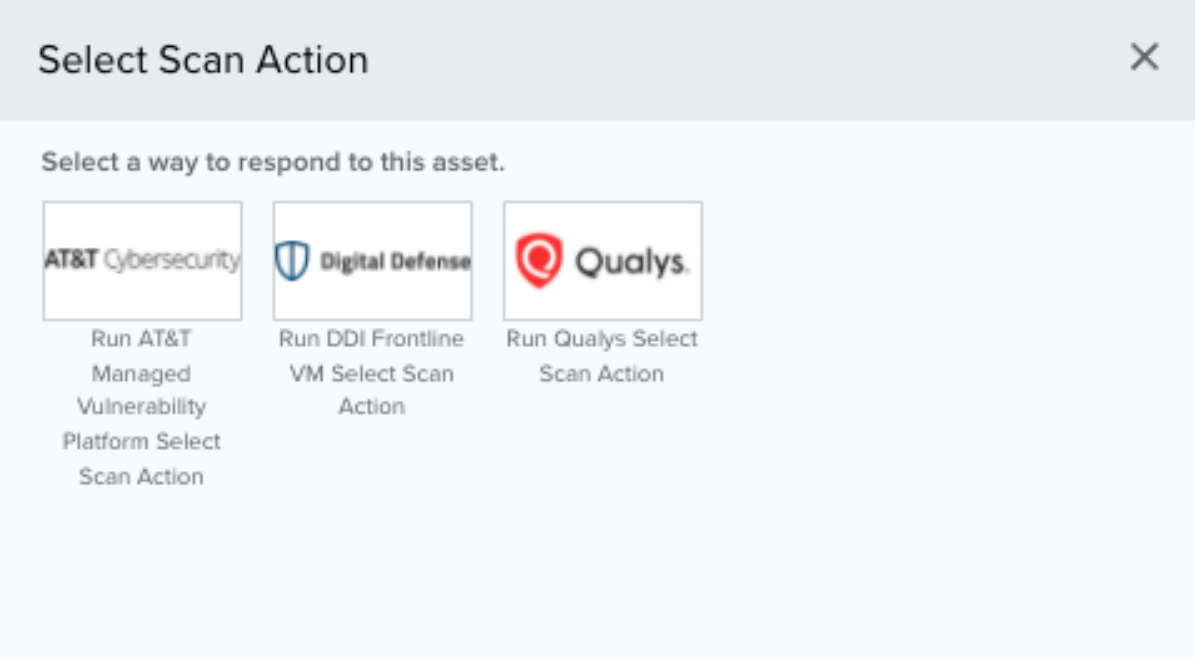
Scan an Asset

You can scan a single asset with BlueApp for Qualys from either the Asset or Vulnerabilities pages.

Too run an asset scan from the Vulnerabilities Page

1. Go to **Environment > Assets**.
2. Complete one of these options to open the Select Scan Action dialog box:
   - Next to the asset name that you want to scan, click the icon, select **Full Details**, and then select **Actions > Scan with BlueApp**.
   - Next to the asset name that you want to scan, click the icon that you want to scan, and then select **Scan with BlueApp**.

   The Select Scan Action dialog box opens.



3. Click **Run Qualys Select Scan Action**.
4. Select **VM Single Asset Scan** from the App Action dropdown menu and fill out the fields that are populated below

To run an asset scan from the Assets page

1. Go to **Environment > Assets**.
2. Click the icon next to the Asset and click **Scan with BlueApp**.
3. Select **VM Single Asset Scan** from the App Action dropdown menu and fill out the fields that are populated below.

You can also run a Qualys asset scan by selecting **Action > Scan with BlueApp** on an asset's Full Asset Details page.

Creating Qualys Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Qualys response action when vulnerabilities, match the criteria that you specify. This way, you can automate the way you filter IP addresses into the policies within Qualys.

Note: The BlueApp for Qualys does not support Qualys's IP tracking feature. If you have enabled IP tracking in Qualys, asset filtering and orchestration rules will not be available in the AlienApp.

After you create a rule, new vulnerabilities that match the rule conditions will trigger the Qualys response action to create a new incident. The rule does not trigger for existing vulnerabilities.

You can create a new rule as follows:

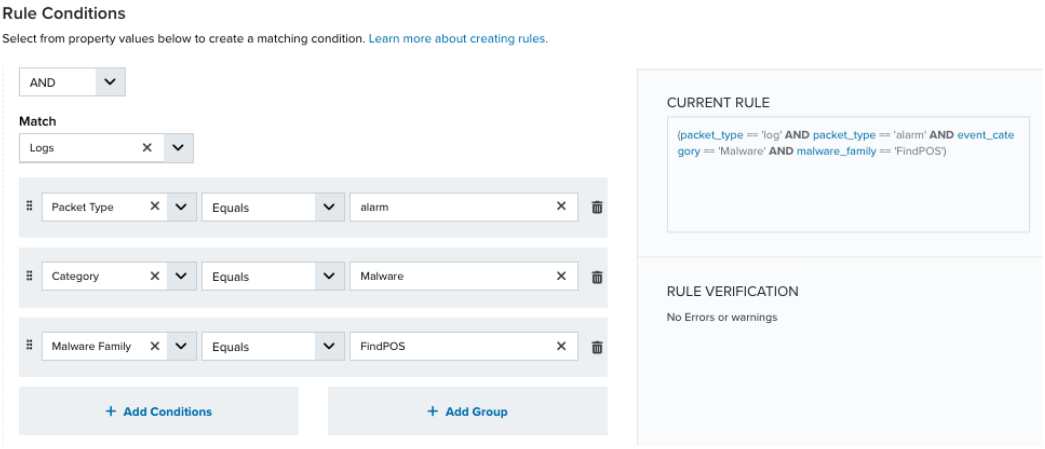
- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the App**: Go to the BlueApp for Qualys page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new Qualys response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the Qualys incident.
3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected vulnerability that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Salesforce

The BlueApp for Salesforce streamlines incident response activities by automatically opening Salesforce cases in response to threats detected by USM Anywhere. Upon execution of the action, USM Anywhere generates the Salesforce case and populates the case fields with details from an alarm, event or vulnerability.

Edition: The BlueApp for Salesforce is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: The BlueApp for Salesforce uses the Salesforce hourly event log API to pull events from your Salesforce instance on an hourly basis to minimize the latency of your important security event data. This is a paid feature and not enabled in a production Salesforce instance by default. Please ask your Salesforce Account Executive to enable it in your account if you have not done so already. The hourly event log feature is not required to use the case creation actions. USM Anywhere does not currently support importing events from the Salesforce Daily Event Log API.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Salesforce

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To use the BlueApp for Salesforce in USM Anywhere, you first need to log in to Salesforce to create the connected app and obtain the appropriate credentials. Because the account used to create the app will be responsible for creating all the Salesforce cases and will potentially be used by multiple users, it is recommenced that you create a separate, dedicated "service account" user. This user should have only enough permissions to allow the user to create cases. Do not reuse an admin account. Multiple accounts or users on different sensors may result in duplicated cases or cause confusion.

Important: Because of the way the Salesforce API implements event log processing, events can take at least three to six hours to be processed, potentially more.

Warning: The BlueApp for Salesforce uses the Salesforce hourly event log API to pull events from your Salesforce instance on an hourly basis to minimize the latency of your important security event data. This is a paid feature and not enabled in a production Salesforce instance by default. Please ask your Salesforce Account Executive to enable it in your account if you have not done so already. The hourly event log feature is not required to use the case creation actions. USM Anywhere does not currently support importing events from the Salesforce Daily Event Log API.

Salesforce Configuration Requirements

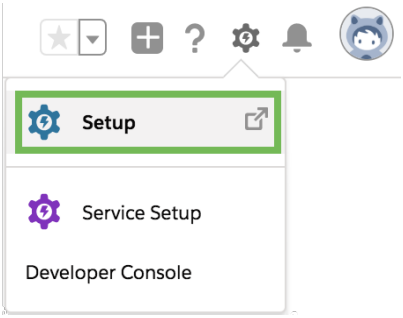
A user with a read-only (viewer) role will not be able to view log events from other users. Refer to the Salesforce permissions guidance to configure your service account user with adequate permissions:

- User Roles and Permissions
- Give Integration Users API Only Access
- Create a Permission Set and Grant API Enabled Access

Creating and Configuring the Connected App in Salesforce

To create the connected app in Salesforce

1. Log in to Salesforce with your username and password.
2. Go to the Settings Console by clicking the **Settings** icon.



3. In the Platform Tools menu on the left, go to **Apps > App Manager**.
4. Click the **New Connected App** button at the top of the Lightning Experience App Manager header.

   The New Connected App modal displays.

5. Fill out the required Basic Information fields:

- Connected App Name
- API Name
- Contact Email

6. In the API (Enable OAuth Settings) section, select the **Enable OAuth Settings** checkbox.

   The section expands with further options.

7. Leave the **Enable for Device Flow** checkbox checked, do not deselect it.

   The Callback URL field automatically populates the `https://login.salesforce.com/services/oauth2/success` link.

8. In the Available OAuth Scopes section, select the following options and click **Add** for each:

   - Access and manage your data (api)
   - Perform requests on your behalf at any time (refresh_token, offline_access)

9. Select the **Require Secret for Web Server Flow** checkbox.
10. Click **Save** to complete the app creation process and then click **Continue**.

Note: It takes time before the Salesforce app is completely created and recognized. LevelBlue recommends that you wait at least 20 minutes before entering the credentials in USM Anywhere.

To obtain your credentials and configure the Salesforce app

1. In the Salesforce Settings page, go to **Platform Tools > Apps > Connected Apps > Manage Connected Apps**.
2. Click the app you just created.

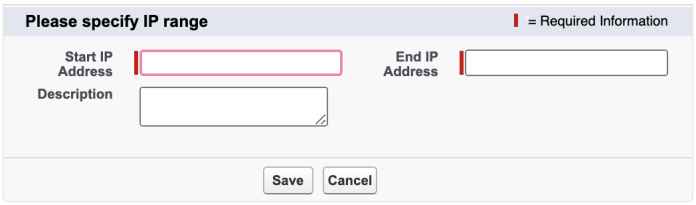
   The page displays the Consumer ID (which you will enter in USM Anywhere as the Client ID), and the Consumer Key (which is the Client Key in USM Anywhere).

3. In OAuth Policies, make sure **All users may self-authorize** is selected for Permitted Users, and make sure **Enforce IP Restrictions** is selected for IP Relaxation.

   Both should be set by default, but if not, click the **Edit Policies** button to change them.

4. In the menu tree on the left of the screen, select **Settings > Security > Network Access**.
5. On the Network Access page, in the Trusted IP Ranges section, click **New**.
6. Enter the global trusted IP range that contains the public IP address of the USM Anywhere

Sensor you are using, enter a description, and click **Save**.



Connecting the Salesforce App in USM Anywhere

After you obtain the OAuth, you must configure the connection within USM Anywhere.

To enable the BlueApp for Salesforce

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Client ID, Client Secret, Username, and Password for the Salesforce app you created.
7. In the Event Types field, you can specify the event types you want the BlueApp for Salesforce to collect.

   The BlueApp for Salesforce collects a default set of event types when the field is left blank. If you enter your own list of event types into the Event Types field, then USM Anywhere will collect those event types instead of the default set.

   The default event types are as follows:

   ```
   ApexCallout, ApexRestApi, ApexSoap, API, AsynchronousReportRun,
   DocumentAttachmentDownoads, InsecureExternalAssets, Login,
   LoginAs,TransactionSecurity, Search
   ```

Some event types may require an upgraded Salesforce subscription. A full list of Salesforce's supported event types and details on purchasing them can be found on their EventLogFile Supported Event Types documentation page.

8. Click **Save**.
9. Verify the connection.

   After USM Anywhere completes a successful connection to the Salesforce APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Salesforce connection.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.

4. (Optional.) Click the icon to customize the frequency of the event collection.

BlueApp for Salesforce Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, your team determines which items require the opening of a new Salesforce case. Rather than manually opening each case in the Salesforce user interface (UI) and entering the relevant alarm, event, or vulnerability information, you can use the BlueApp for Salesforce response actions to automatically create a Salesforce case with the short description and description fields pre-populated with content from your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Salesforce

Action	Description
Create a Salesforce Case	Run this action to generate a new Salesforce case from an alarm, event, response action, or vulnerability.
Pull Login History Events	Run this action to pull login history events from SalesForce
Pull Events	Run this action to pull events from SalesForce

Upon execution of a response action, USM Anywhere generates the Salesforce case and passes the associated information to that new incident case.

Note: Before launching a Salesforce response action or creating a Salesforce response action rule, the BlueApp for Salesforce must be enabled and connected to your Salesforce instance. See Configuring the BlueApp for Salesforce for more information.

To view information about these actions in USM Anywhere

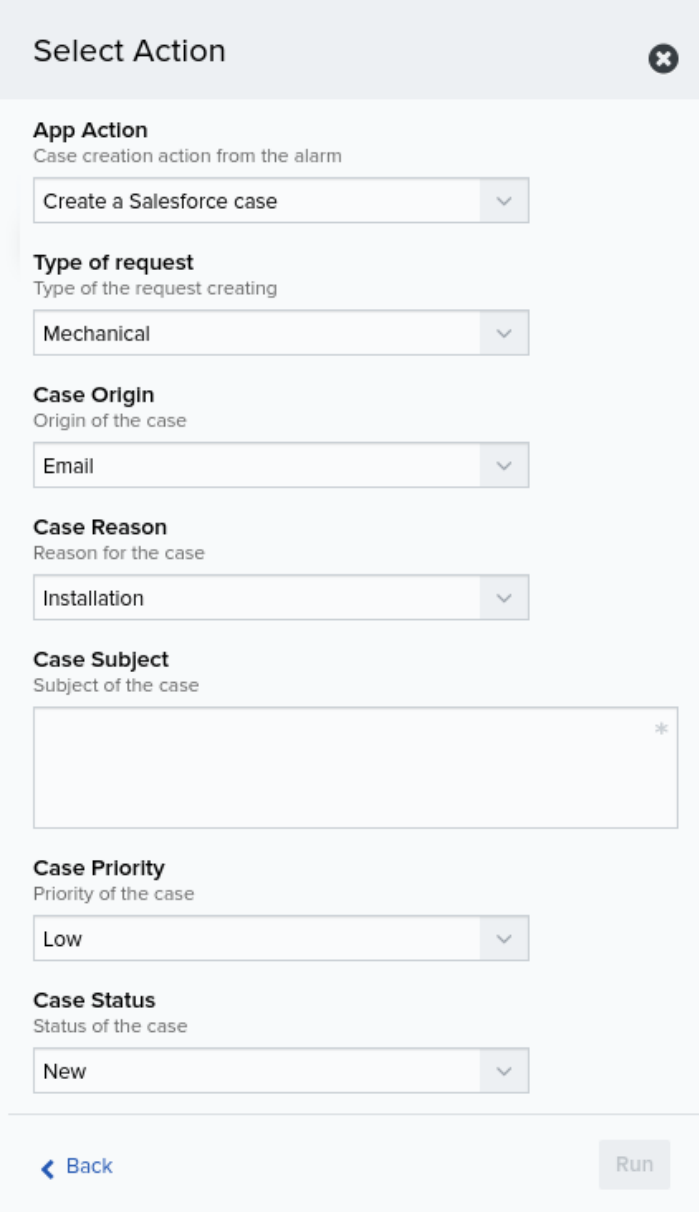
1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms

You can launch an action directly from alarms, events, or vulnerabilities. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm, event, or vulnerability.

To launch a Salesforce response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run Salesforce Action**.
5. Modify the information for the new incident for the following fields:
   - Type of Request
   - Case Reason
   - Case Subject
   - Case Priority
   - Case Status



6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Salesforce Response Action Rules

Role Availability ✗ Read-Only ✗ Investigator ✓ Analyst ✓ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Salesforce response action when events, alarms, or vulnerabilities match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically creates a new Salesforce incident when malware is detected so that a member of your response team can manage and address the issue. Salesforce events are updated on an hourly basis.

After you create a rule, new events, alarms, or vulnerabilities that match the rule conditions will trigger the Salesforce response action to create a new incident. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation pane. Then click **Create Response Action Rule** to define the new rule.

To define a new Salesforce response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the Salesforce incident.

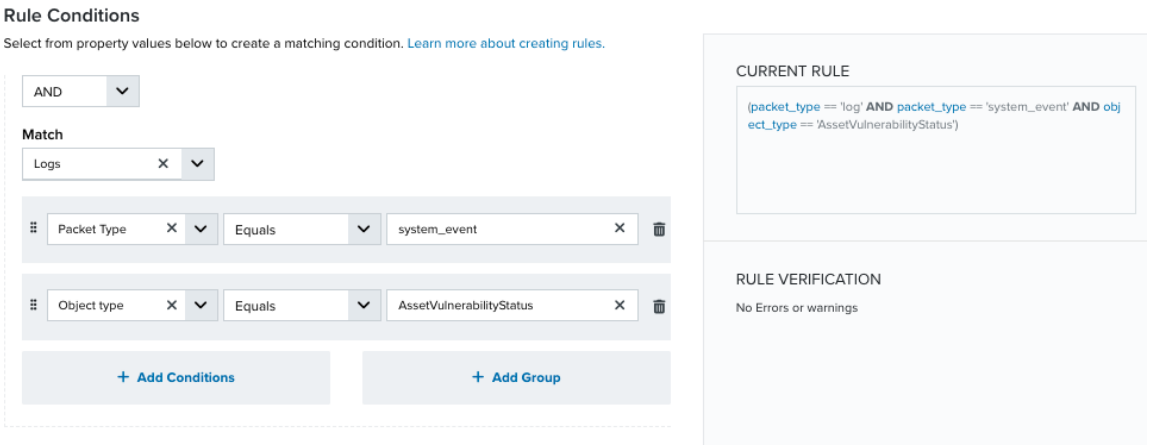
   The Salesforce parameters that you set will depend on the action that you select.

   - Create a New Incident from a Vulnerability Status Update

     Creating a new incident from a vulnerability status update is the default action if you create the rule after applying a Salesforce response action to a vulnerability. Use this action to open a new incident when a status change occurs for vulnerabilities that satisfy the matching criteria.

     Important: To match vulnerability status updates, your rule must include the following criteria: `(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus').`

     However, it is important to be aware that this will return all vulnerability status changes matching these rules. It is advisable to narrow the rule with further conditions. Additionally, you can create a similar alarm rule first to test the amount of responses it would generate when active before you use the rule to create Salesforce cases.



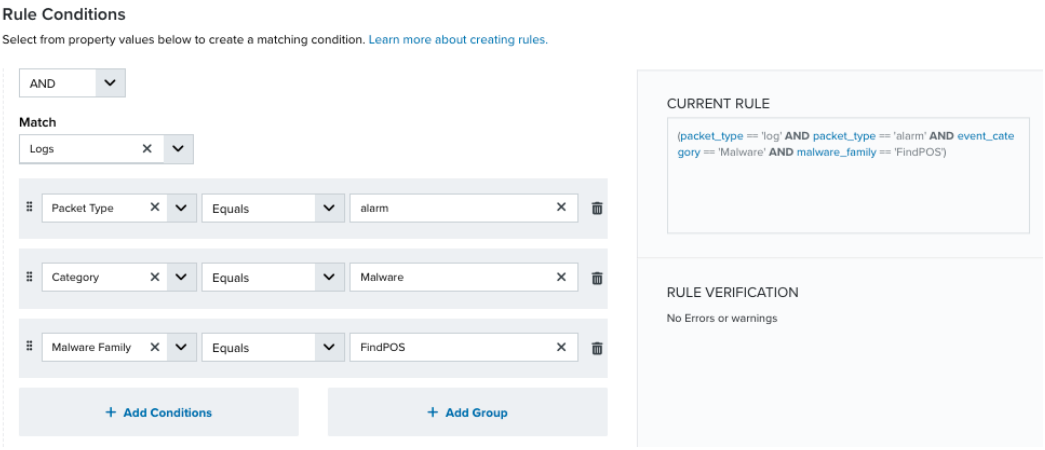
   - Create a New Incident from an Alarm

     Creating a new incident from an alarm is the default action if you create the rule after applying a Salesforce response action to an alarm. Use this action to open a new Salesforce incident for a new alarm that satisfies the matching criteria.

- Create a New Issue from Event-Based Orchestration

  Use the action of creating a new issue from event-based orchestration to open a new Salesforce incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for SentinelOne

The BlueApp for SentinelOne enables you to integrate the SentinelOne threat protection and scanning capabilities with your USM Anywhere instance. The BlueApp for SentinelOne enhances the capabilities of your threat detection management by utilizing the SentinelOne

asset scanning abilities. It takes the asset scan results (vulnerabilities) and asset management capabilities, including the SentinelOne Storyline Active-Response (STAR) custom detection rules, and merges them with USM Anywhere.

The BlueApp for SentinelOne also adds unique threat collection, orchestration and response capabilities to your workflow.

Note: SentinelOne STAR custom detection rules are only available to customers who purchase SentinelOne through AT&T. USM Anywhere users who have purchased USM Anywhere and SentinelOne separately will not have access to the STAR detection rules.

Edition: The BlueApp for SentinelOne is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

This topic discusses these subtopics:

Configuring the BlueApp for SentinelOne

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

SentinelOne API Configuration

To configure BlueApp for SentinelOne in USM Anywhere, you need to generate an API key in your SentinelOne instance and enter it into USM Anywhere.

To set up your SentinelOne API

1. Log in to your SentinelOne management console.
2. Select **My User** under your name in the upper right of the console.
   The permissions granted to your user account will also be the permissions available to your BlueApp for SentinelOne. Ensure that your account has either Admin or Incident Response Team privileges.
3. In the My User window, click **Actions**, and then **Generate API token**.

Note: Users with Admin permissions will click the **Actions** button, but users with IR Team or similar permissions will click **Options** in its place.

4. Click **Download** to save the API token, or copy it to paste into the AlienApp.
   You will enter the API token in the BlueApp for SentinelOne when you configure the AlienApp.

Important: If you generate a new API token at some point in the future, it will revoke the token you just generated and render the connection configured with it unauthorized. To reestablish your connection through the AlienApp, you must update the token configured in your BlueApp for SentinelOne.

Note: If you have previously enabled syslog collection for the SentinelOne Syslog BlueApp, you need to disable syslog collection when you connect the SentinelOne API to USM Anywhere to prevent duplicate logs.

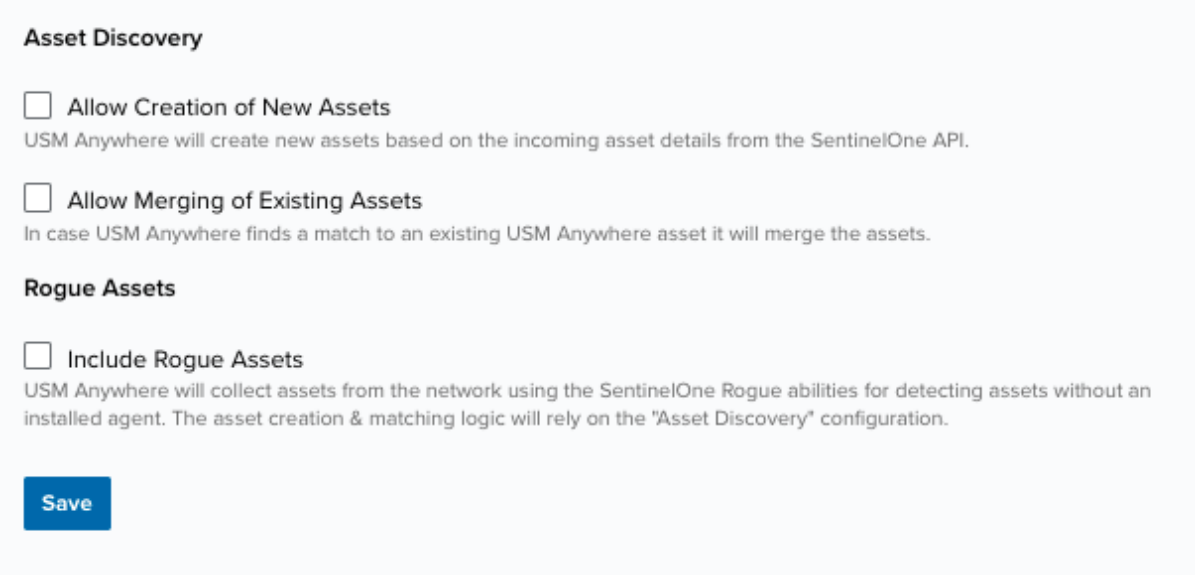
In the SentinelOne management console, go to **Settings > Integrations > Syslog** and click **Disable Syslog** if it is currently enabled.

Configure BlueApp for SentinelOne in USM Anywhere

To enable the BlueApp for SentinelOne

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Enter the Management URL of your SentinelOne instance, your SentinelOne Username, and the API Token you created.
7. Use the checkboxes to enable the BlueApp for SentinelOne to create and merge assets.



- Select the **Allow Creation of New Assets** checkbox to enable SentinelOne scans to create new assets in USM Anywhere.
- Select the **Allow Merging of Existing Assets** checkbox to enable USM Anywhere to run a match against the SentinelOne identification to merge the assets found with existing USM Anywhere assets.

  Important: If you want to create new assets, you need to select both options, **Allow Creation of New Assets** and **Allow Merging of Existing Assets** to prevent the duplication of assets. USM Anywhere won't create new assets if you only select one of the options.

- Select the **Include Rogue Assets** checkbox to enable USM Anywhere to collect and detect assets without an installed agent.

  See BlueApp for SentinelOne Asset Discovery and Management for more details on the asset creation and merging processes.

8. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

The BlueApp for SentinelOne and the BlueApp for AT&T Managed Endpoint Security

Because both the BlueApp for SentinelOne and the BlueApp for AT&T Managed Endpoint Security share configuration components through BlueApp for SentinelOne, configuring one BlueApp will cause the other to appear as configured in your My Apps page. This is expected behavior. Do not delete or disable the BlueApp for SentinelOne or the BlueApp for AT&T Managed Endpoint Security. Changes to one BlueApp will cause configuration errors with the other BlueApp.

To ensure your API tokens remain up-to-date, the SentinelOne and AT&T Managed Endpoint Security Apps both include a scheduler job that automatically regenerates the API token. This job is not editable and runs automatically once the app is configured.

Note: Whether you are using the BlueApp for SentinelOne or the AlienApp for AT&T Managed Endpoint Security, this job will appear in your scheduled jobs as a SentinelOne job.

Important: This job will appear in your scheduled jobs as disabled until your SentinelOne app is fully configured.

BlueApp for SentinelOne Asset Discovery and Management

The BlueApp for SentinelOne features powerful vulnerability assessment capabilities than can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow Sentinel One to create assets that are discovered in scans, as well as merge the asset information provided from the SentinelOne scan with the existing asset information in USM Anywhere.

Asset Creation from BlueApp for SentinelOne

When SentinelOne runs a scan, it identifies all assets in the scan and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in app's configuration menu. Assets created from a SentinelOne scan will include the information ported from SentinelOne in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in SentinelOne scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the SentinelOne configuration menu, USM Anywhere will merge the information from the SentinelOne scan with the existing asset. Assets are matched by comparing the Sentinel One ID, MAC address, IP address, and host name (if valid) from the SentinelOne scan with the same asset details in USM Anywhere.

Rogue Assets

You can select the **Include Rogue Assets** checkbox in the SentinelOne configuration menu. This checkbox enables USM Anywhere to collect assets from the network using the SentineOne Rogue abilities for detecting assets without an installed agent.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the SentinelOne configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for SentinelOne page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the SentinelOne scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the SentinelOne scan.
- **Merge:** Merge the information from the SentinelOne scan with the matching asset details in USM Anywhere
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a SentinelOne profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the button next to the asset, and then click **Full Details**.
3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window displays showing the existing asset and the new asset that will be created once the two are split.
4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for SentinelOne Actions

The BlueApp for SentinelOne provides a set of orchestration actions that you can use to identify threats and manage assets in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Important: Most BlueApp for SentinelOne actions can only be applied to associated events generated from the SentinelOne BlueApp scheduler or events that contain a SentinelOne threat identifier (ID). Events not associated with SentinelOne will not trigger most actions from USM Anywhere.

Events that do not contain a SentinelOne threat ID can be used to create a denylist entry enabling you to add any process or file to your denylist, not just ones that SentinelOne detects as suspicious.

Actions for the BlueApp for SentinelOne

Action	Description
Initiate Scan	Run this action to initiate a full disk scan on the endpoint asset
Mitigate Threats	Run this action to kill, remediate, rollback, quarantine, or un-quarantine a threat based on the analyst verdict of the threat
Add to Denylist	Run this action to add a threat to the denylist Scope of restrictions can be defined by account, group, or site
Add to Exclusion List	Run this action to add a threat to exclusion list Scope of restrictions can be defined by account, group, or site Exclusion is defined by type (certificate, path, or hash)
Disconnect Asset from Network	Run this action to disconnect the asset from the network
Disable Agent	Run this action to disable an asset, and disables detection, device control (Microsoft Windows only), firewall, SentinelOne Ranger scanning (Windows only), and anti-tampering (Windows only) on that asset
Enable Agent	Run this action to enable an agent that has been previously disabled
Reconnect Asset to Network	Run this action to reconnect the asset to the network
Restart Machine	Run this action to restart the machine connected to the asset
Activity Logs	Run this action to collect activity logs performed on SentinelOne
Add Note to Threats from Rule	Run this action to add a note to threats from a rule
New Report Task	Run this action to add a new report task

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

To launch a SentinelOne response action for an alarm or event

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run SentinelOne Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Threat Hunting Library

The Threat Hunting Library is a tool that allows you to run predefined queries using the BlueApp for SentinelOne. The Hunting Library contains a list of queries you can select from and a list of endpoints you can click on to expand and see more information in relation to the queries. The Threat Hunting Library is only accessible to users receiving events from the configured BlueApp for SentinelOne.

To access the Threat Hunting Library, go to **Data Sources > Threat Hunting Library**.

Note: The ability to perform Queries with the BlueApp for SentinelOne is only available for customers with the SentinelOne Singularity Control license, the SentinelOne Singularity Complete license, or for customers who have AT&T Managed Endpoint Security with SentinelOne.

Creating SentinelOne Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a SentinelOne response action when events or alarms, match the criteria that you specify. This way, you can automate the way you filter IP addresses into the policies within the SentinelOne UI.

After you create a rule, new events or alarms that match the rule conditions will trigger the SentinelOne response action to create a new incident. The rule does *not* trigger for existing events or alarms.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the App**: Go to the BlueApp for SentinelOne page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new SentinelOne response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the SentinelOne incident.

   The SentinelOne parameters that you set will depend on which of the following actions you select:

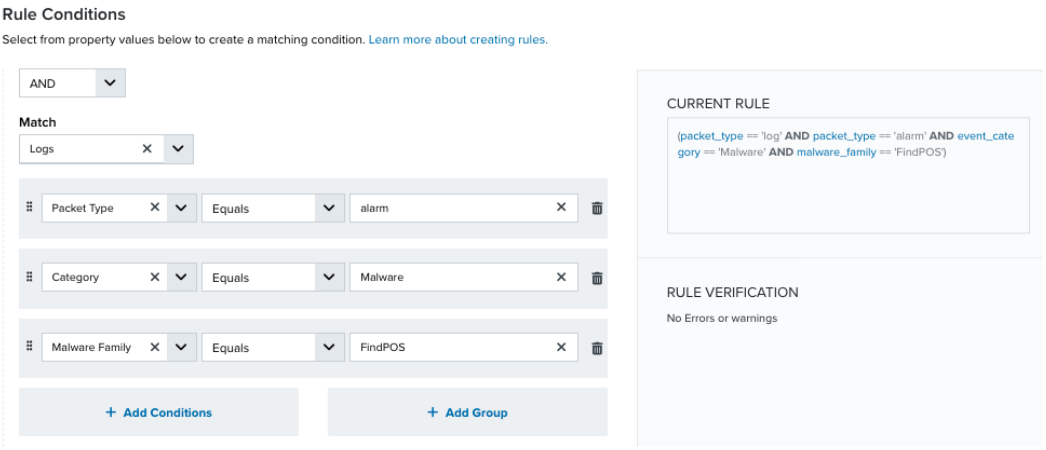
   - Create a New Incident from an Alarm

     This is the default action if you create the rule after applying a SentinelOne response action to an alarm. Use this action to run a new SentinelOne rule for the addresses of a new alarm that satisfies the matching criteria.

- Create a New Issue from Event-Based Orchestration

  Use this action to add information to the designated SentinelOne groups based on an incident for any event that satisfies the matching criteria.

3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- If you create the rule from an applied action, this section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for ServiceNow

Using the BlueApp for ServiceNow, you can streamline incident response activities by collecting data from ServiceNow and automatically opening ServiceNow incident tickets in response to threats detected by USM Anywhere.

The BlueApp for ServiceNow gathers data from the following ServiceNow tables. When you enable access to these tables, the BlueApp pulls *all* their records and creates events in USM Anywhere.

ServiceNow Tables Pulled by the BlueApp

Table Name	Description
pwd_reset_request	A table containing password reset requests
sysevent	A table containing events generated by the ServiceNow system
syslog_transaction	A table containing transaction logs
sys_audit	A table containing inserts and updates to audited records
sys_audit_delete	A table containing audit-deleted records
sys_user	A table containing all the user records
sys_user_role	A table containing all the user role records
sys_attachment	A table containing all the attachment records
report_view	A table containing report_view access control records

Edition: The BlueApp for ServiceNow is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for ServiceNow

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To enable the BlueApp for ServiceNow actions within USM Anywhere, you must configure the BlueApp by setting up the integration with your ServiceNow instance. After validation of the configuration, you can include an action as part of an orchestration rule triggered by an event, or launch the action from the details page for a specific alarm, event, or vulnerability. See BlueApp for ServiceNow Actions for more information about using this functionality.

BlueApp for ServiceNow Requirements

You or your ServiceNow administrator must create a user account in your ServiceNow instance to be used by USM Anywhere through the ServiceNow Representational State Transfer (REST) APIs. This user account must have rights to perform create, read, update, and delete (CRUD) operations using the ServiceNow Table API and ServiceNow Aggregate API. If you are using the ServiceNow Security Incident Response (SIR) application and want the BlueApp for ServiceNow to create new security incidents, this user must also have the *sn_si.integration_user* or *sn_si.admin* role.

If you choose to use OAuth, you must create an endpoint for BlueApp for ServiceNow to access your ServiceNow instance. See ServiceNow Product documentation for more details.

Note: It is a best practice to have a user account configured in your ServiceNow instance that can be used exclusively for USM Anywhere. With this exclusive user account, you can easily filter incidents in the ServiceNow user interface (UI) to display incident tickets created by USM Anywhere. Also, the incidents created by the BlueApp for ServiceNow and its history are displayed in USM Anywhere according to this username. By using an exclusive user account, this information will be confined to the USM Anywhere alarm, vulnerability, and event responses.

If you are a service provider or enterprise that manages more than one USM Anywhere instance, you can configure the BlueApp for ServiceNow on each instance to connect to the same ServiceNow environment. In this case, you should create a unique user account to be used by each USM Anywhere instance so that you can not only differentiate them in the ServiceNow UI, but also separate the history and incident information displayed in USM Anywhere by the instance.

Before you configure the BlueApp for ServiceNow, make sure you have these requirements in place:

- Fully-qualified domain name (FQDN) for your ServiceNow instance
- Username and password to use for USM Anywhere access
- (OAuth only) ServiceNow client identification (ID)
- (OAuth only) ServiceNow client secret

Configure the ServiceNow Connection in USM Anywhere

To support the ServiceNow response actions in USM Anywhere, you must configure a connection with the ServiceNow instance. This connection enables the BlueApp to perform CRUD operations using the ServiceNow Table and Aggregate REST APIs.

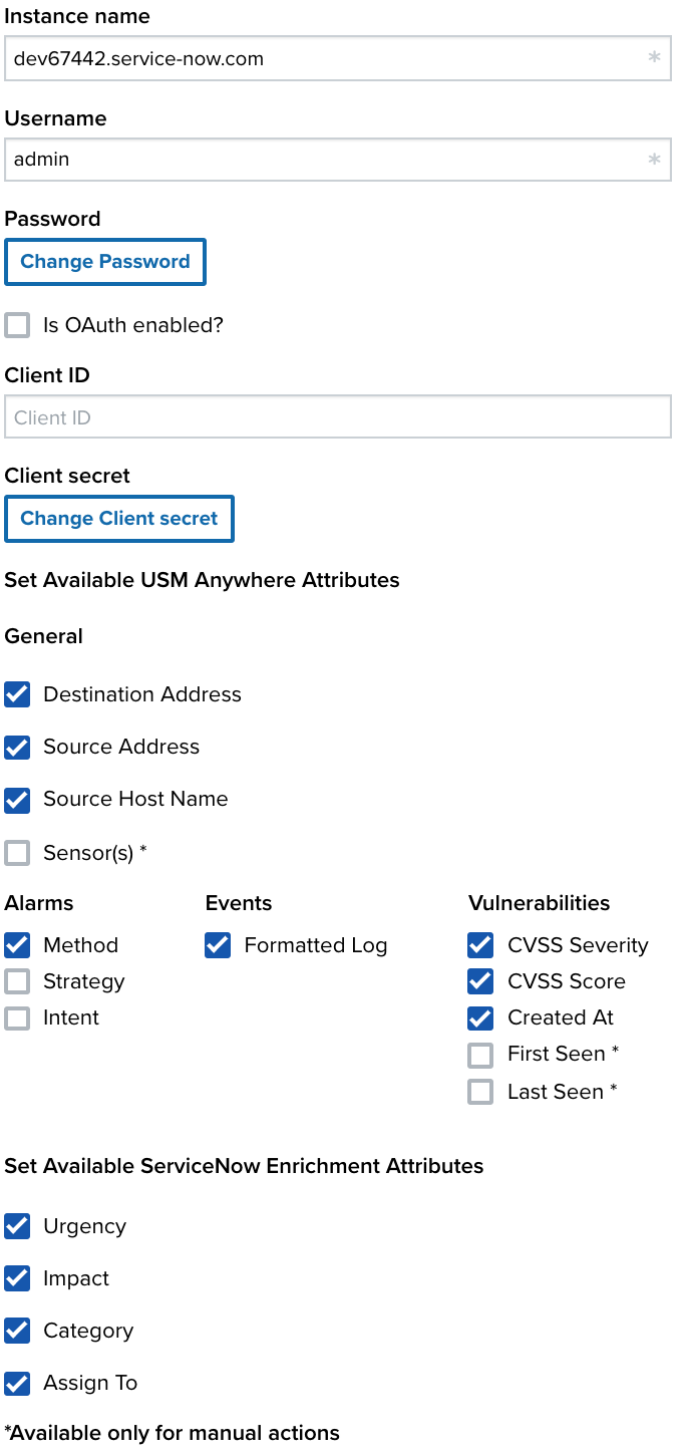
To configure the connection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Specify the basic connection information for ServiceNow:
   - **Instance name**: Enter the FQDN for your ServiceNow instance.

     For example, if you access your ServiceNow instance at https://mycorp.service-now.com, you must enter *mycorp.service-now.com* in this field.
   - **Username**: Enter the username for the account that USM Anywhere will use to access ServiceNow.
   - **Password**: Enter the password for the account.

7. (OAuth only.) Specify the OAuth authentication parameters:
   - **Is OAuth enabled?**: Select this checkbox to use OAuth for the ServiceNow connection.
   - **Client ID**: Enter the client ID that is configured in the ServiceNow *OAuth Application Registry*.
   - **Client secret**: Click **Change Client secret** to enter the client secret for the client ID.
8. In the Set Available USM Anywhere Attributes section, select the checkboxes for the options you want to make available for populating the Incident descriptions in ServiceNow when you create a response action rule.



9. Click **Save**.
10. Verify the connection.

After USM Anywhere completes a successful connection to the ServiceNow instance and the APIs, a icon displays in the Health column.

If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your ServiceNow connection.

ServiceNow Event Collection

Once the BlueApp for ServiceNow has been configured, you can choose to have BlueApp for ServiceNow collect events from the app.

To configure ServiceNow event collection

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the ServiceNow app on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive ServiceNow events job.

   The icon turns green and hourly event collection from ServiceNow is enabled.

Configure the BlueApp for ServiceNow to Map ServiceNow Data Fields to USM Anywhere Data Fields

Once the BlueApp for ServiceNow has been configured, you can choose to create templates to map your ServiceNow fields to their equivalent data fields in USM Anywhere.

Important: Without this configuration, all incident data is created in the description field of your ServiceNow incidents.

When users create incidents from USM Anywhere events or alarms, they will be able to select the appropriate template to ensure that the USMA fields and ServiceNow fields will accurately reflect the incident's information. See Creating ServiceNow Response Action Rules for more information on including these templates in your incidents.

To map incident data in the BlueApp for ServiceNow

1. Open your BlueApp for ServiceNow and navigate to the **Mapping Templates** tab.
2. Click the **Add Template** button.
3. Enter a name for your new template.

4. Use the drop-down rows to configure which USM Anywhere fields map to which ServiceNow fields.
   Add multiple rows to the same template with the **Add Row** button.
5. Click **Save** when you are done configuring your mapping template.

BlueApp for ServiceNow Actions

As USM Anywhere surfaces events, alarms, and vulnerabilities, your team determines which items require the opening of a new ServiceNow incident. Rather than manually opening each incident ticket in the ServiceNow user interface (UI), you can use the BlueApp for ServiceNow response actions to automatically create a ServiceNow ticket with the *Short description* and *Description* fields pre-populated with content from your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for BlueApp for ServiceNow

Action	Description
Create New Incident from Alarm	Run this action to generate a new ServiceNow incident for an alarm This action is available when you launch a response action directly for an existing alarm
Create New Incident from Vulnerability	Run this action to generate a new ServiceNow incident for a vulnerability This action is available only when you launch a response action directly for an existing vulnerability
Create New Incident from Event	Run this action to generate a new ServiceNow incident for an event This action is available only when you launch a response action directly for an existing event
Create New Incident from Orchestration Rule	Run this action to generate a new ServiceNow incident for future events that match your criteria This action is available only when you launch a response action in an orchestration rule

Actions for BlueApp for ServiceNow (Continued)

Action	Description
Create a change request	Run this action from an alarm or investigation to generate a change request in ServiceNow
Update Alarm Status	Run this action to update the status of an alarm
Pull Events	Run this action to pull events from ServiceNow

Upon execution of a response action, USM Anywhere generates the ServiceNow incident and passes the associated information to that new incident ticket.

Note: Before launching a ServiceNow response action or creating a ServiceNow response action rule, the BlueApp for ServiceNow must be enabled and connected to your ServiceNow instance. See Configuring the BlueApp for ServiceNow for more information.

To view information about these actions in USM Anywhere

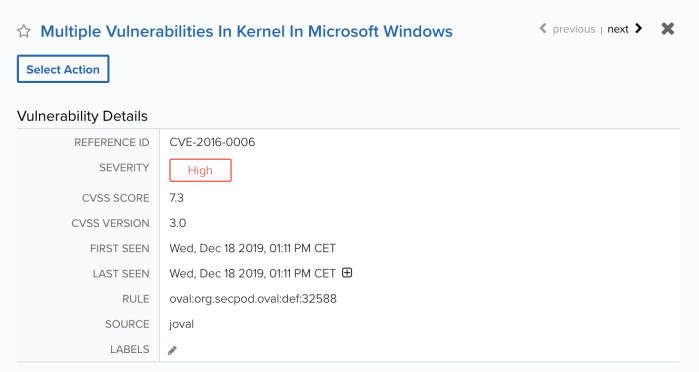
1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

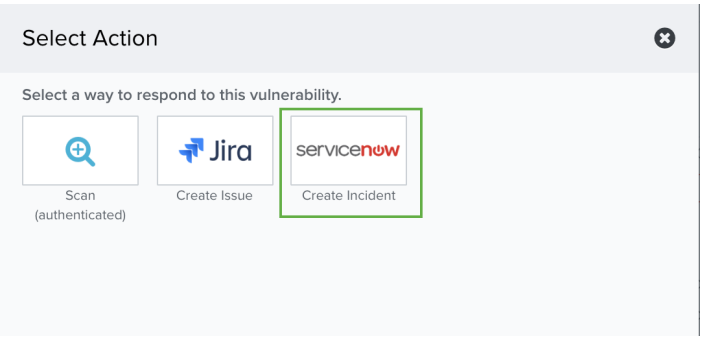
You can launch an action directly from alarms, events, or vulnerabilities. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm, event, or vulnerability.

To launch a ServiceNow response action for an alarm, event, or vulnerability

1. Go to **Activity > Alarms**, **Activity > Events**, or **Environment > Vulnerabilities**.
2. Click the alarm, event, or vulnerability to open the details.
3. Click **Select Action**.



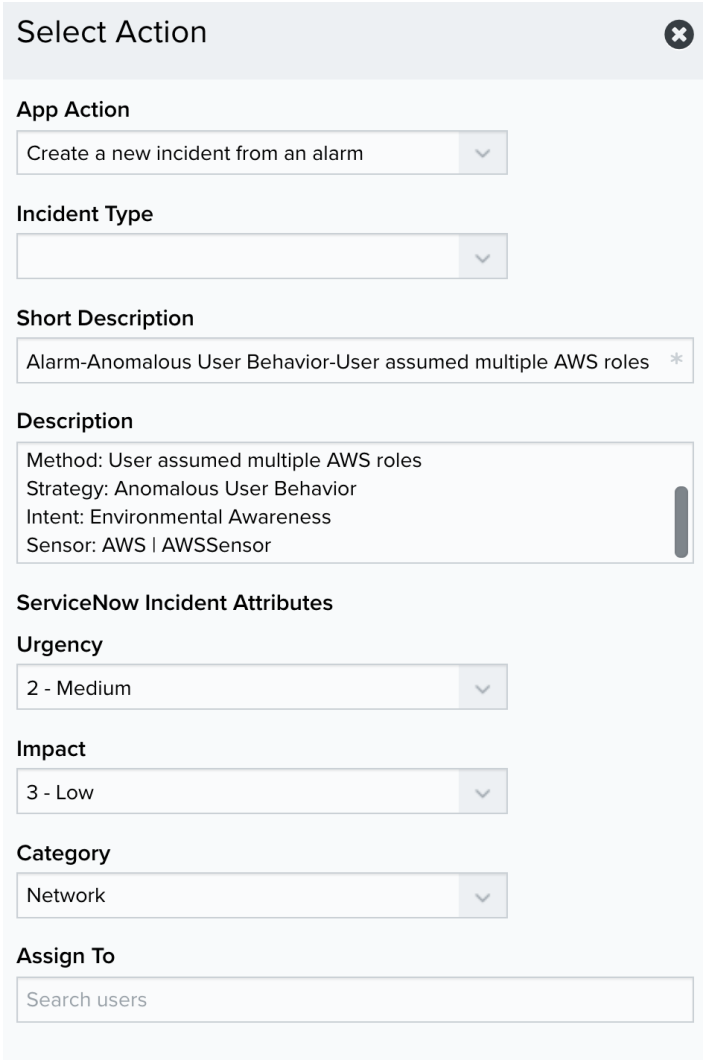
4. In the Select Action dialog box, select the **ServiceNow** tile.



   This displays the options for the selected response app. The App Action is set automatically according to the item type.

5. (Optional.) If you have more than one USM Anywhere Sensor configured for the BlueApp for ServiceNow, use the Select Sensor option to set the sensor that you want to use for the action.

6. Set **Service Desk** as the Incident Type.

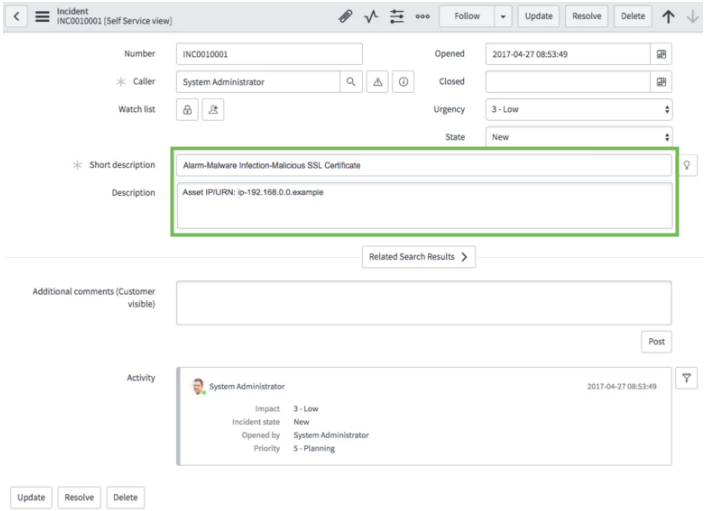


7. (Optional.) Modify the description information for the new incident.

   The BlueApp populates these fields automatically from information in the alarm, event, or vulnerability; however, you can add your own static text in these fields if needed:

   - **Short Description**: This field contains the subject for the new incident. By default, the BlueApp populates the name of the alarm, event, or vulnerability.
   - **Description:** This field contains information used to respond to the incident. By default, the BlueApp populates the information according to the item type and provides the source and destination. You might choose to include additional comments here, such as suggestions for the incident response handling.

Additionally, you can further define the ServiceNow incident parameters that are populated using the Urgency, Impact, and Category drop-down fields. You can use the Assign To field to automatically assign all resulting incidents to a specific user.



8. Click **Run**.

Creating ServiceNow Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a ServiceNow response action when events, alarms, or vulnerabilities match the criteria that you specify. For example, you might create a rule where USM Anywhere automatically creates a new ServiceNow incident when malware is detected so that a member of your response team can manage and address the issue.

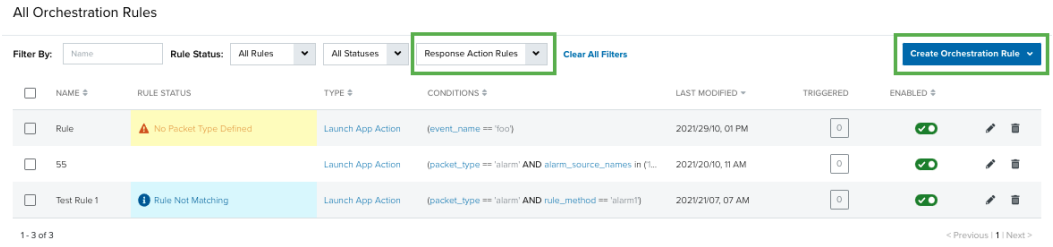
Note: Before creating a ServiceNow response action rule, the BlueApp for ServiceNow must be enabled and connected to your ServiceNow instance. See Configuring the BlueApp for ServiceNow for more information.

After you create a rule, new events, alarms, or vulnerabilities that match the rule conditions will trigger the ServiceNow response action to create a new incident. The rule does *not* trigger for existing events, alarms, or vulnerabilities.

You can create a new rule the following way:

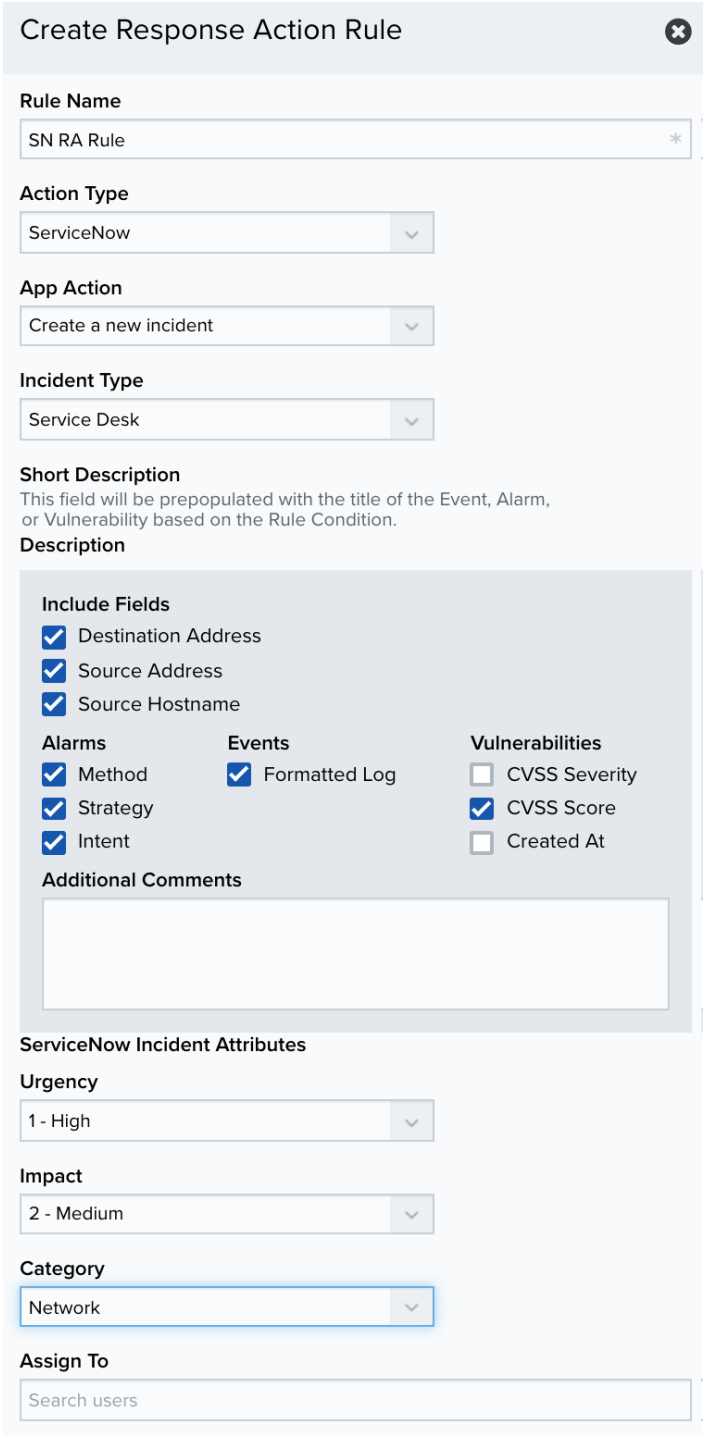
- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

  In the left navigation menu, go to **Settings > Rules > Orchestration Rules**. Then click **Create Orchestration Rule > Response Action Rule** to define the new rule.



To define a new ServiceNow response based on orchestration

1. Enter a name for the rule.
2. Select **ServiceNow** for Action Type and **Create a new incident** for App Action.
3. Set **Service Desk** as the Incident Type.


Create Response Action Rule
Rule Name
SN RA Rule
Action Type
ServiceNow
App Action
Create a new incident
Incident Type
Service Desk
Short Description
This field will be prepopulated with the title of the Event, Alarm, or Vulnerability based on the Rule Condition.
Description
Include Fields
Destination Address
Source Address
Source Hostname
Alarms
Method
Strategy
Intent
Events
Formatted Log
Vulnerabilities
CVSS Severity
CVSS Score
Created At
Additional Comments
ServiceNow Incident Attributes
Urgency
1 - High
Impact
2 - Medium
Category
Network
Assign To
Search users

USM Anywhere uses the title of the alarm, event, or vulnerability that triggers the rule to populate the short description of the incident.

For a description of the incident, you can decide which fields to use by selecting the checkboxes as follows:

- **Include Fields**: Select the checkboxes to include any of the information fields in your incident.
- **Alarms**: Select the checkboxes to include any of these fields from an Alarm in your incident.
- **Events**: Select the checkboxes to include any of these fields from an Event in your incident.
- **Vulnerabilities**: Select the checkboxes to include any of these fields from a Vulnerability in your incident.
- **Additional Comments**: Enter any additional information that you want to include in the notes field of the ServiceNow incident.

Note: The checkboxes are determined by those you selected on the **Data Sources > Integrations > ServiceNow > Settings** page when configuring the BlueApp.

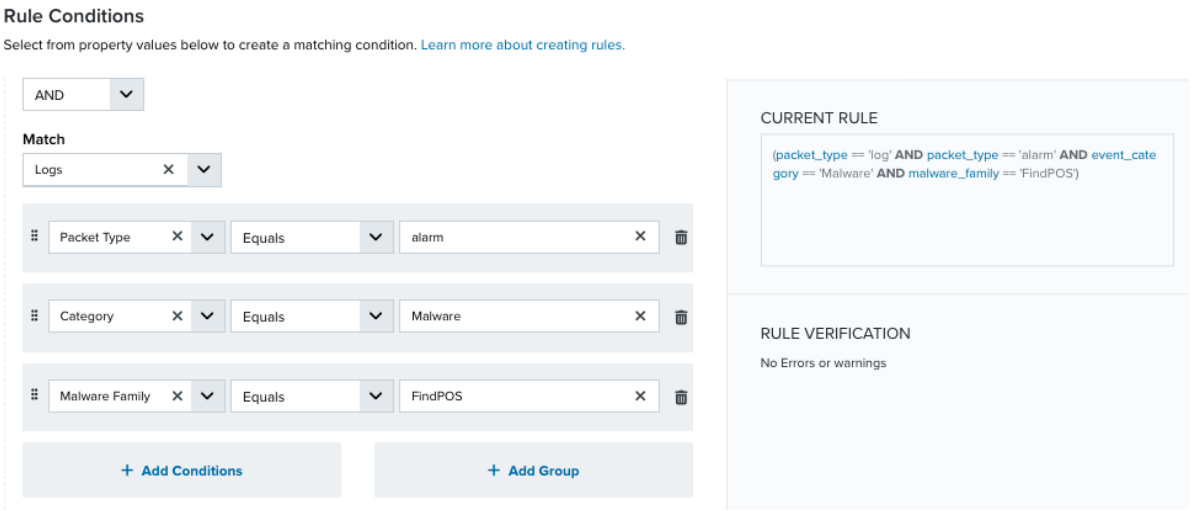
Additionally, you can further define the ServiceNow incident parameters that are populated by using the Urgency, Impact, and Category drop-down fields.

You can use the **Assign To** field to automatically assign all resulting incidents to a specific user. Use the drop-down list to select the correct user.

4. (Optional.) Set the appropriate mapping template using the **Template** dropdown.

Note: The templates available to you are determined by your app's configurations under Mapping Templates. See Configure ServiceNow Fields to Map to Equivalent USM Anywhere Fields for more information about using and configuring these templates.

5. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

6. Click **Save Rule**.
7. In the confirmation dialog box, click **OK**.

Managing Your ServiceNow Incidents

Role Availability ✔ Read-Only ✔ Investigator ✔ Analyst ✔ Manager

After the BlueApp for ServiceNow is configured and users execute the supported actions directly or through an orchestration rule, you can easily view a list of the ServiceNow incidents created by USM Anywhere and look at the events, alarms, and vulnerabilities related to the executed actions.

Viewing ServiceNow Incidents Created by USM Anywhere

In USM Anywhere, you can view a list of incidents created by an action applied directly to an alarm, event, or vulnerability, as well as any from actions that were triggered by an orchestration rule. From the list, you can open the incident in your ServiceNow account to view additional information about the incident or make updates to the incident, such as assigning the item to a team member or changing the priority.

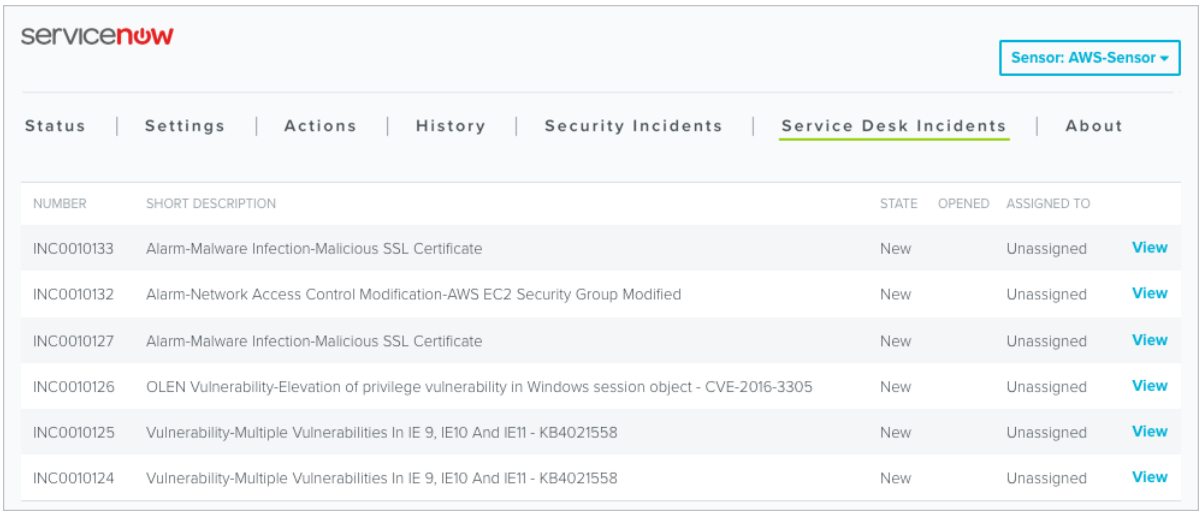
To access the ServiceNow incidents

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the tab for the incidents type that you want to display.

   The available incident types depend on the ServiceNow products that are active for the ServiceNow user account configured for the BlueApp.

   Select **Service Desk Incidents** to view incidents created in the IT Service Management product.

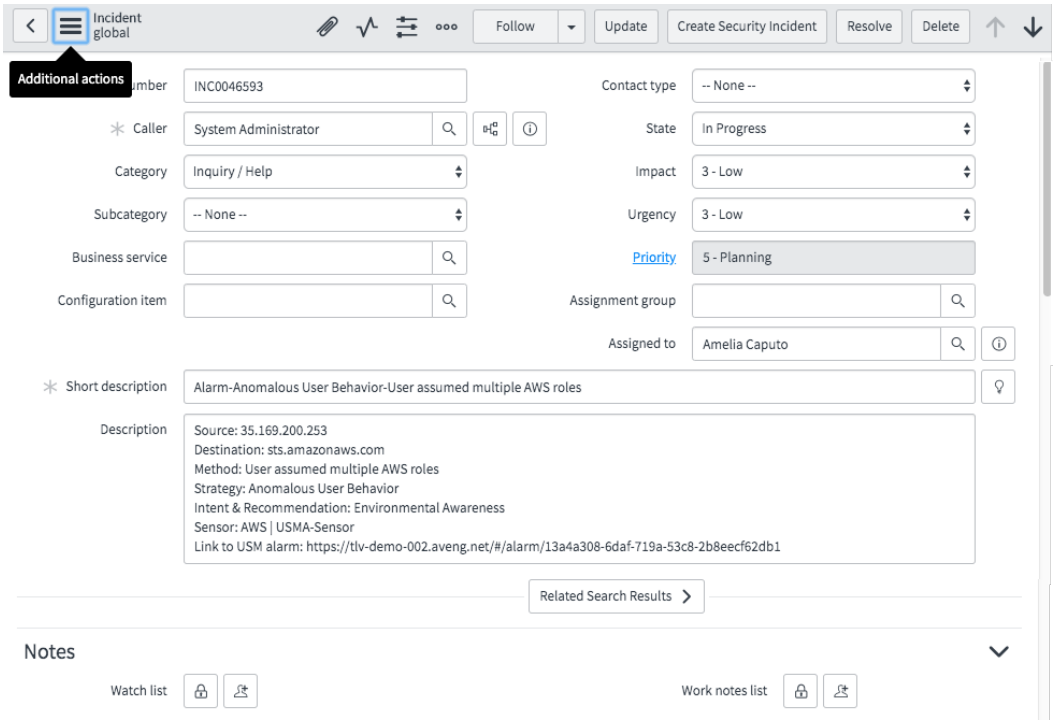
   If your account has the ServiceNow Security Incident Response (SIR) product enabled, click the **Security Incidents** tab to view the security incidents created in that product.



The displayed list includes all ServiceNow incidents generated by USM Anywhere, with the most recently opened items at the top. Here you can view the current status and assignment for the incident as reported by your ServiceNow instance.

5. Click **View** to open the incident in the ServiceNow user interface (UI).

   In ServiceNow, you can assign the issue, change its status, access the source of the incident in USM Anywhere from the link included in the ServiceNow incident, or perform any of the functions supported for your account.



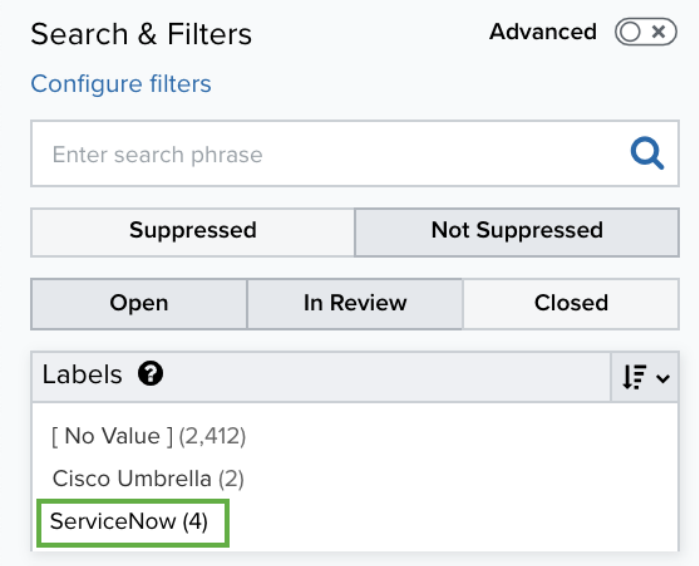
Filtering the Labeled Alarms and Vulnerabilities

USM Anywhere uses labels as a mechanism to classify alarms and vulnerabilities. These labels make it easy to filter items by label so that you can locate them easily and track their status. When the BlueApp for ServiceNow executes a response action for an alarm or vulnerability, it automatically applies the ServiceNow label to it. You can use this label as a filter so that a page displays data for only those items related to an BlueApp for ServiceNow response action.

To view ServiceNow action alarms or vulnerabilities

1. Open the Alarms page or Vulnerabilities page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

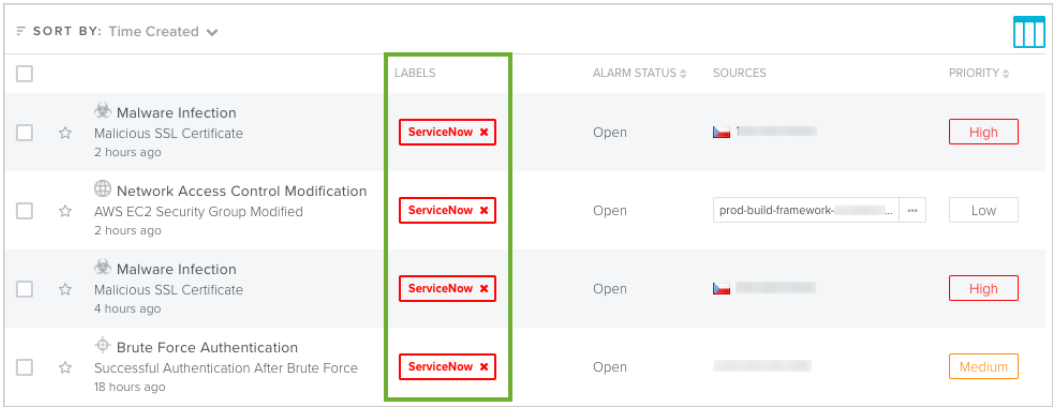
   USM Anywhere includes several filters displayed by default.
3. Locate the Labels filter and select **ServiceNow**.



If the Labels filter is not displayed, click **Configure Filters** at the bottom of the Search & Filters pane to configure filters for the page. See Managing Filters in the *USM Anywhere*

User Guide for more information about configuring filters for the page display.

In the displayed list, you can scroll the list to the right and view the Labels column.



BlueApp for Sophos Central

The BlueApp for Sophos Central enhances the threat detection capabilities of USM Anywhere by collecting and analyzing event and alert data from Sophos Central, which enables management of multiple products within its Synchronized Security platform.

Sophos Central unifies security data from across the Sophos suite of products for server security, endpoint protection, email security, and more. The BlueApp for Sophos Central collects data through the Sophos Central API and parses it to generate normalized events, making it available for threat analysis and incident response within USM Anywhere.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Sophos Central

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

With a configured connection between the BlueApp for Sophos Central on a deployed USM Anywhere Sensor and your Sophos Central environment, the predefined log collection jobs perform scheduled API queries for Sophos events or alerts. When USM Anywhere collects and analyzes the first of these, the normalized events are available on the Events page.

Configuration for the Sophos Central Connection

To enable BlueApp for Sophos Central functionality within USM Anywhere, you must configure the BlueApp by providing a valid Sophos Central API client ID and client secret. With a successful connection to your Sophos Central environment, the BlueApp for Sophos Central log collection jobs query the API every 20 minutes for events, alerts, or both. It parses all collected data and displays it as events and alarms in USM Anywhere.

Note: The Computer Isolation feature is only available for customers with a Sophos Intercept X Advanced with XDR license. See Sophos Central: Computer Isolation for more information.

Generate the Client ID and Client Secret

As a Sophos Central administrator, you must create the API client ID and secret to be used by the BlueApp for the connection to your Sophos Central data through the Sophos Central APIs. These API credentials are valid for one year. To maintain the USM Anywhere connection, you will need to renew these API credentials to extend their validity.

To generate API credentials for Sophos Central

1. Log in to your Sophos Central environment and navigate to **Global Settings > API Credentials Management**.
2. Click **Add Credentials**.
3. Enter the required information to configure new credentials.
   - **Credential Name**: Enter an identifiable credential name.
   - (Optional.) **Description**: Enter a description of the credentials you are generating.
   - **Role**: Use this dropdown to select the appropriate role for these credentials.
4. Click **Add** to generate your credentials.
   You will be shown your newly generated client ID.
5. Click **show Client Secret** to view your client secret.

Warning: For security reasons, you will only be able to view your client secret one time. When you click show Client Secret, you must save the client secret for future use or you will have to generate new credentials.

Configure the BlueApp for Sophos Central Connection

After you create the client ID and client secret in Sophos Central, you can configure the connection within USM Anywhere.

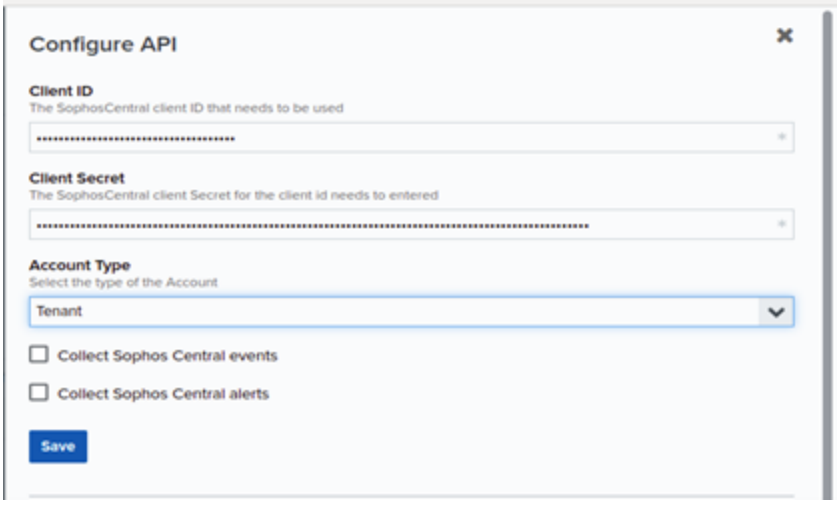
To enable the BlueApp for Sophos Central connection

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

   Enter the client ID and client secret you generated from your Sophos Central environment.

   Use the drop-down to select the appropriate account type.

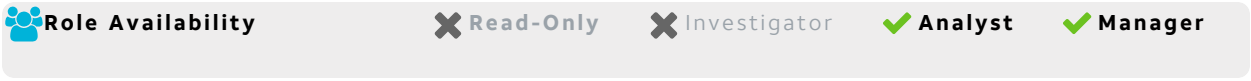
6. 

7. Select **Collect Sophos Central events** or **Collect Sophos Central alerts** to limit the data collection from your Sophos Central environment.
8. Click **Save**.
9. Verify the connection.

   After USM Anywhere completes a successful connection to the Sophos Central APIs, a  icon displays in the Health column.

   If the  icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Sophos Central connection.

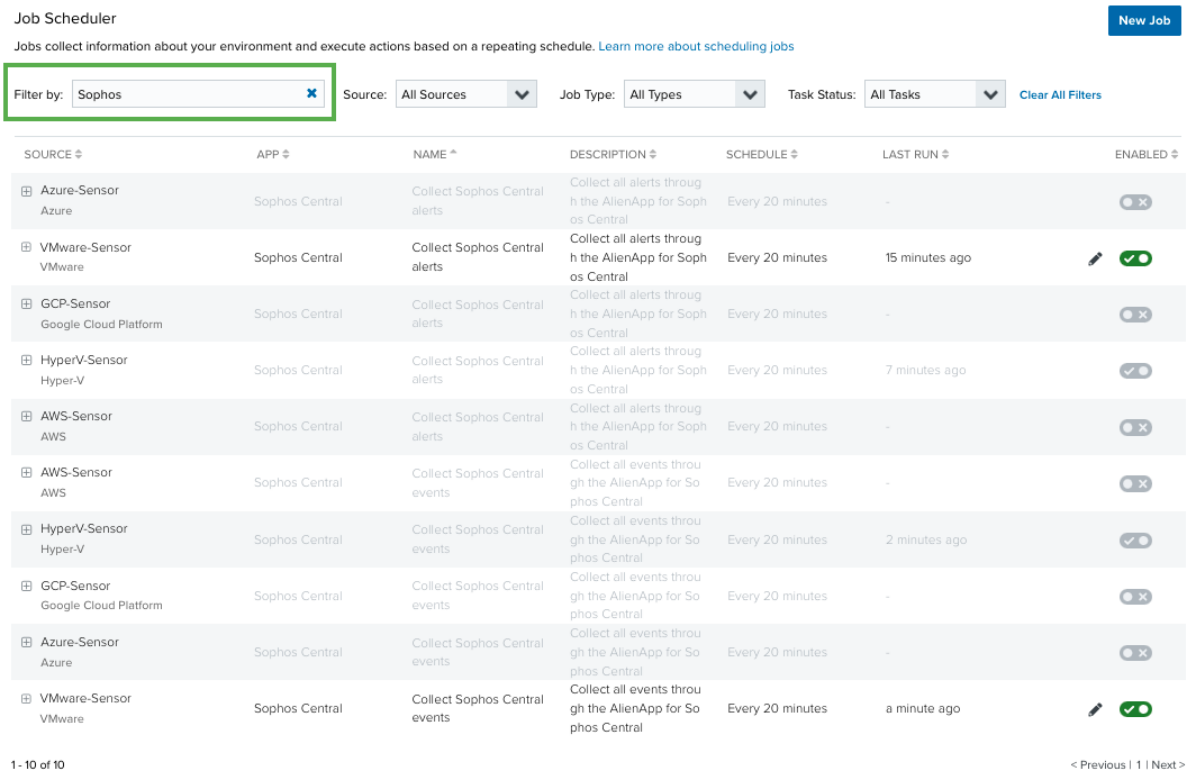
Verifying the BlueApp for Sophos Central Collection Jobs



After you configure the BlueApp for Sophos Central and have a successful connection, you should verify that the scheduled collection jobs are enabled. For each deployed sensor, USM Anywhere includes two out-of-the-box log jobs to support BlueApp for Sophos Central data collection. You can view these jobs in the Job Scheduler page and make sure that these jobs are enabled for the sensor where you configured the BlueApp for Sophos Central.

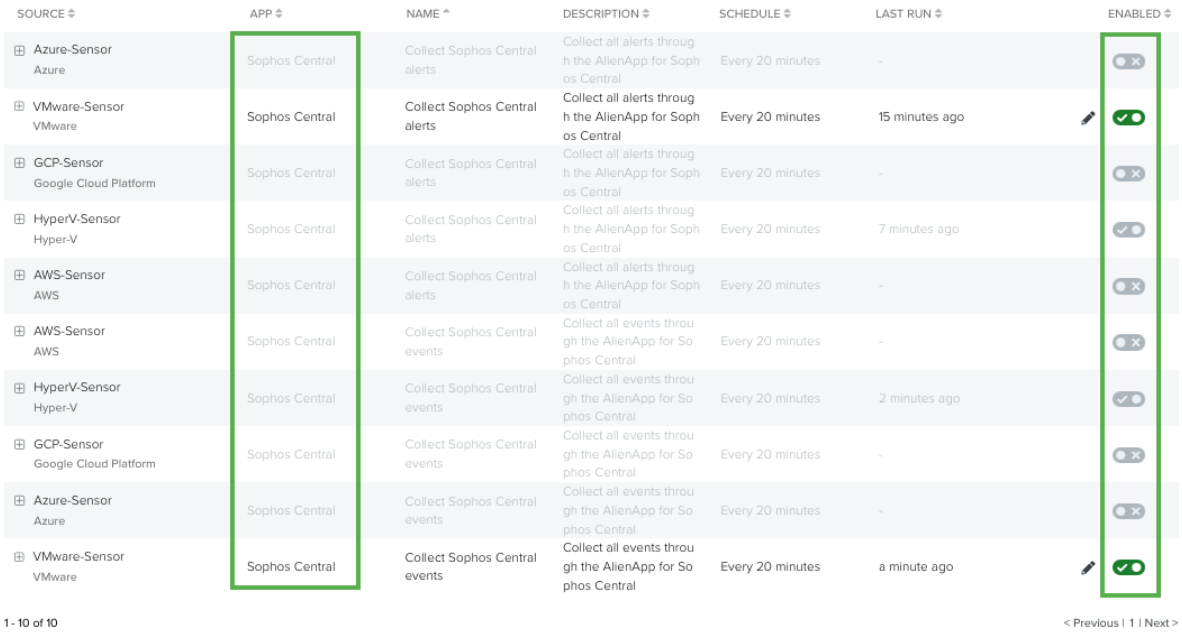
To verify the Sophos Central collection jobs

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the Filter by option at the top of the list, enter **Sophos** to filter the displayed list for the Sophos Central app jobs.



3. Locate the jobs you want to verify for the collection of alerts, events, or both:
   - Collect Sophos Central alerts
   - Collect Sophos Central events

If you have enabled both data collection options in the BlueApp for Sophos Central configuration, you should verify both collection jobs for the sensor. If only one of these options is configured, you can verify the one that matches the selected option.



SOURCE	APP	NAME	DESCRIPTION	SCHEDULE	LAST RUN	ENABLED
Azure-Sensor Azure	Sophos Central	Collect Sophos Central alerts	Collect all alerts through the AlienApp for Sophos Central	Every 20 minutes	-	
VMware-Sensor VMware	Sophos Central	Collect Sophos Central alerts	Collect all alerts through the AlienApp for Sophos Central	Every 20 minutes	15 minutes ago	
GCP-Sensor Google Cloud Platform	Sophos Central	Collect Sophos Central alerts	Collect all alerts through the AlienApp for Sophos Central	Every 20 minutes	-	
HyperV-Sensor Hyper-V	Sophos Central	Collect Sophos Central alerts	Collect all alerts through the AlienApp for Sophos Central	Every 20 minutes	7 minutes ago	
AWS-Sensor AWS	Sophos Central	Collect Sophos Central alerts	Collect all alerts through the AlienApp for Sophos Central	Every 20 minutes	-	
AWS-Sensor AWS	Sophos Central	Collect Sophos Central events	Collect all events through the AlienApp for Sophos Central	Every 20 minutes	-	
HyperV-Sensor Hyper-V	Sophos Central	Collect Sophos Central events	Collect all events through the AlienApp for Sophos Central	Every 20 minutes	2 minutes ago	
GCP-Sensor Google Cloud Platform	Sophos Central	Collect Sophos Central events	Collect all events through the AlienApp for Sophos Central	Every 20 minutes	-	
Azure-Sensor Azure	Sophos Central	Collect Sophos Central events	Collect all events through the AlienApp for Sophos Central	Every 20 minutes	-	
VMware-Sensor VMware	Sophos Central	Collect Sophos Central events	Collect all events through the AlienApp for Sophos Central	Every 20 minutes	a minute ago	

1 - 10 of 10 < Previous | 1 | Next >

Jobs that are currently enabled display the icon.

4. If one or both jobs for the sensor are not enabled, click the icon to toggle it.

Viewing Your Sophos Central Events and Alarms

Role Availability ✔ **Read-Only** ✔ **Investigator** ✔ **Analyst** ✔ **Manager**

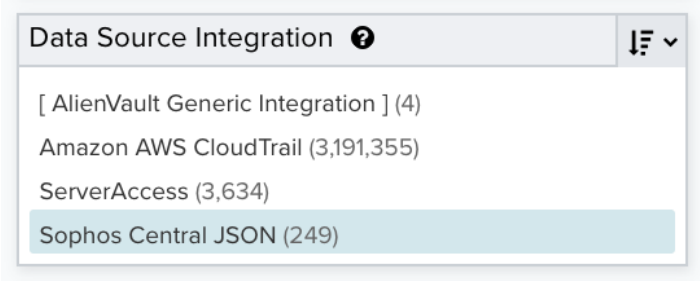
BlueApp for Sophos Central translates the Sophos event and alert data collected through the USM Anywhere Sensor into normalized events for analysis. These normalized events are accessible from the Events page.

Note: A correlation rule automatically identifies Sophos Central alerts where there is a threat detected for malware on an endpoint, and it generates a USM Anywhere alarm. If you want to generate an alarm for other types of Sophos Central events or alerts, you can create your own custom alarm rules and define the matching conditions to fit your criteria.

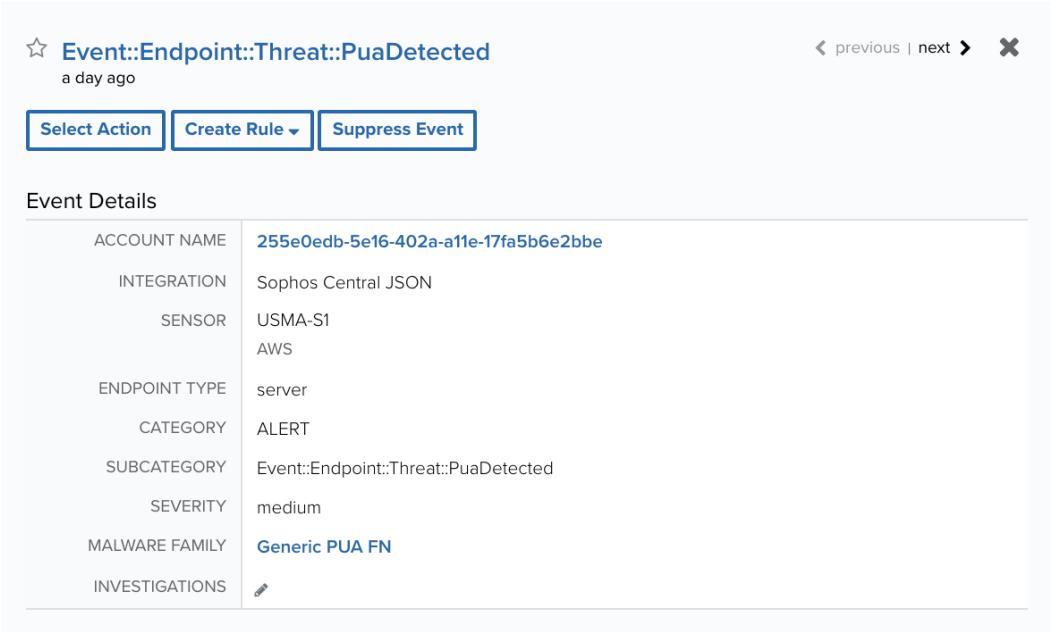
To view Sophos Central events

1. Select **Activity > Events** to open the events page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

   USM Anywhere includes several filters displayed by default.
3. Scroll down to the Data Source filter and select **Sophos Central JSON** to display only those events on the page.



   If this filter is not displayed, click the **Configure filters** link, which is in the upper left corner of the page, to configure filters for the page. See Managing Filters in the *USM Anywhere User Guide* for more information about configuring filters for pages.
4. Select an event in the list to view detailed information.



BlueApp for Sophos Central Actions

The BlueApp for Sophos Central provides a set of orchestration actions that you can use to integrate your BlueApp for Sophos Central in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Office 365

Action	Description
Lift Isolation of Endpoint	Run this action to lift the isolation of an endpoint from alarms, events, and investigations
Initiate Scans	Run this action to initiate scans from alarms, events, and investigations
Isolation of Endpoint	Run this action to isolate an endpoint from alarms, events, and investigations
Turn On Tamper-Protection for Endpoint	Run this action to turn on tamper protection for an endpoint from alarms, events, and investigations
Update Checks	Run this action to update checks from alarms, events, and investigations
Turn Off Tamper-Protection for Endpoint	Run this action to turn off tamper protection for an endpoint from alarms, events, and investigations

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Alarms, Events, or Investigations

You can launch an action directly from alarms, events, or investigations. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm, event, or investigation.

To launch a BlueApp for Sophos Central response action for an alarm, event, or investigation

1. Go to **Activity > Alarms**, **Activity > Events**, or **Investigations**.
2. Click the alarm, event, or investigation to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select **Run BlueApp for Sophos Central Action**.
5. Select the app action and fill out the fields that are populated below.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm, event, or investigation it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar investigations**, **Create rule for similar alarms**, or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Sophos Central Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Sophos Central response action when alarms, events, and investigations match the criteria that you specify. After you create a rule, new vulnerabilities that match the rule conditions trigger the Sophos Central response action to create a new incident. The rule does *not* trigger for existing alarms, events, or investigations.

You can create a new rule as follows:

- **From the Rules page:** The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

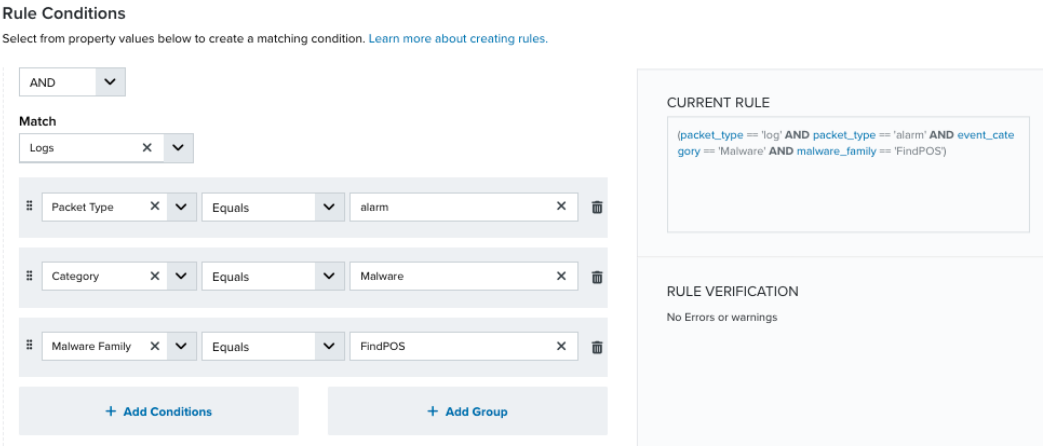
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel.

Then click **Create Response Action Rule** to define the new rule.

- **From the app:** Go to the BlueApp for Sophos Central page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new BlueApp for Sophos Central response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the BlueApp for Sophos Central incident.
3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for SpyCloud Dark Web Monitoring

The BlueApp for SpyCloud Dark Web Monitoring enables you to detect if your users' credentials have been compromised in a third-party breach and trafficked on the dark web, so that you can take immediate action to prevent another breach. LevelBlue provides this functionality on a limited-time trial basis at no additional cost through a partnership with SpyCloud, a pioneer in breach discovery. At the conclusion of the trial, customers may purchase this functionality from SpyCloud to continue using it. SpyCloud uses human and machine intelligence to monitor public, private, and covert sources on the dark web, identifying user credentials that have been stolen. This data is collected within USM Anywhere through the BlueApp for SpyCloud Dark Web Monitoring.

Edition: The BlueApp for SpyCloud Dark Web Monitoring is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for SpyCloud Dark Web Monitoring

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To enable BlueApp for SpyCloud Dark Web Monitoring functionality within USM Anywhere, you must configure the BlueApp by setting up your watchlist or connecting your SpyCloud-managed watchlist. After this configuration is complete, the BlueApp for SpyCloud Dark Web Monitoring queries the SpyCloud API every 24 hours for information regarding all watchlist items. Then it parses all collected data and displays it as events and alarms in the USM Anywhere interface.

Required Connectivity on the USM Anywhere Sensor

An BlueApp operates through a deployed USM Anywhere Sensor. To use the BlueApp for SpyCloud Dark Web Monitoring, you must open the following ports on the sensor to support these functions.

Port	Endpoint(s)	Function
UDP, TCP port 53	8.8.8.8, 209.244.0.3, 64.6.64.6	Domain Name System (DNS) lookup to verify the domain
80, 443	Domain configured in the watchlist	Validate the verification marker of the domain
443	api.spycloud.io	Check the SpyCloud breach database

Configuration for SpyCloud Dark Web Monitoring

The BlueApp for SpyCloud Dark Web Monitoring supports two configuration types that USM Anywhere can use to query the SpyCloud database:

- **Domain and email watchlist** defined for the BlueApp in USM Anywhere.

  This type of watchlist is limited to 1 domain and up to 10 email addresses. You do not need a SpyCloud account to use this feature. To monitor additional domains and emails through the LevelBlue partnership with SpyCloud, complete the form on this page: https://cybersecurity.att.com/app/spycloud/signup.

- **A valid SpyCloud customer API key** used to retrieve breach data from a watchlist managed in SpyCloud.

  When using the SpyCloud API key method, you do not need to manually add domain or email addresses in USM Anywhere. The BlueApp for SpyCloud Dark Web Monitoring retrieves all domains and email addresses from your existing SpyCloud watchlists.

You can use one of these configuration types to query the SpyCloud database and collect data for breach events for your users' credentials using a default collection job.

Define Your Watchlist in USM Anywhere

USM Anywhere supports a watchlist that includes 1 domain, a list of up to 10 email addresses, or both. When combining these watchlist item types, for example, you could add your company domain as well as a list of email addresses to expand the scope of monitoring to include personal accounts of top executives or other high-risk employees.

Note: USM Anywhere enforces this limitation across all of your deployed USM Anywhere Sensors. If you enable the BlueApp for SpyCloud Dark Web Monitoring on more than one sensor, the USM Anywhere user interface (UI) does not allow you to create new watchlist items if you have already reached the maximum across all sensors. If you add an email watchlist item that is already configured on another sensor, USM Anywhere removes the item from the other configuration to avoid duplication.

Monitoring a domain or email address using a watchlist managed by USM Anywhere requires verification:

- **Monitored domain**: You can verify ownership by adding an automatically generated verification key to either the DNS record or a page on the domain website.

  Important: If you want to monitor a private domain, it must have DNS set (forward and reverse). Otherwise, USM Anywhere cannot locate the domain and validate the key.

- **Monitored email address**: The address owner must click a link in a verification email sent by USM Anywhere.

When the SpyCloud collection job runs after validation of a new domain or email address, it collects all records related to the item from that point forward. Then USM Anywhere creates an event for each record and generates alarms for each breach event. If you want to generate events and alarms for all known records, you can use the BlueApp for SpyCloud Dark Web Monitoring app action to collect historical breach events.

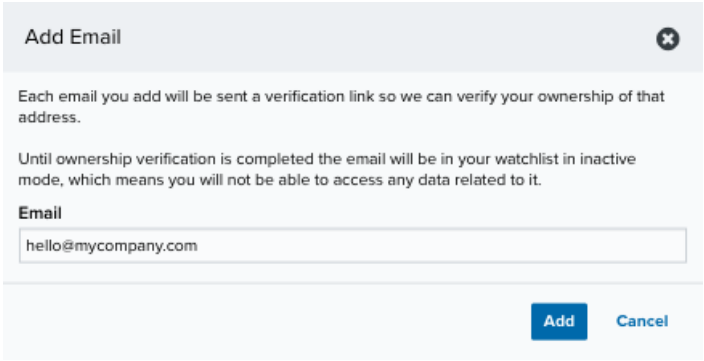
To configure a watchlist for the BlueApp for SpyCloud Dark Web Monitoring

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. If you want to monitor a list of email addresses, click the **Email Watchlist** tab.

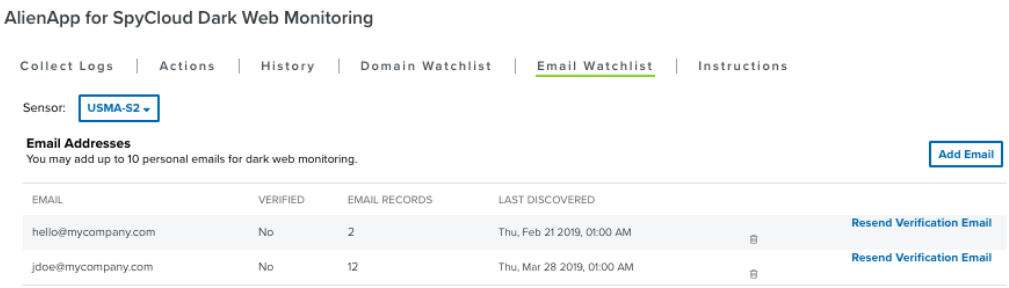
The email watchlist supports up to 10 email addresses.

a. For each address that you want to add, click **Add Email**.

b. In the Add Email dialog box, enter the email address and click **Add**.



The email watchlist includes the new email address and the Verified status = No. USM Anywhere automatically sends a message to the email address to verify it. Upon verification, the BlueApp for SpyCloud Dark Web Monitoring includes the address in its event data queries.



c. If an email address remains unverified, click **Resend Verification Email** to send the message again.

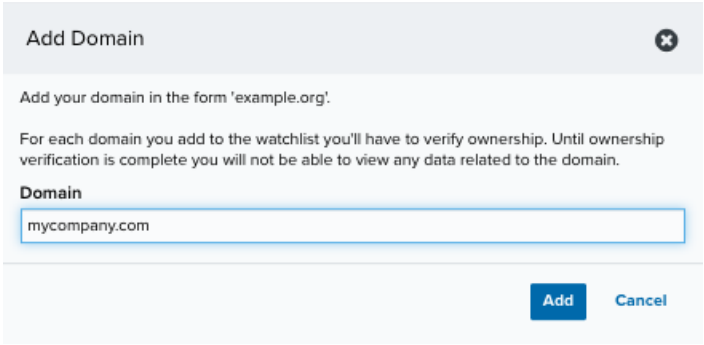
Note: The Add Email function is disabled when you enter a SpyCloud API key. The BlueApp for SpyCloud Dark Web Monitoring automatically retrieves the list of email addresses from your existing SpyCloud watchlists.

5. If you want to monitor a domain, click the **Domain Watchlist** tab.

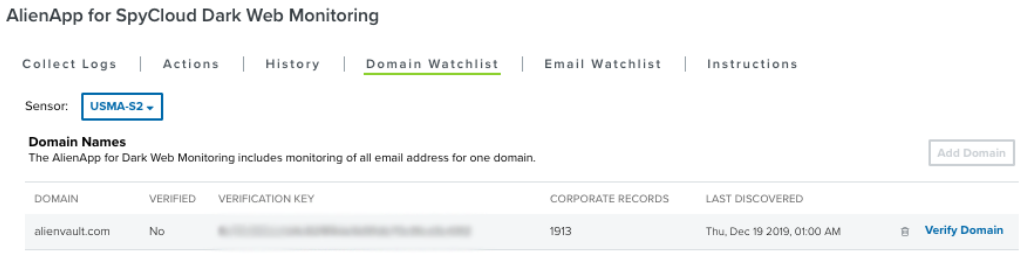
The domain watchlist supports one domain.

a. Click **Add Domain**.

b. In the Add Domain dialog box, enter the domain and click **Add**.

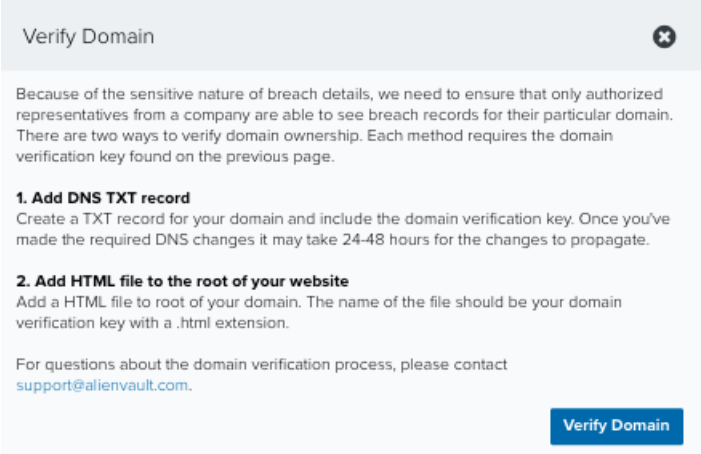


This adds the domain to the watchlist, but it is not yet verified. Upon verification, the BlueApp for SpyCloud Dark Web Monitoring includes the domain in its event data queries.



c. Copy the value of the Verification Key and click **Verify Domain**.

The Verify Domain dialog box provides instructions for adding the verification key to your domain.



d. When you have the information that you need, click **Verify Domain** to close the dialog box.

   This also executes a successful verification check if you have already completed the configuration, and an automated job that checks every six hours to verify the domain.

> **Note:** The monitored domain will be listed as Pending in the UI until the domain is verified. Once the domain has been verified and data collection is running, the domain status will be updated.
> After the domain has been verified but before any data has been collected, the domain status will be listed as No Records.

> **Note:** The Add Domain function is disabled when you enter a SpyCloud API key. The BlueApp for SpyCloud Dark Web Monitoring automatically retrieves the list of domains from your existing SpyCloud watchlists.

Use a Watchlist Managed in a SpyCloud Account

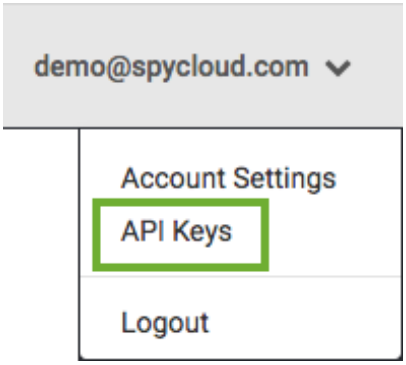
If your organization has a SpyCloud account and manages a watchlist in the SpyCloud portal, you can configure a connection in the BlueApp for SpyCloud Dark Web Monitoring so that USM Anywhere can retrieve the associated breach events. This provides a single view of security events and alarms in the USM Anywhere UI.

With a successful connection, the SpyCloud collection job includes all domains and email addresses in your SpyCloud watchlist to collect all records related to the item from that point forward. In addition, USM Anywhere creates an event for each record and generates alarms for each breach event. If you want to generate events and alarms for all known records, you can use the BlueApp for SpyCloud Dark Web Monitoring app action to collect historical breach events.

Important: If you previously enabled the BlueApp for SpyCloud Dark Web Monitoring using USM Anywhere-managed watchlist items and then you configure a connection to your SpyCloud account, USM Anywhere removes those watchlist items from its SpyCloud collection job. The collection job then only includes those items for your SpyCloud-managed watchlist.

To acquire your API key for SpyCloud

1. Go to the SpyCloud portal and log in to your account.
2. In the upper-right corner, click your username and select **API Keys**.

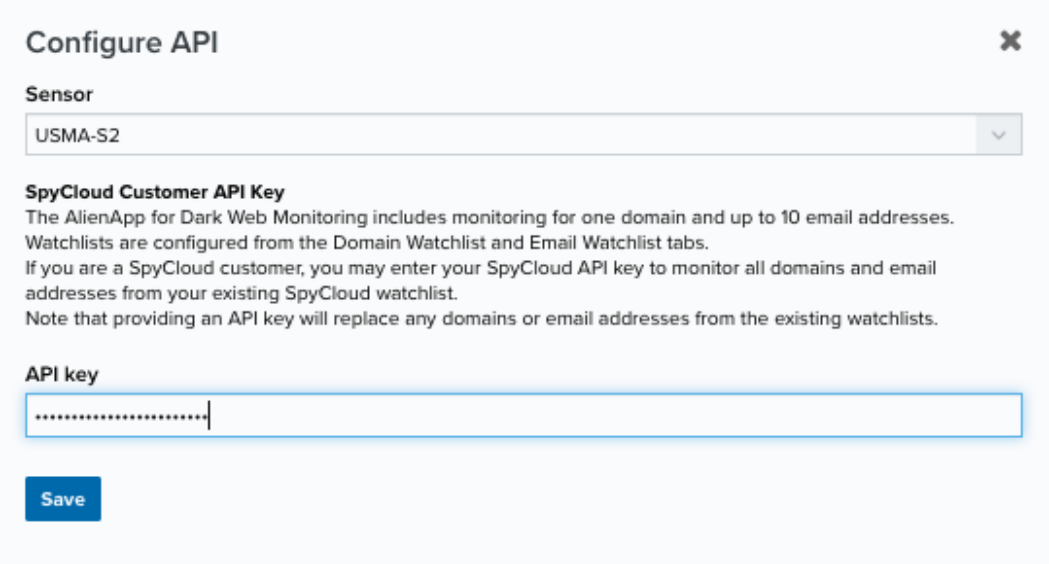


3. Copy the value for an existing key, or generate a new key for your USM Anywhere integration.

To connect the BlueApp for SpyCloud Dark Web Monitoring to your SpyCloud account

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.
6. Click **Change API key**.
7. Enter your key in the field.



8. Click **Save**.

> **Note:** By entering the API key, you allow the BlueApp for SpyCloud Dark Web Monitoring to retrieve all domains and email addresses from your existing SpyCloud watchlists. If you have manually added domain or email addresses to the BlueApp, they are removed. You will not be able to manually add domain or email addresses.

9. Verify the connection.

   After USM Anywhere completes a successful connection to the SpyCloud APIs, a icon displays in the Health column.

   If the icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your SpyCloud connection.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the icon for the inactive collection job.

   The icon turns green, and collection is enabled.
4. (Optional.) Click the icon to customize the frequency of the event collection.

Collecting Your Historical Breach Events

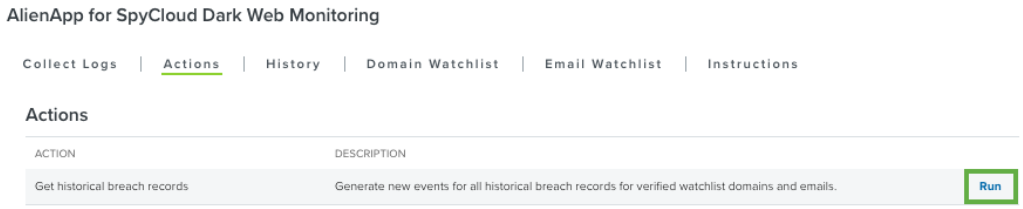
Role Availability | Read-Only | Investigator | **Analyst** | **Manager**

Upon configuration of the BlueApp for SpyCloud Dark Web Monitoring, the SpyCloud Dark Web Monitoring scheduler job collects new records every 24 hours for all validated watchlist items. The BlueApp for SpyCloud Dark Web Monitoring also supports a manual action that you can use to collect all historical records for your watchlist items.

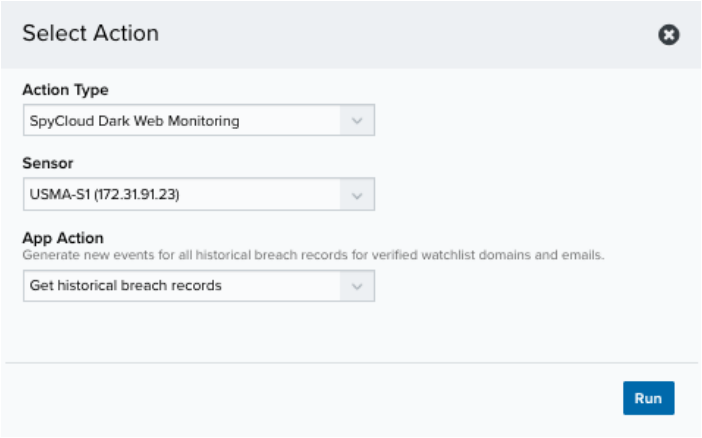
Important: If you run this action after the automated collection job has already collected SpyCloud database records or if you have run this action before, it will result in duplicate events and alarms within USM Anywhere.

To collect the historical breach records

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab.
5. Click **Run** to execute the action.



6. Verify the selected action type and action, and then click **Run**.



7. A record of this action displayed on the History tab. You can view these events under Activity > Events.

SpyCloud Dark Web Monitoring Events and Alarms

Role Availability ✔ **Read-Only** ✔ **Investigator** ✔ **Analyst** ✔ **Manager**

The BlueApp for SpyCloud Dark Web Monitoring monitors reports that breach records of compromised emails from that domain or assetsassociated with it. You can use this information to identify employees and consumers that have malware infections and protect yourself from potential fraud.

Malware often captures user credential information, such as usernames and passwords, along with other information and stores the stolen information on command and control (C2) servers. In cases where SpyCloud has recovered C2 data, it will analyze the records and classify them as either infected employee records or infected customer records.

For example, if one of the monitored domains is "example.com," then emails addressed from "[name]@example.com" that indicate a breach would be classified as an "employee" record. If the malware came from an unmonitored external domain, it is then classified as a "customer" record.

See the guide on infected users for more information.

The following table lists the fields available for SpyCloud events.

Examples of SpyCloud Events

Field	Description
Source DNS Domain	Domain name associated with the breach record.
Event Ref Date	The date on which the record entered the SpyCloud systems, in ISO 8601 date-time format.
Source Username	Username associated with the breach record.
Source User Email	The email address associated with the breach record.
Public Breach	A true/false flag that indicates if the breach has been disclosed to the public.
Infected User	A true/false flag that indicates if the credentials were obtained by a keylogger.
Source ID	SpyCloud-generated numerical identifier for the breach in which the credentials were found.
Password Type	The password type identified in the breach record.
IP Addresses	List of one or more IP addresses in alphanumeric format (both IPV4 and IPv6 addresses are supported).
Sighting	(SpyCloud subscriptions only) An integer that indicates the occurrence of a breached credential across the entire SpyCloud breach catalog A value of “3” would indicate that this breach record is the third occurrence of the credential in the catalog.

Note: The BlueApp for SpyCloud Dark Web Monitoring leverages the SpyCloud APIs to retrieve breach records. See the SpyCloud API documentation for more information about the attributes (data fields) it stores in these breach records.

USM Anywhere generates an alarm from one or more of these events using built-in correlation rules, which analyze the events for patterns that indicate a new breach that requires attention and investigation. It generates the alarm as a Security Critical Event with the following assessed breach method:

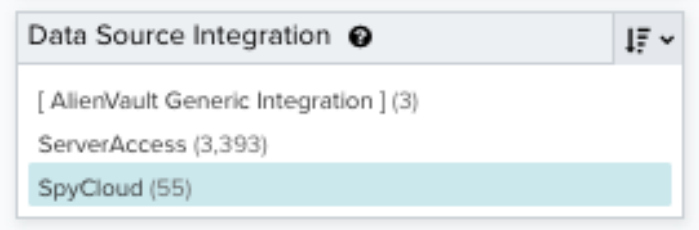
- Credentials Stolen — Public Breach
- Credentials Stolen — Private Breach
- Credentials Stolen — Infected User

Additional parameters of a generated alarm are determined by the information in the associated events. For example, an alarm will provide different guidance if an event indicates that the compromised credential is from an infected user, because a simple password reset would be an ineffective response in that situation.

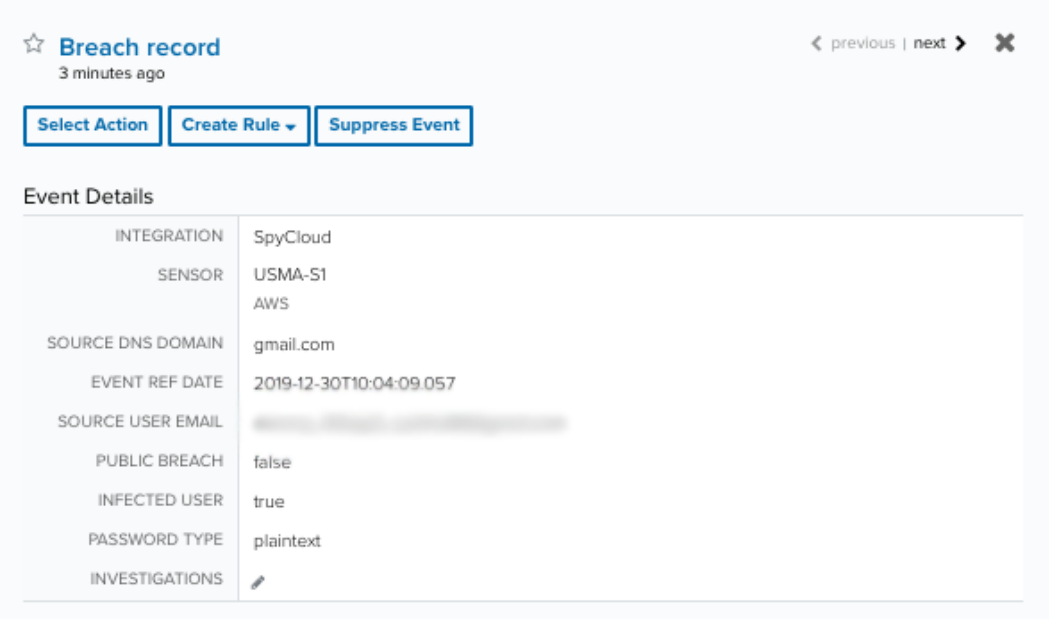
To view Dark Web Monitoring events

1. Go to **Activity > Events** to open the Events page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

   USM Anywhere includes several filters displayed by default.
3. (Optional.) Scroll down to the Data Source filter and select **SpyCloud** to display only the Dark Web Monitoring events on the page.



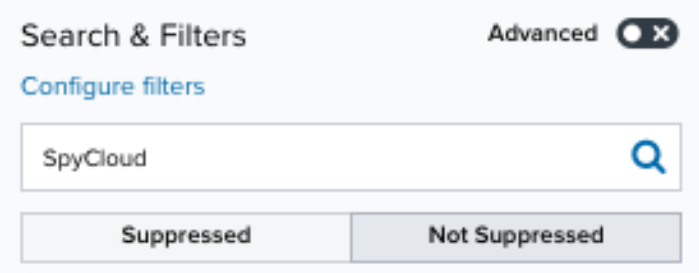
   If this filter is not displayed, click the **Configure filters** link, which is in the upper left corner of the page, to configure filters for the page. See Managing Filters in the *USM Anywhere User Guide* for more information about configuring filters for pages.
4. Select an event in the list to view detailed information.



To view Dark Web Monitoring alarms

1. Go to **Activity > Alarms** to open the Alarms page.
2. If the Search & Filters panel is not displayed, click the icon to expand it.

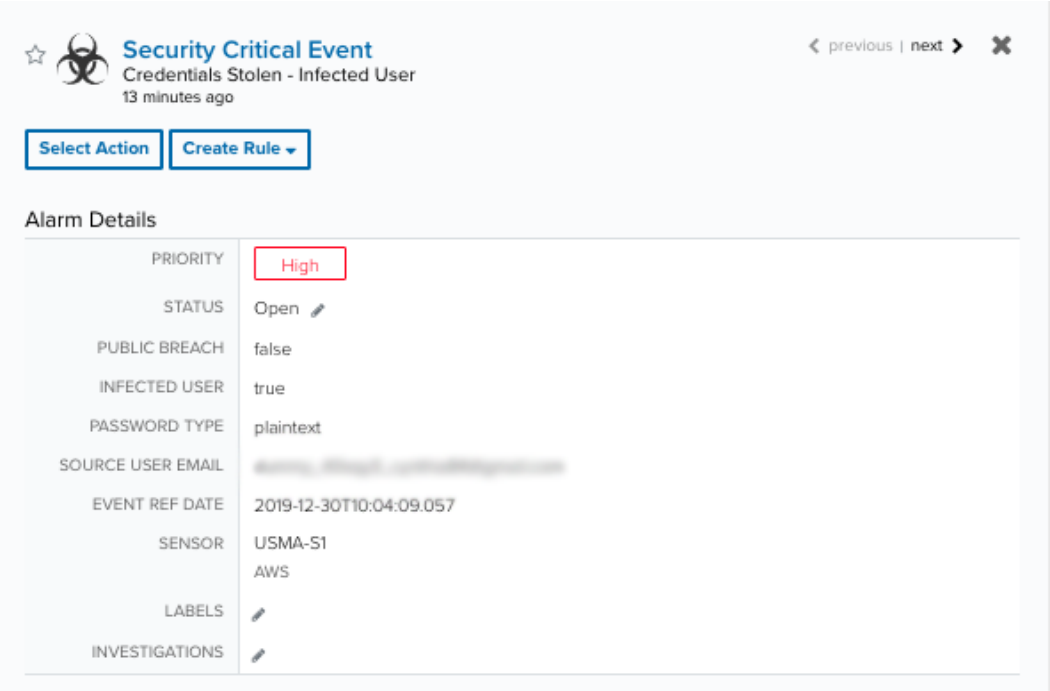
   USM Anywhere includes several filters displayed by default.
3. Enter **SpyCloud** as a search phrase and click the icon.



4. (Optional.) Scroll down to the Method filter and select a type to view only those alarms.

If this filter is not displayed, click the **Configure filters** link, which is in the upper left corner of the page, to configure filters for the page. See Managing Filters in the *USM Anywhere User Guide* for more information about configuring filters for pages.

5. Select an alarm in the list to view detailed information and recommendations.



BlueApp for Tenable.io

The BlueApp for Tenable.io enables you to gain actionable insight into your entire infrastructure's security risks, allowing you to quickly and accurately identify, investigate, and prioritize vulnerabilities and misconfigurations in your environment. The BlueApp for Tenable.io enhances the threat detection capabilities of USM Anywhere by collecting and analyzing data from the Tenablie.IO Vulnerability Management platform and provides orchestration actions to streamline incident response activities and to get deeper visibility into the assets on networks and their respective vulnerabilities based on risks identified in USM Anywhere.

Edition: The BlueApp for Tenable.io is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Note: The BlueApp for Tenable.io is compatible with the Tenable.io cloud-based cyber exposure platform.

This topic discusses these subtopics:

Configuring the BlueApp for Tenable.io

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ Manager

To configure the BlueApp for Tenable.io in USM Anywhere, you need to have the Tenable host URL, access key, and secret key.

Set Up Your Tenable.io API

Before USM Anywhere can collect information from Tenable.io, you must first connect the BlueApp with the Tenable.io API.

To acquire API keys from Tenable.io

1. Log in to Tenable.io Login Page using a valid user account.
   This account must be a member of the Administrators role in Tenable.io.
2. Generate the API keys according to the Generate API Keys.
3. Copy the access key and secret key to your clipboard or a secure location. You will need to enter them in USM Anywhere to configure the BlueApp.

Configure BlueApp for Tenable.io in USM Anywhere

To enable the BlueApp for Tenable.io

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.
5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the host URL, access key, and key secret.
7. Click **Save**.

BlueApp Log Collection

Once the BlueApp has been configured, you can choose to have USM Anywhere collect logs from the app on a regular basis.

To configure log collection for the BlueApp

1. Go to **Settings > Scheduler**.
2. In the Job Scheduler, search for the BlueApp on the sensor to which it was deployed.
3. In the enabled column, click the  icon for the inactive collection job.

   The  icon turns green, and collection is enabled.
4. (Optional.) Click the  icon to customize the frequency of the event collection.

BlueApp for Tenable.io Asset Discovery and Management

The BlueApp for Tenable.io features powerful vulnerability assessment capabilities that can be paired with USM Anywhere for extended security management. When you configure the app in USM Anywhere, you have the option to allow Tenable.IO Vulnerability Management to create assets that are discovered in scans, as well as merge the asset information provided from the Tenable.IO scan with the existing asset information in USM Anywhere.

Asset Creation from BlueApp for Tenable.io

When Tenable.IO runs a scan, it identifies all assets in the scan and assigns them an individual identifier (ID). These assets can be added to USM Anywhere by selecting the **Allow Creation of New Assets** checkbox in app's configuration menu. Assets created from a Tenable.IO scan will include the information ported from Tenable.IO in the USM Anywhere asset details.

Duplicate Asset Merge

Assets discovered in Tenable.IO scans may duplicate the assets already discovered in USM Anywhere. When you select the **Allow Merging of Existing Assets** checkbox in the Tenable.IO configuration menu, USM Anywhere will merge the information from the Tenable.IO scan with the existing asset. Assets are matched by comparing the variable IDs, IP address, and hostname from the Tenable.IO scan with the same asset details in USM Anywhere.

Manual Asset Merge

If the Merge Duplicate Assets checkbox in the Tenable.IO configuration menu isn't checked, USM Anywhere will keep a record of the assets that match one another. These assets are contained in the Merge Asset tab in the BlueApp for Tenable.io page.

To review these duplicate assets, click the **Merge Asset** tab and click **Review** next to the asset in the list. From here, you can respond to the asset discrepancy with one of the following actions:

- **Reject:** Cancel the match without creating a new asset or merging it with an existing asset, effectively ignoring the new asset discovered in the Tenable.IO scan.
- **Create New Asset**: Create an asset in USM Anywhere based on the information from the Tenable.IO scan.
- **Merge:** Merge the information from the Tenable.IO scan with the matching asset details in USM Anywhere.
- **Manually Match:** Choose the matching asset manually.

Once you have selected a response to the asset review, the status of your choice is reflected in the table of assets in the Merge Asset tab.

Asset Split

A USM Anywhere asset that has been merged with a Tenable.IO profile can be split back into two separate assets after they have been merged.

To split a merged asset

1. Go to **Environment > Assets**.
2. Locate the asset you want to split and click the ⌄ button next to the asset, and then click **Full Details**.

3. In the full asset view window, click **Split Asset** in the Asset Discovery section.

   A window opens showing the existing asset and the new asset that will be created once the two are split.

4. Click **Split Asset** to undo the asset merge and create a separate, new asset.

BlueApp for Tenable.io Actions

The BlueApp for Tenable.io provides a set of orchestration actions that you can use to streamline incident response activities in your USM Anywhere environment. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Tenable.io

Action	Description
Run Scan	Run this action to perform a vulnerability scan on an asset in the network
Run Scan with Tag	Run this action to perform a scan on all assets sharing the same tag
Create a Tag	Run this action to add a new tag in Tenable.io to be used later to group assets
Asset Discovery	Asset discovery for Tenable.io
Audit Events	Run this action to gather and record audit events
Add Tag	Run this action to create and assign a tag

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from Vulnerabilities

You can launch an action directly from vulnerabilities, and from the Full Asset Details page. If you want to apply an action to similar vulnerabilities that occur in the future, you can also create orchestration rules directly from the action applied to a Vulnerability.

To launch a Tenable.io response action for a vulnerability

1. Go to **Environment > Vulnerabilities**.
   Click the Vulnerability to open the details.
2. Click **Select Action**.
3. In the Select Action dialog box, select **Run Tenable.io Action**.
4. Select the app action and fill out the fields that are populated below.
5. Click **Run**.

   After USM Anywhere initiates the action for a vulnerability, it opens a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar vulnerabilities** and define the new rule. If not, click **OK**.

Creating Tenable.io Response Action Rules

Role Availability ✖ Read-Only ✖ Investigator ✔ Analyst ✔ Manager

You can create orchestration rules in USM Anywhere that automatically trigger a Tenable.io response action when vulnerabilities match the criteria that you specify. After you create a rule, new vulnerabilities that match the rule conditions will trigger the Tenable.io response action to create a new incident. The rule does *not* trigger for existing vulnerabilities.

You can create a new rule as follows:

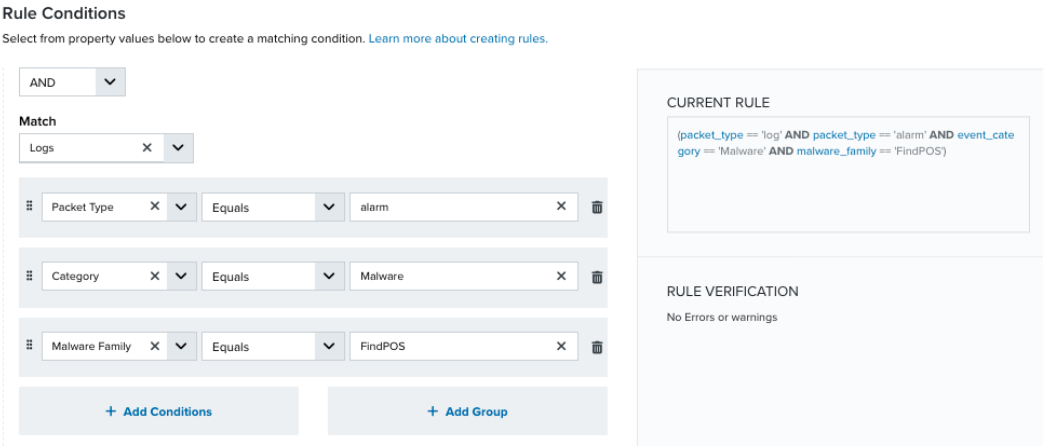
- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

Go to **Settings > Rules** and select **Response Action Rules** on the left navigation panel. Then click **Create Response Action Rule** to define the new rule.

- **From the App**: Go to the BlueApp for Tenable.io page and click the **Rules** tab. Click **Create New Rule** to define the new rule.

To define a new BlueApp for Tenable.io response action rule

1. Enter a name for the rule.
2. Select the App Action for the rule and specify the information for the BlueApp for Tenable.io incident.
3. At the bottom of the dialog box, set the Rule Condition parameters to specify the criteria for a matching vulnerability to trigger the rule.



- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. In the confirmation dialog box, click **OK**.

BlueApp for Zscaler

The BlueApp for Zscaler enables you to use the Zscaler Internet gateway tools to block IP addresses and URLs in response to threats detected in USM Anywhere. When an alarm, event, or rule is triggered, the BlueApp for Zscaler can add the source or destination IP address to the denylist in the Zscaler Internet Access (ZIA) interface.

Edition: The BlueApp for Zscaler is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

Warning: If the BlueApp fails and you receive a message informing you that it has not been loaded, please contact LevelBlue Technical Support to solve the problem.

This topic discusses these subtopics:

Configuring the BlueApp for Zscaler

Role Availability ✖ Read-Only ✖ Investigator ✖ Analyst ✔ **Manager**

To configure the BlueApp for Zscaler, you must first have the information listed in the Zscaler documentation, which includes the following:

- An API subscription
- An enabled API key
- An API admin account

To acquire Zscaler configuration details

1. Log in to the Zscaler admin page using your Zscaler credentials.
2. Go to **Administration > API Key Management**.

   The page displays the base Uniform Resource Identifier (URI) and API key.
3. Copy the base URI and key value to your clipboard or a secure location. You will need to enter them in USM Anywhere to configure the AlienApp.

To connect the Zscaler API to USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click **Configure API**.

5. If you have more than one deployed USM Anywhere Sensor, select the sensor that you want to use for the enabled BlueApp.

   BlueApps operate through a deployed sensor and use APIs to integrate with the connected third-party technology. Select the sensor that can access the integration endpoint. The HTTPS connections to the API will originate from this sensor, so it is important to make sure the sensor has network access to the BlueApp API endpoints.

6. Enter the information you collected previously:

   - Base URI
   - Username
   - Password
   - Zscaler API Key

7. Click **Save**.

8. Verify the connection.

   After USM Anywhere completes a successful connection to the Zscaler APIs, a  icon displays in the Health column.

   If the  icon displays, there is a problem with the connection. The Message column provides information about the issue. Repeat the steps to fix the configuration or troubleshoot your Zscaler connection.

The BlueApp for Zscaler and the BlueApp for LevelBlue Secure Remote Gateway

Because both the BlueApp for Zscaler and the BlueApp for LevelBlue Secure Remote Gateway share configuration components through BlueApp for Zscaler, configuring one BlueApp will cause the other to appear as configured in your My Apps page. This is expected behavior. Do not delete or disable the BlueApp for Zscaler or the BlueApp for LevelBlue Secure Remote Gateway. Changes to one BlueApp will cause configuration errors with the other BlueApp.

Forward Syslog Messages to BlueApp for Zscaler

To fully integrate USM Anywhere with the BlueApp for Zscaler, you can configure syslog forwarding in the Zscaler device to send events to your sensor. To collect logs from Zscaler Nanolog Streaming Service (NSS), you can add an NSS feed for alerts and enter the USM Anywhere Sensor IP address for the SIEM. See Adding NSS Feeds for Alerts for detailed instructions from the vendor.

However, the BlueApp for Zscaler can also act on events not generated from Zscaler. The actions you can use with this BlueApp take the source or destination IP addresses from any event or alarm and place them in an allowed list or blocked list, and then send it to Zscaler. See BlueApp for Zscaler Actions for details.

BlueApp for Zscaler Actions

The BlueApp for Zscaler provides a set of orchestration actions that you can use to identify and categorize items to block as a response to threats identified by USM Anywhere and add them to the lists maintained in your Zscaler Internet Access (ZIA).

As USM Anywhere surfaces events, vulnerabilities, and alarms, your team determines which items require a response action. Rather than manually tagging threats, you can use the BlueApp for Zscaler orchestration actions to enforce protection based on the information associated with the event or alarm. The following table lists the available actions from the BlueApp.

Actions for the BlueApp for Zscaler

Action	Description
Add Items to Block List from Event/Alarm	Run this action to add a source or destination to the Zscaler blocked list from an event or alarm to restrict their access
Add Items to Allowed List Using Event/Alarm	Run this action to add a source or destination to the Zscaler allowed list from an event or alarm to grant authorized access
Remove Items from Allowed List Using Event/Alarm	Run this action to remove items from an allowlist using an event or alarm

Actions for the BlueApp for Zscaler (Continued)

Action	Description
Add to Custom Category	Run this action to add a source or destination to a Zscaler category. Typing a category will bring up autocomplete suggestions of existing categories. When selecting this action, the Select Action window will also display two additional links at the bottom on the window. • Click **Search for existing categories** to see if the IP address is currently associated with any categories. • Click **URL Lookup** to obtain further information about the IP address such as the type of address and whether or not Zscaler has any registered security alerts associated with it.
Remove Items from Block List from Event/Alarm	Run this action to remove items from a block list from an event or alarm to restrict their access
Add Items to Allowed List Using Rule	Run this action to add items to an allowlist using a rule to grant authorized access
Remove Items from Allowed List	Run this action to remove items from an allowlist using a rule
Remove Items from Allowed List Using Vulnerability	Run this action to remove items from an allowlist using a vulnerability
Add Items to Block List Using Rule	Run this action to add items to a blocked list using a rule to restrict their access
Add Items to Allowed List Using Vulnerability	Run this action to add items to an allowlist using a vulnerability
Add Items to Block List Using Vulnerability	Run this action to add items to a blocked list using a vulnerability to restrict their access
Remove Items from Blocked List Using Rule	Run this action to remove items from blocked list using a rule
Remove Items from Blocked List Using Vulnerability	Run this action to remove items from blocked list using a vulnerability

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > BlueApps**.
2. Click the **Available Apps** tab.
3. Search for the BlueApp, and then click the tile.
4. Click the **Actions** tab to display information for the supported actions.
5. Click the **History** tab to display information about the executed orchestration actions.

Launch Actions from USM Anywhere

You can launch an action directly from alarms or events. If you want to apply an action to similar events that occur in the future, you can also create orchestration rules directly from the action applied to an alarm or event.

To launch a Zscaler orchestration action for an alarm

1. Go to **Activity > Alarms** or **Activity > Events**.
2. Click the alarm or event to open the details.
3. Click **Select Action**.
4. In the Select Action dialog box, select the **Zscaler** tile.
5. For the App Action, select the action you want to launch.

   You can launch an action to add or remove an IP address to the allowed list, add an IP address to the blocked list, or add the IP address to a custom category.

   Additional fields will be populated based on the action you've selected. Fill out the necessary fields for the app action.
6. Click **Run**.

   After USM Anywhere initiates the action for an alarm or event, it displays a confirmation dialog box.

   If you want to create a rule to apply the action to similar items that occur in the future, click **Create rule for similar alarms** or **Create rule for similar events** and define the new rule. If not, click **OK**.

Creating Zscaler Response Actions

Role Availability | ✗ Read-Only | ✗ Investigator | ✓ Analyst | ✓ Manager

Use the BlueApp for Zscaler to access the Zscaler response actions, which enable you to quickly respond to threats identified by USM Anywhere. You can create response action rules in USM Anywhere that automatically trigger when alarms or events match the criteria that you specify.

After you create a rule, new events or alarms that match the rule will trigger the Zscaler action to tag to the associated source or the destination host. The rule does **not** trigger for your existing alarms or events.

You can create a new rule as follows:

- **From the Rules page**: The Rules page provides access to all of your orchestration rules. The Orchestration Rules list includes suppression rules, alarm rules, event rules, filtering rules, notification rules, and response action rules. You can create new rules using the specific matching conditions that you define, as well as edit, delete, and enable or disable rules. See Orchestration Rules in the *USM Anywhere User Guide* for more information about managing orchestration rules.

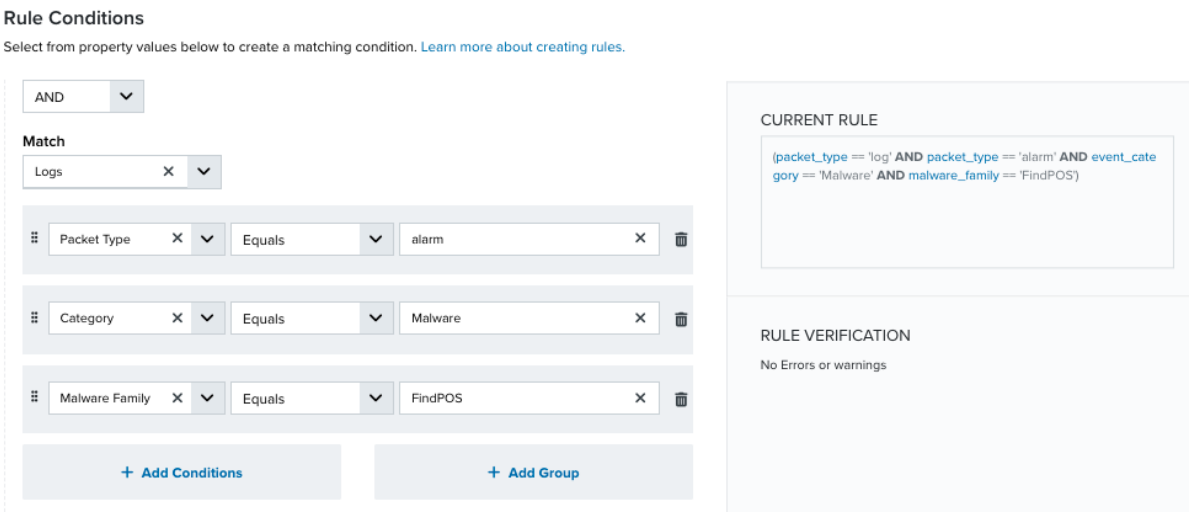
  Go to **Settings > Rules** and select **Response Action Rules** on the left navigation pane. Then click **Create Response Action Rule** to define the new rule.

To define a new Zscaler response action rule

1. Enter a name for the rule.
2. Select the action you want to launch from the **Action** drop-down menu.

   You can launch an action to tag the destination host or source for an alarm or an event.

3. At the bottom of the dialog box, set the rule condition parameters to specify the criteria for a matching alarm or event to trigger the rule.



- This section provides suggested property/value pairs from the selected alarm or event that you can use as conditions for the rule. Click the icon to delete the items that you do not want to include in the matching conditions. You can also add other conditions that are not suggested.
- If you create the rule from the Rules page, you must use the Add Condition and Add Group functions to define the property/value pairs that you want to use as conditions for the rule.
- At the bottom of the dialog box, click **More** to display the optional multiple occurrence and window-length parameters.

Conditional Expression

Select an operator and add one or more conditions to form the conditional expression. You can include a condition group to evaluate a subset of conditions. The Current Rule pane displays the constructed expression in standard syntax. The box displays a red border if the expression is syntactically invalid as currently specified. A valid expression is required to save the rule definition.

Select the operator used to determine the match for multiple conditions:

- **AND**: Match all conditions.
- **OR**: Match any one condition.
- **AND NOT**: Exclude items matching all conditions after the first.
- **OR NOT**: Include all items that do not match any conditions after the first.

Click **Add Condition** to add a condition. For each condition, specify the field name, evaluator, and value. If the evaluation returns *true* for the condition, it is a match.

Click **Add Group** to add a condition group. A new group includes a condition and its own operator used to match the conditions within the group. You can nest condition groups.

Occurrences

Specify the number of event or alarm occurrences that produce a match on the conditional expression to trigger the rule. The default value is 1. You can enter the number of occurrences or use the arrow to scroll the value up or down.

USM Anywhere uses this in conjunction with the Length option to specify the number of occurrences within a time period that will trigger the rule. For example, you can define a rule to trigger for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

Length

Specify the length of the window to identify a match for multiple occurrences. Enter the number and choose a time unit value of seconds, minutes, or hours. This time period identifies the amount of time that transpires from the first occurrence to the last occurrence. If the number of occurrences is not met within this period, the rule does not trigger.

4. Click **Save Rule**.
5. Click **OK** in the confirmation dialog box.

Custom BlueApps and Log Parsers

In addition to the many BlueApps offered by USM Anywhere, LevelBlue offers you the option of configuring an advanced BlueApp custom to your resources and the way you use them. With custom BlueApps, you can better monitor activity in your environment according to your needs. Custom BlueApps enable you to collect and analyze log data from any third-party applications your environment relies upon and gives you ultimate granularity to configure precisely how USM Anywhere should view and process your data.

You can also create a custom log parser. Custom log parsers are designed to parse logs from any application that uses Amazon Simple Storage Service (S3) or syslog authentication and for which USM Anywhere does not already provide a BlueApp.

Like regular advanced BlueApps, your custom BlueApp or log collector enables you to do the following:

- Log collection
- Network inventory
- Orchestration
- Notification
- Vulnerability assessment
- Response

Note: Although custom BlueApps are flexible, not every third-party tool is currently supported. Differences in standards, vendor implementation, authentication methods, and more may limit which third-party apps can be connected using a custom BlueApps.

Edition: The ability to create a custom BlueApp or log collector is available in the Standard and Premium editions of USM Anywhere. See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

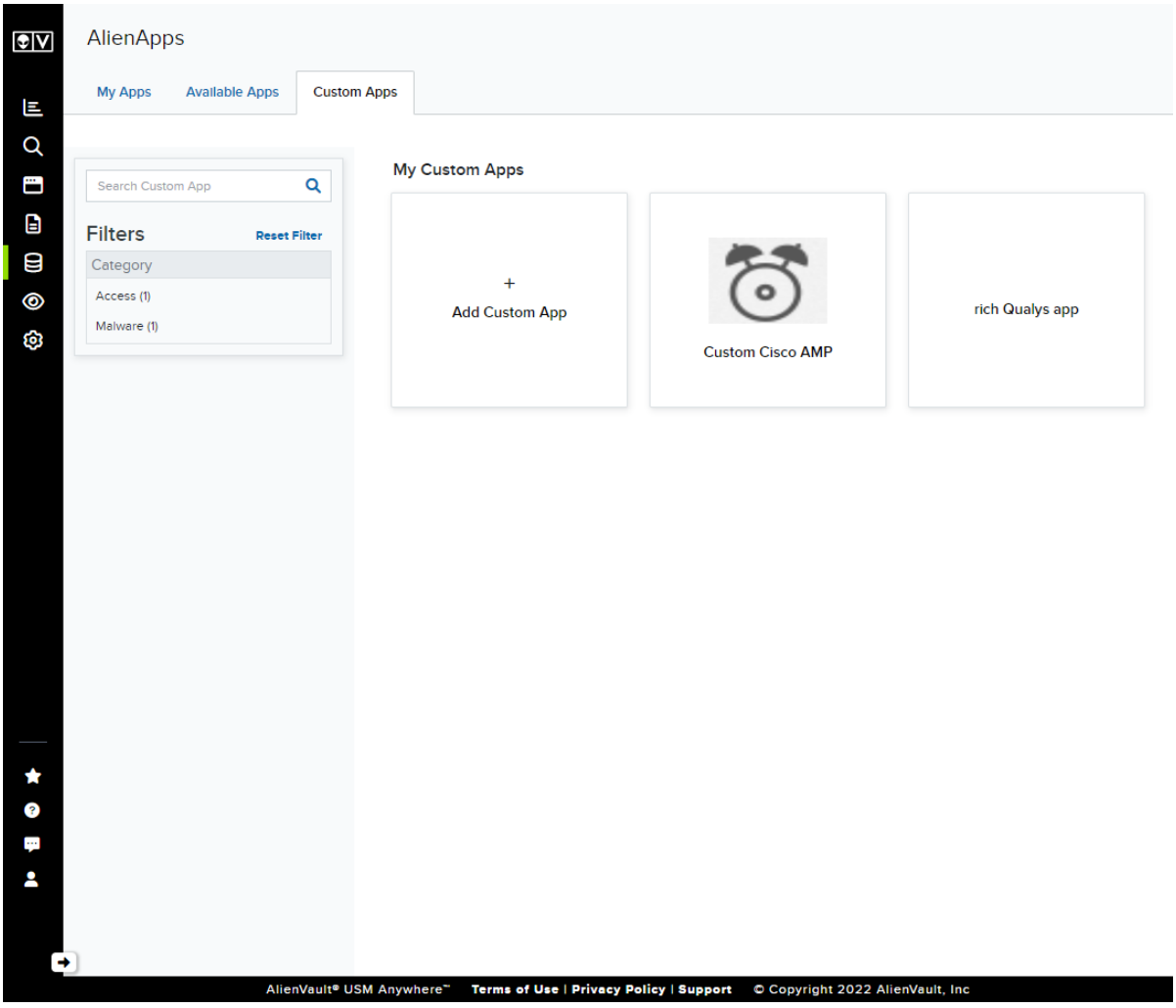
Configuring a Custom BlueApp for Use with Your USM Anywhere

LevelBlue provides the opportunity to configure your own custom BlueApps to better monitor activity in your USM Anywhere environment. You can use custom BlueApps to extend the threat detection and response capabilities of the USM Anywhere platform according to your needs. Import data from products and services that use a Representational State Transfer (REST) API by configuring your custom BlueApp using basic authentication, an API key, or OAuth2.

Important: Custom BlueApps connect using dynamic IP addresses. LevelBlue recommends that you allow BlueApps outbound access across all IP addresses.

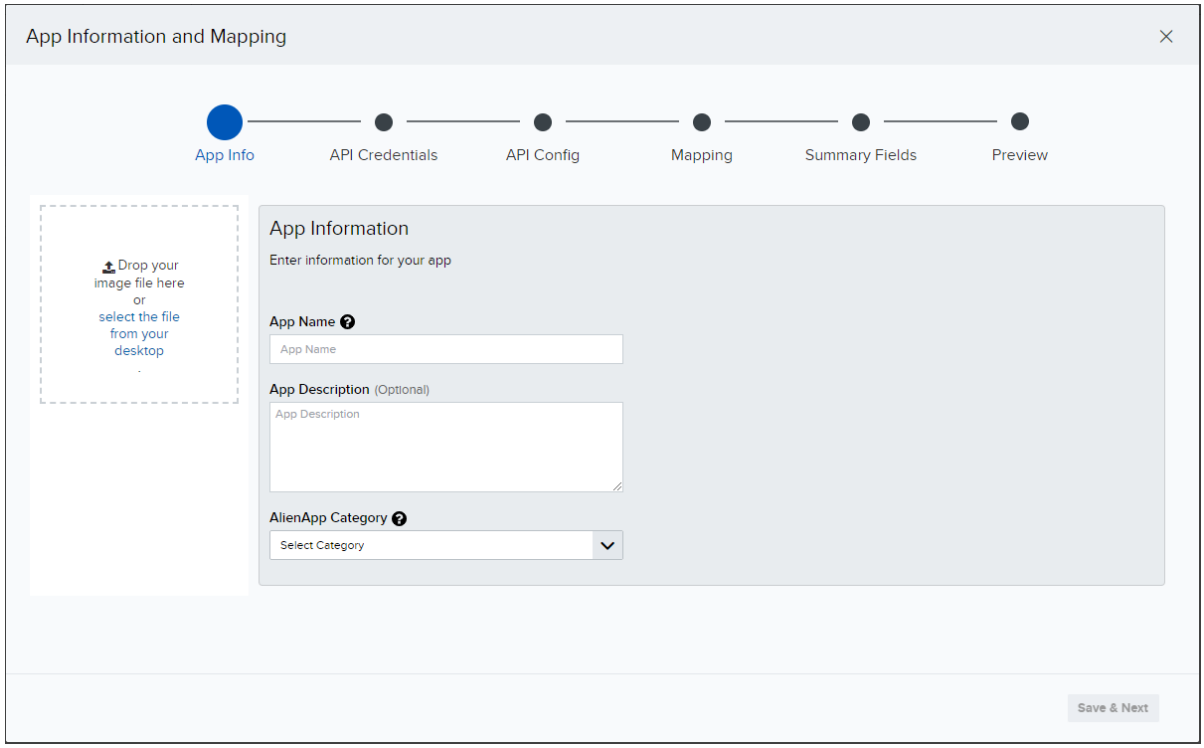
To configure a custom BlueApp

1. Go to **Data Sources > BlueApps > Custom Apps**.



2. Click **Add Custom App** to begin creating your new BlueApp.

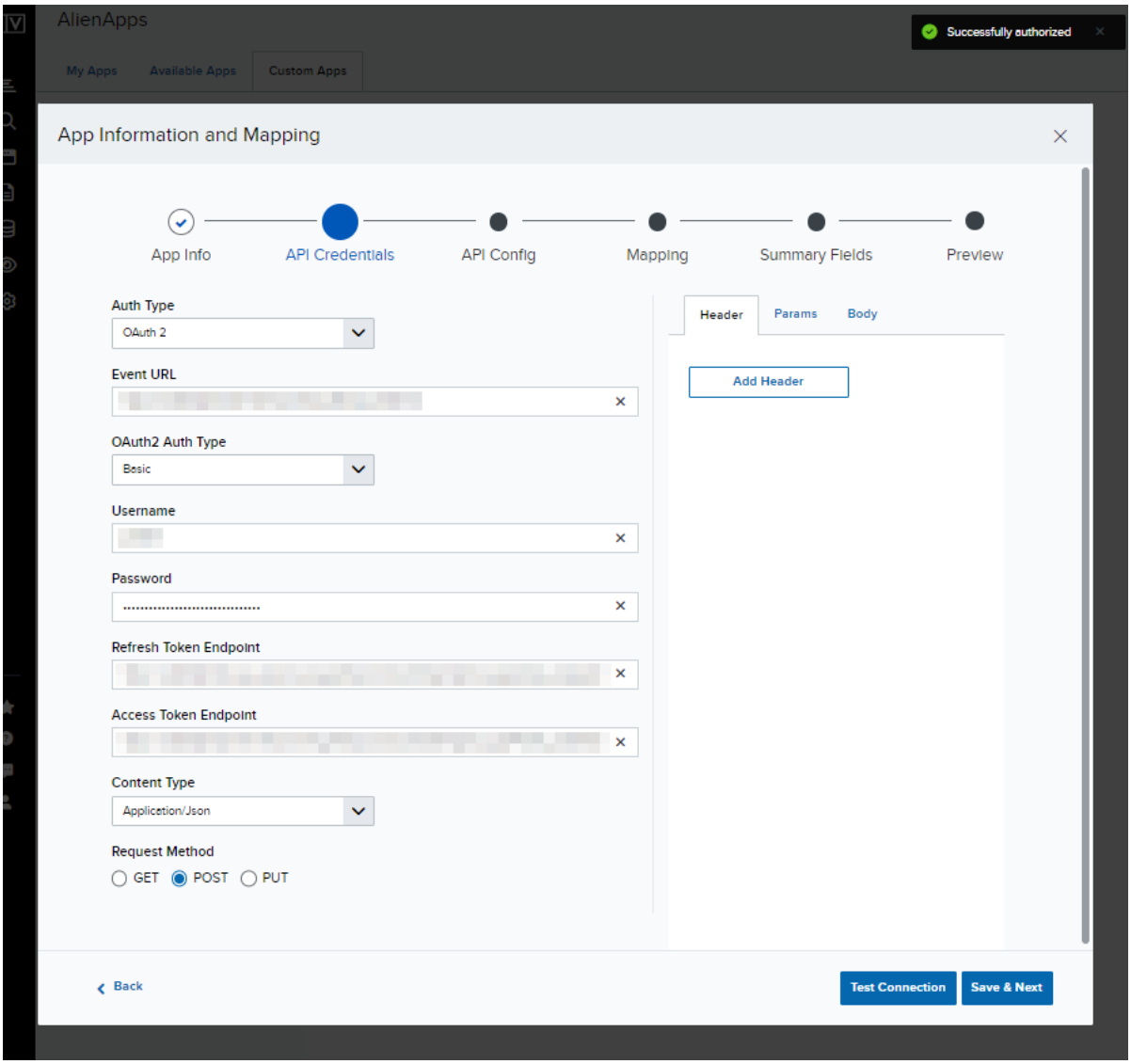
3. On the App Information and Mapping page, give your BlueApp a name and some identifying information.



   - **App Name:** Provide a unique name for your BlueApp.
   - **(Optional.) App Description:** Describe the new BlueApp's intent or functionality.
   - **AlienApp Category:** Tag your app with a category, which will help you organize your BlueApps. You can search for BlueApps by category in the Custom App main page.
   - **(Optional.) Logo:** You may import a logo for this BlueApp.

4. Click **Save & Next** to save your new BlueApp and begin configuring it.
5. Configure the authentication credentials your BlueApp will use to connect to the third-party application. When you have finished entering your credentials, confirm them by clicking **Test Connection**.

> **Important:** This is entirely dependent upon your third-party application. Be sure to make selections in line with the authentication method required by your third-party application.



If configuring a custom BlueApp via API key

1. In the Auth Type drop-down list, select **API Key**.
2. Enter the necessary connection information for your BlueApp to connect to the API:
   - **Event URL:** The destination address for the API connection.
   - **Header Name and Header Value:** The API authentication key-value pair for your BlueApp to use when connecting to the third-party API.
   - **Request Method:** Select **GET**, **POST**, or **PUT**.
3. Click **Test Connection** to verify the connection information you have just entered.

If configuring a custom BlueApp via Basic Authentication

1. In the Auth Type drop-down list, select **Basic Auth**.
2. Enter the necessary connection information for your BlueApp to connect to the API:
   - **Event URL:** The destination address for the authenticated connection.
   - **Username and Password:** The authentication credentials for your BlueApp to use when connecting to the third-party API.
   - **Request Method:** Select **GET**, **POST**, or **PUT**.
3. Click **Test Connection** to verify the connection information you have just entered.

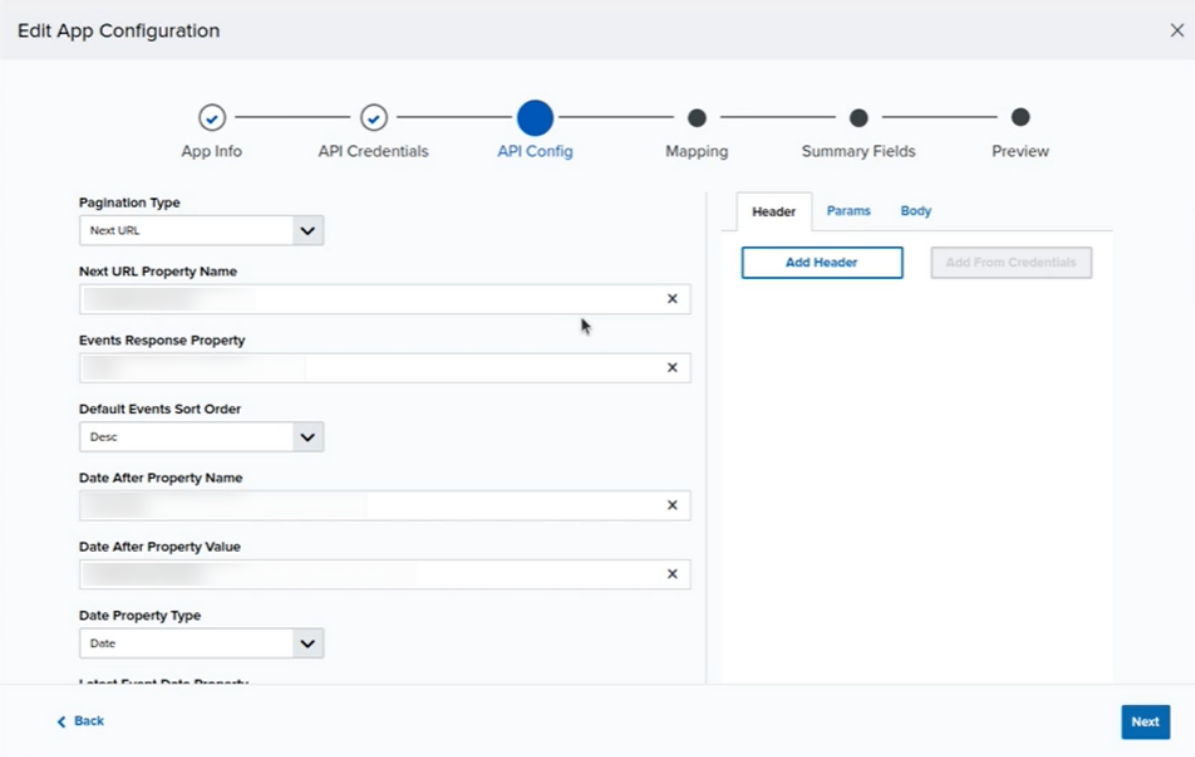
If configuring a custom BlueApp via OAuth2

1. In the Auth Type drop-down list, select **OAuth2**.
2. Enter your Event URL.
3. Use the OAuth2 Auth Type drop-down to select your authentication type, and then enter the information required by that authentication type:
   - **Basic:** Configure the app to authenticate with a username and password.
   - **Client ID and Client Secret:** Configure the app to authenticate with a client ID and secret.
4. Enter the necessary connection information for your BlueApp to connect to the API:
   - **Client ID and Client Secret:** The authentication credentials for your BlueApp to use when connecting to the third-party API if using client ID and client secret authentication.
   - **Username and Password:** The authentication credentials for your BlueApp to use when connecting to the third-party API if using basic authentication.
   - **Access Token Endpoint:** The access token endpoint for your OAuth2 connection.
   - **Refresh Token Endpoint:** The refresh token endpoint for your OAuth2 connection.
   - **Content Type:** The appropriate content type for your connection.
   - **Request Method:** Select **GET**, **POST**, or **PUT**.
5. Click **Test Connection** to verify the connection information you have just entered.

6. Once your credentials have been verified, click **Save & Next**.

Important: The credentials you have entered will be validated when you click **Test Connection**. If they cannot be verified at this step, you must correct them and ensure they are validated before moving on to the next step.

7. Represent the API configuration your custom AlienApp should expect from your third-party resource.



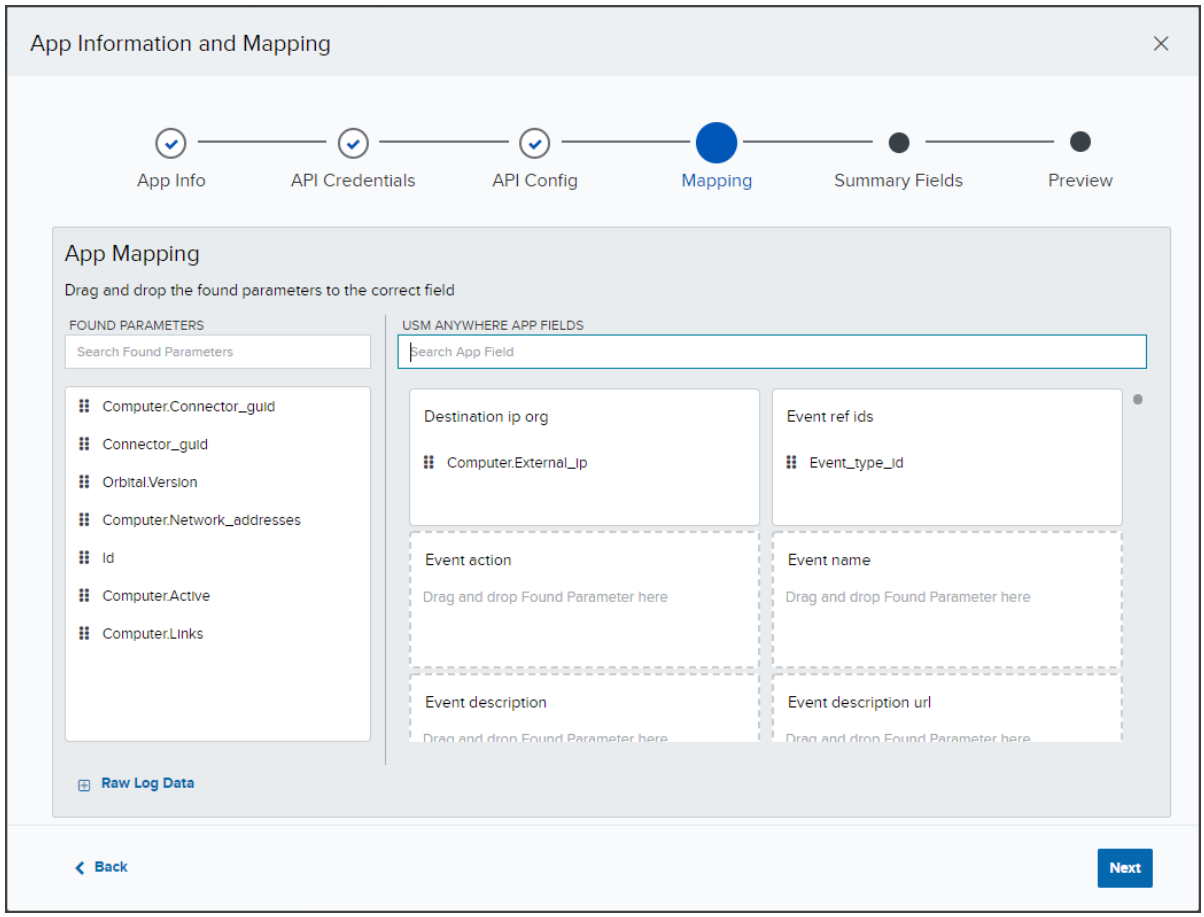
Warning: This is entirely dependent upon your third-party application. Be sure to make selections in line with the authentication method required by your third-party application.

1. Specify the return format, pagination methods, date format, and output format (JSON, XML, or CEF).
2. Configure the required values your API call may require. When the field is nested in the return under parent fields, use a period to separate parent and child fields.
3. Configure Headers, Params, and Body as required by the third-party application's API.

Note: If there are any fields you want to be able to filter against, you must configure them under Params.

Click **Next** to continue.

8. USM Anywhere uses the configuration details from the previous two steps to connect with your third party and extract data fields found in the logs they send. Use this page to configure the mapping details between the third-party application's data fields and fields in USM Anywhere by dragging and dropping from the detected fields to their matching fields in USM Anywhere.



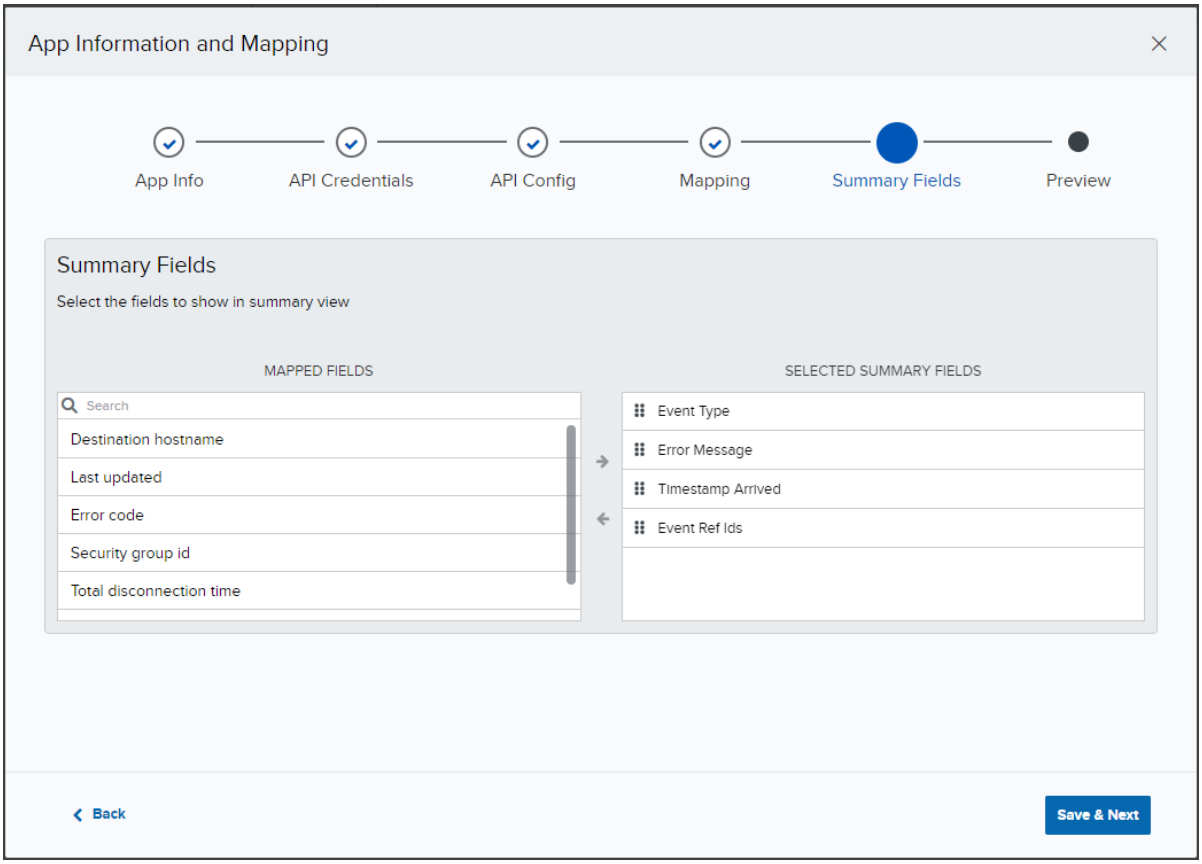
- **Found Parameters:** Fields on the left are extracted from logs fetched from your third-party application.
- **USM Anywhere App Fields:** Fields on the right are the standard USM Anywhere data

labels. Users can map multiple found parameters to the same USM Anywhere app field.

Important: See **Event Keys** descriptions to help you match extracted fields with standard USM Anywhere data fields.

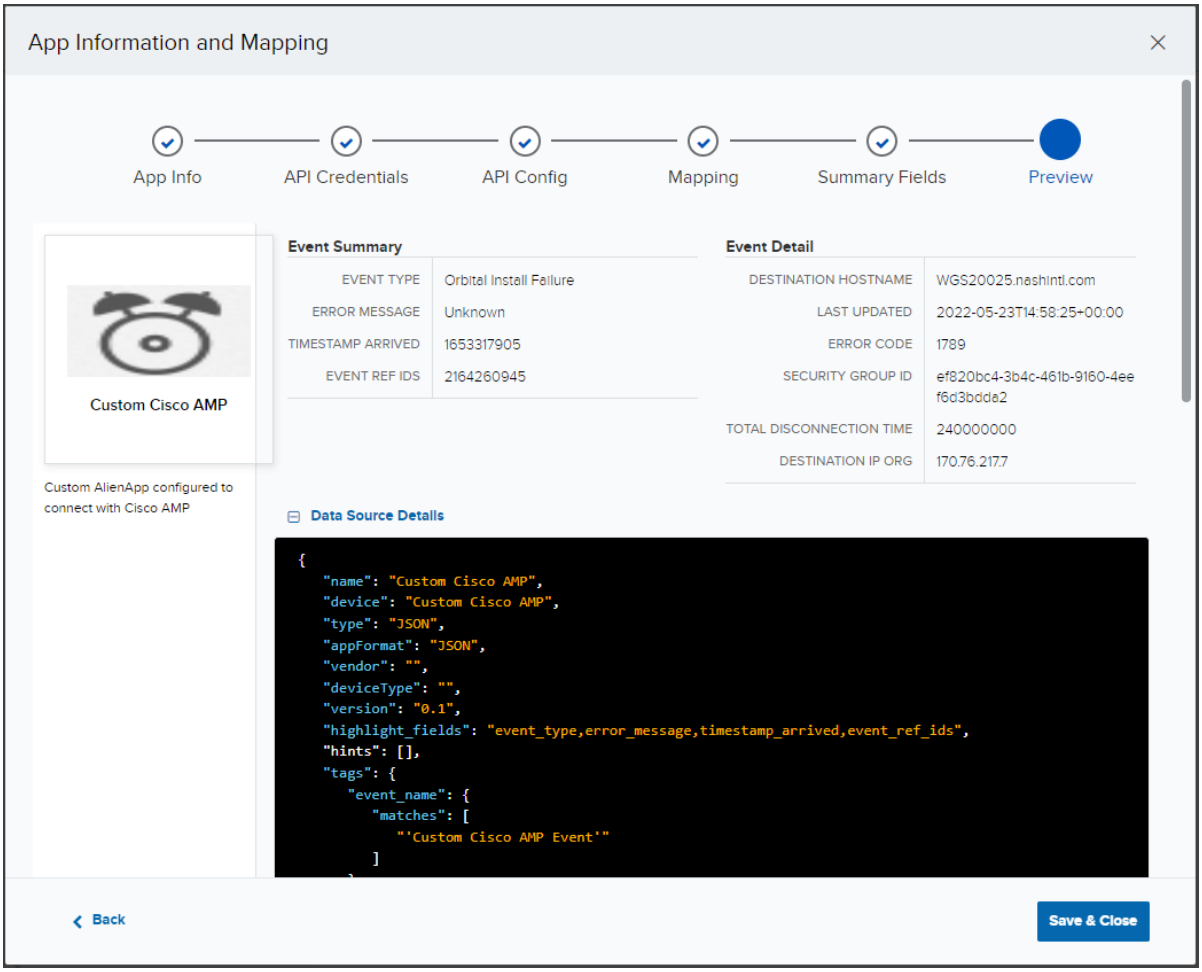
Click **Next** to continue.

9. Select which log fields to include in the Event Details for events your new BlueApp will generate.



Click **Save & Next** to continue.

10. Use the Preview screen to review your custom BlueApp's configuration.



    You can use the Back button to navigate to any previous page and make changes.

11. Once you have finalized your BlueApp details and configuration, click **Save & Close** to finish creating your new BlueApp.

After you have finalized and created your custom BlueApp, you can continue to make changes or refine its configuration by returning to the Custom Apps page and opening your BlueApp for editing.

Configuring a Custom Log Parser for Use with Your USM Anywhere BlueApp

In addition to the various BlueApps offered by USM Anywhere, LevelBlue gives you the option of configuring your own custom log parser to better monitor activity in your environment according to your needs.

The custom log parser operates by taking an event of your choosing and using the logs that generated it to model how to parse similar logs in the future. The configuration decisions you make when creating your new generic log collector will determine precisely how this parser will interpret such logs in the future. This enables you to create a specialized log parser to process any of the events your USM Anywhere doesn't otherwise know how to parse, which USM Anywhere labels as "generic events".

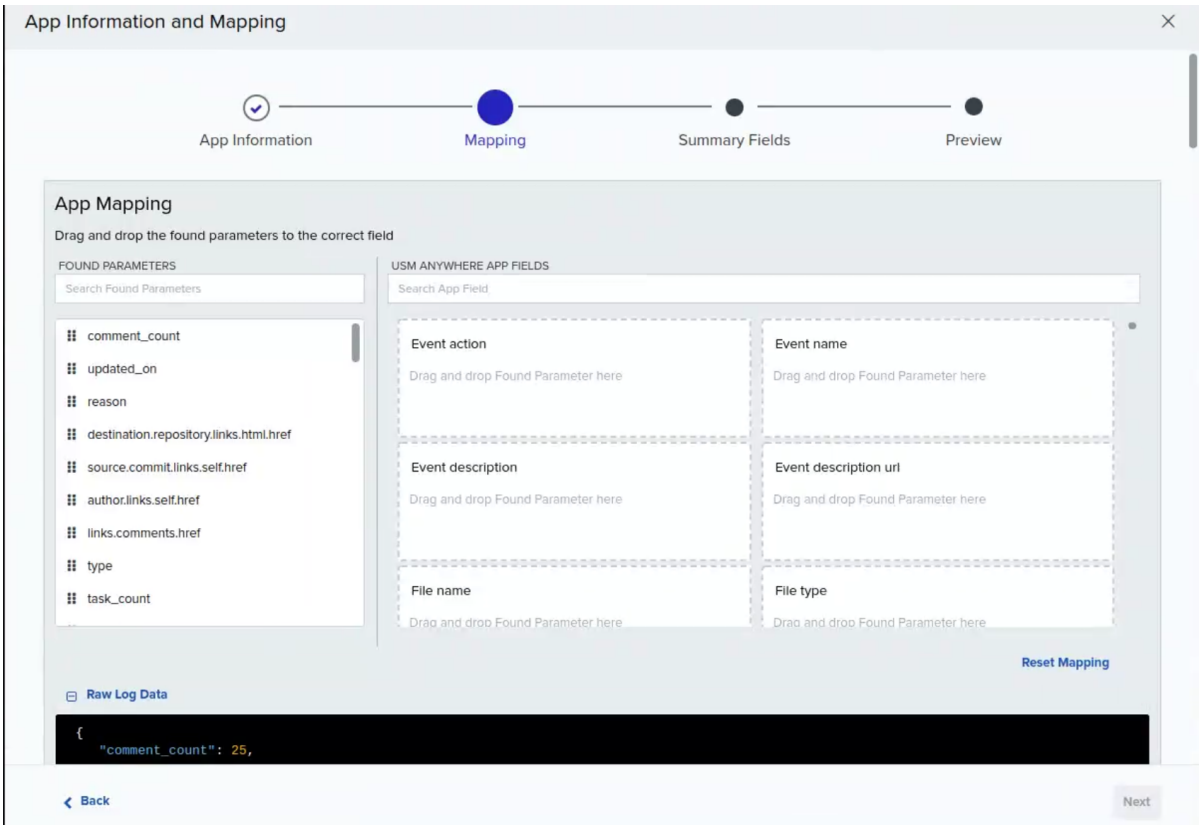
Important: Custom BlueApps connect using dynamic IPs. Please allow access to the data source on any IP.

Note: If you are looking for a more robust integration than a custom log parser offers, you can create a fully customized BlueApp to collect and analyze logs from a third-party application. See Configuring a Custom AlienApp for detailed instructions on how to create an AlienApp to suit your environment's needs.

To configure a custom log collector

1. Within your USM Anywhere, navigate to the generic event for which you want to create a log parser.
2. Click the event to open the Event Details.
3. Click **Custom App** to begin creating your new custom log parser.
   This opens the Custom AlienApp Wizard at the Mapping stage.

   Important: Custom BlueApps only support JSON, XML, and CEF log formats. The entire raw log must be in a single format and cannot contain a syslog header.
4. USM Anywhere uses the configuration details from the previous two steps to connect with your third party and extract data fields found in the logs they send. Use this page to configure the mapping details between the third-party application's data fields and fields in USM Anywhere by dragging and dropping from the detected fields to their matching fields in USM Anywhere.

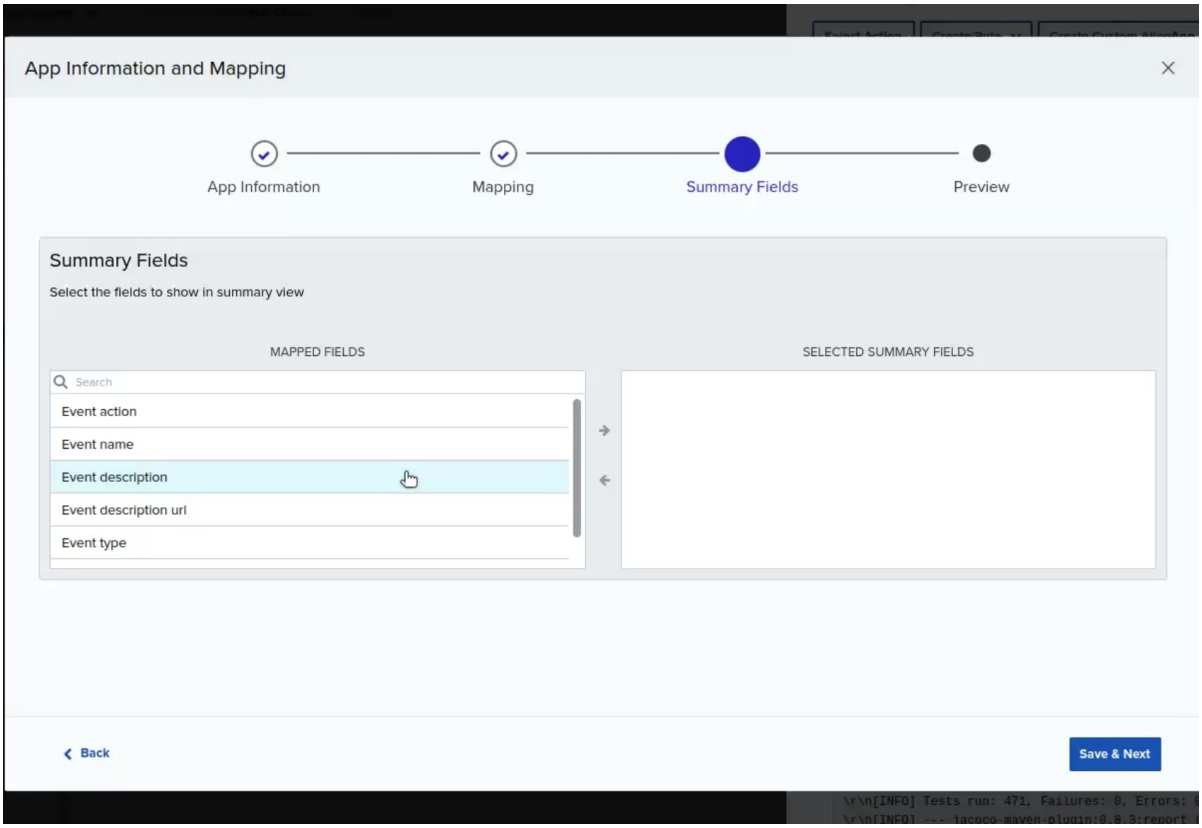


- **Found Parameters:** Fields on the left are extracted from logs fetched from your third-party application.
- **USM Anywhere App Fields:** Fields on the right are the standard USM Anywhere data labels. Users can map multiple found parameters to the same USM Anywhere app field.

> **Important:** See **Event Keys** descriptions to help you match extracted fields with standard USM Anywhere data fields.

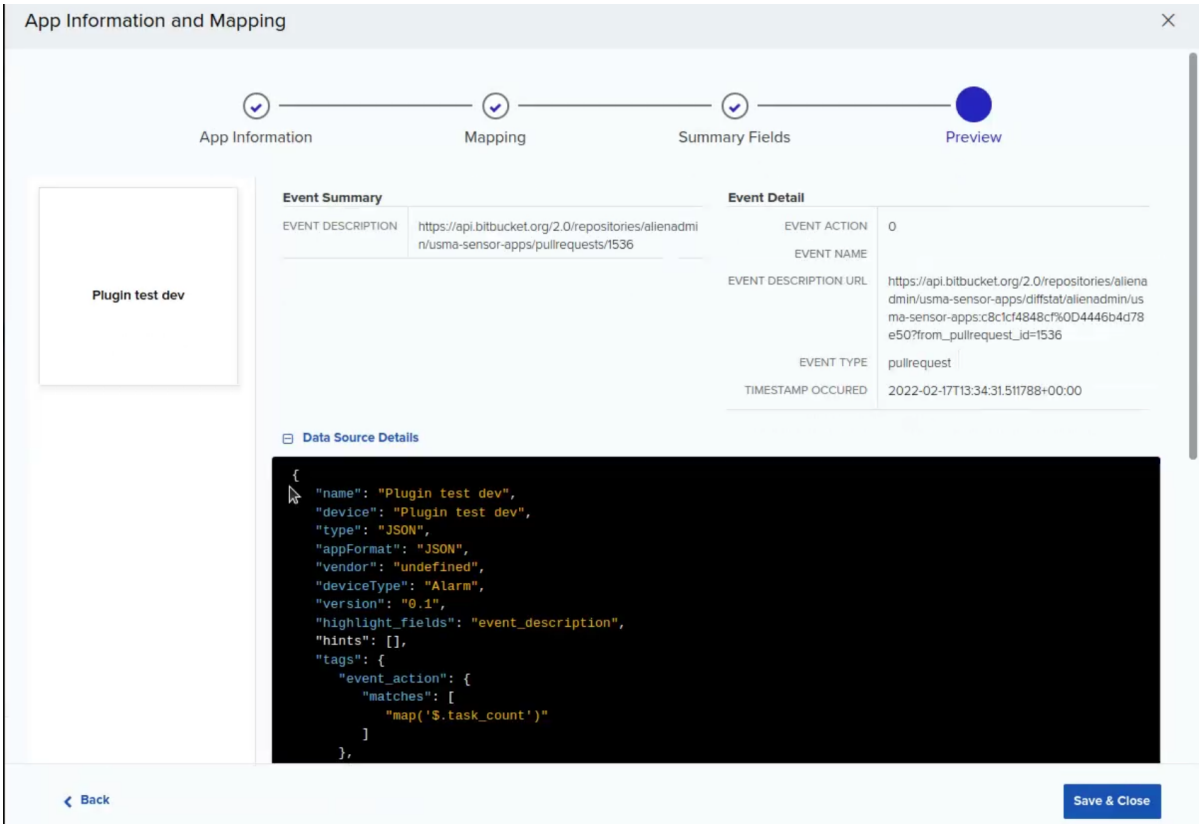
Click **Next** to continue.

5. Select which log fields to include in the Event Details for events your new log parser will generate.



Click **Save & Next** to continue.

6. Click **Data Source Details** to review your custom log parser's configuration.



   You can use the Back button to navigate to any previous page and make changes.

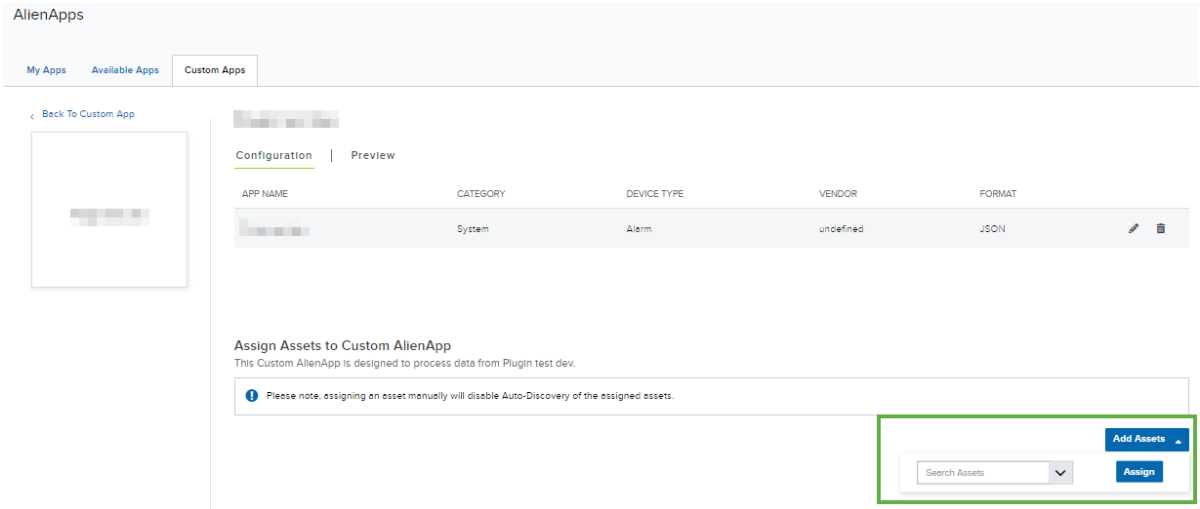
7. Once you have finalized your log parser's configuration, click **Save & Close** to finish creating your new log parser.

Important: You must assign your log parser to one or more assets before it will begin collecting logs.

After you have finalized and created your custom log parser, you can continue to make changes or refine its configuration by returning to the Custom Apps page and opening your log parser for editing.

To assign an asset to a custom log parser

1. Navigate to **Data Sources > Custom Apps > My Custom Apps**.
2. From the list of custom BlueApps and log parsers, click on the log parser you wish to assign an asset to.
3. Click **Add Assets** to open a search field.



4. Search for an asset by entering all or part of the asset name into the search field. Your search results will appear in a drop-down list.
5. Select the asset you wish to assign to this log parser, and then click **Assign**.
6. (Optional.) Continue using the search field to assign as many assets as you wish.

Templates for Custom Advanced BlueApp Configuration

In addition to the many BlueApps offered by USM Anywhere, LevelBlue offers you the option of configuring an advanced BlueApp custom to your resources and the way you use them. With custom advanced BlueApps, you can better monitor activity in your environment according to your needs.

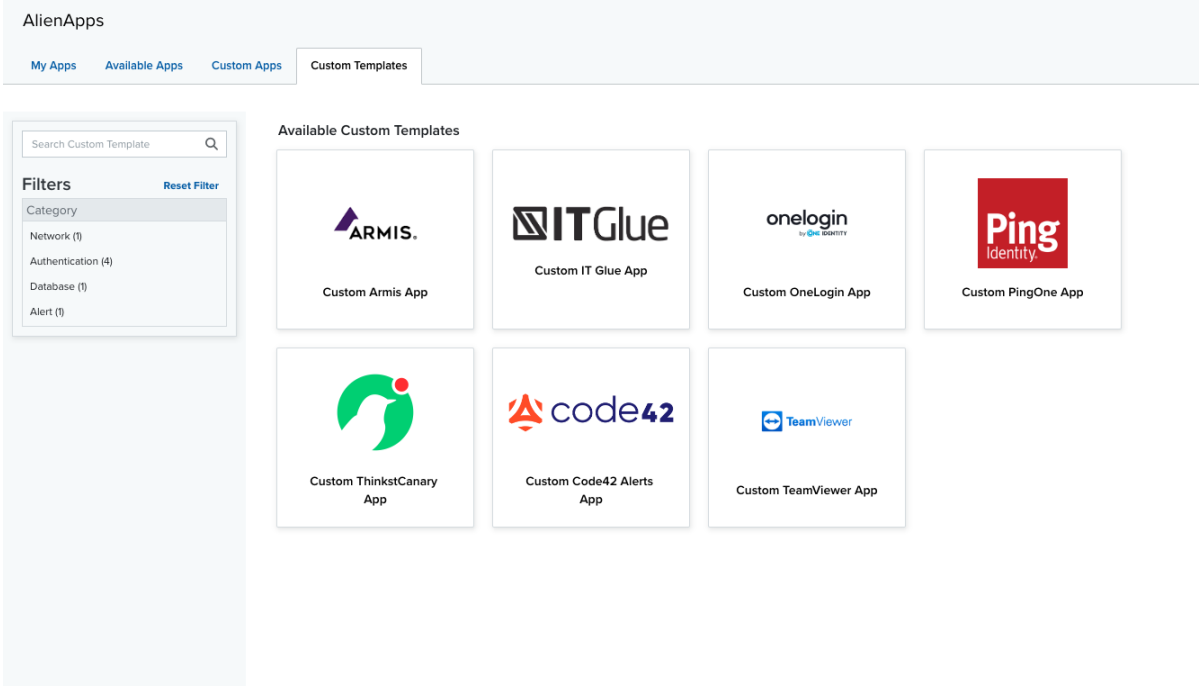
The custom advanced BlueApp feature is quite powerful, unlocking the ability to import events from almost any product or service that uses a REST API. To make this configuration process easy and approachable, LevelBlue offers configuration guides for the most oft-requested custom advanced BlueApps, providing clear guidance on the exact configurations needed to set up authentication of your custom advanced BlueApp.

Before getting started, you will need to ensure that you are able to generate the required authentication information from the application or service for which you are trying to create an application. The configuration guides LevelBlue provides endeavor to document the highest level of security available when connecting to your third party resource. For that reason, LevelBlue recommends that you follow the documented authentication configuration when setting up your custom advanced BlueApp.

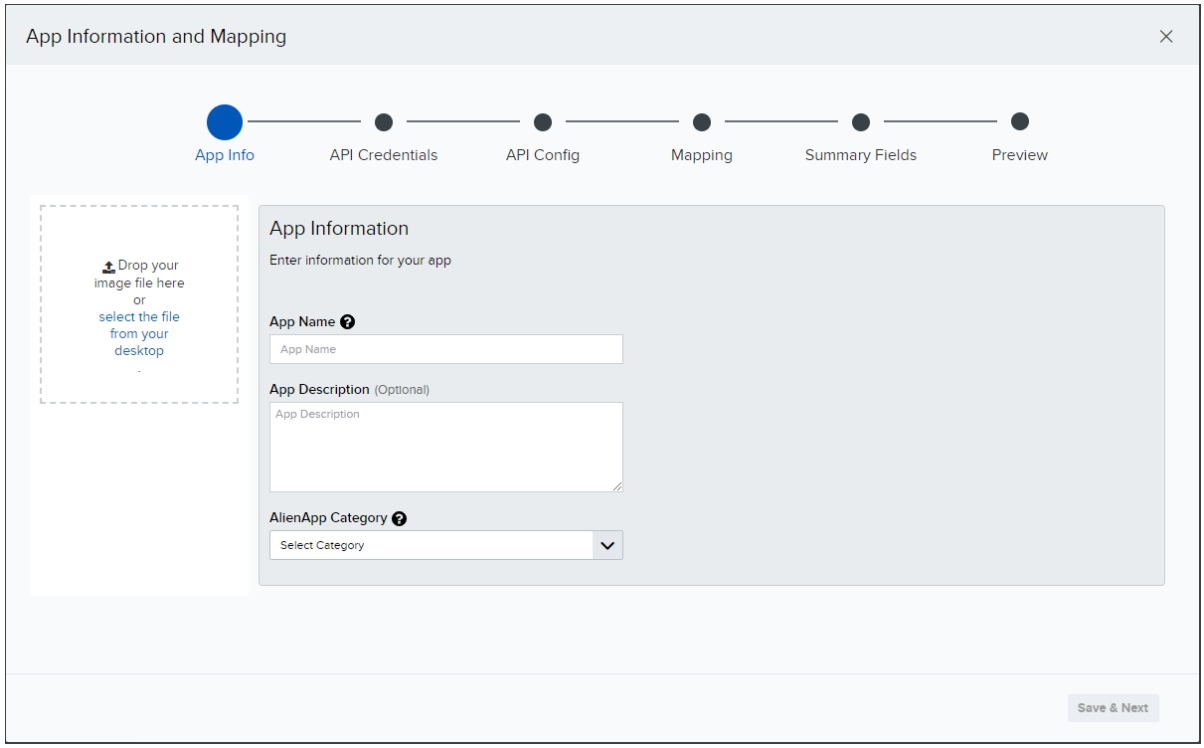
Note: If you don't find a template for the application you need there, you can request one by following the instructions here.

To use a template to create your custom advanced BlueApp

1. Go to **Data Sources > BlueApps > Custom Templates**.
2. Select the template you want to use from the list of available templates.



3. On the first page, give your BlueApp a name and some identifying information.



- **App Name:** Provide a unique name for your BlueApp.
- **(Optional.) App Description:** Describe the new BlueApp's intent or functionality.
- **Category:** Tag your app with a category, which will help you organize your BlueApps. You can filter BlueApps by category in the Custom App main page.
- **(Optional.) Logo:** You may import a logo for this BlueApp.
  The template may include a logo already. If so, you can keep the preconfigured logo or change it per your custom app requirements.

Click **Next** to continue.

4. The template you chose comes preconfigured to use the correct type of authentication your third-party application requires.
   You must provide the credentials your BlueApp will use to connect to the third-party application. When you have finished entering your credentials, confirm them by clicking **Test Connection**.

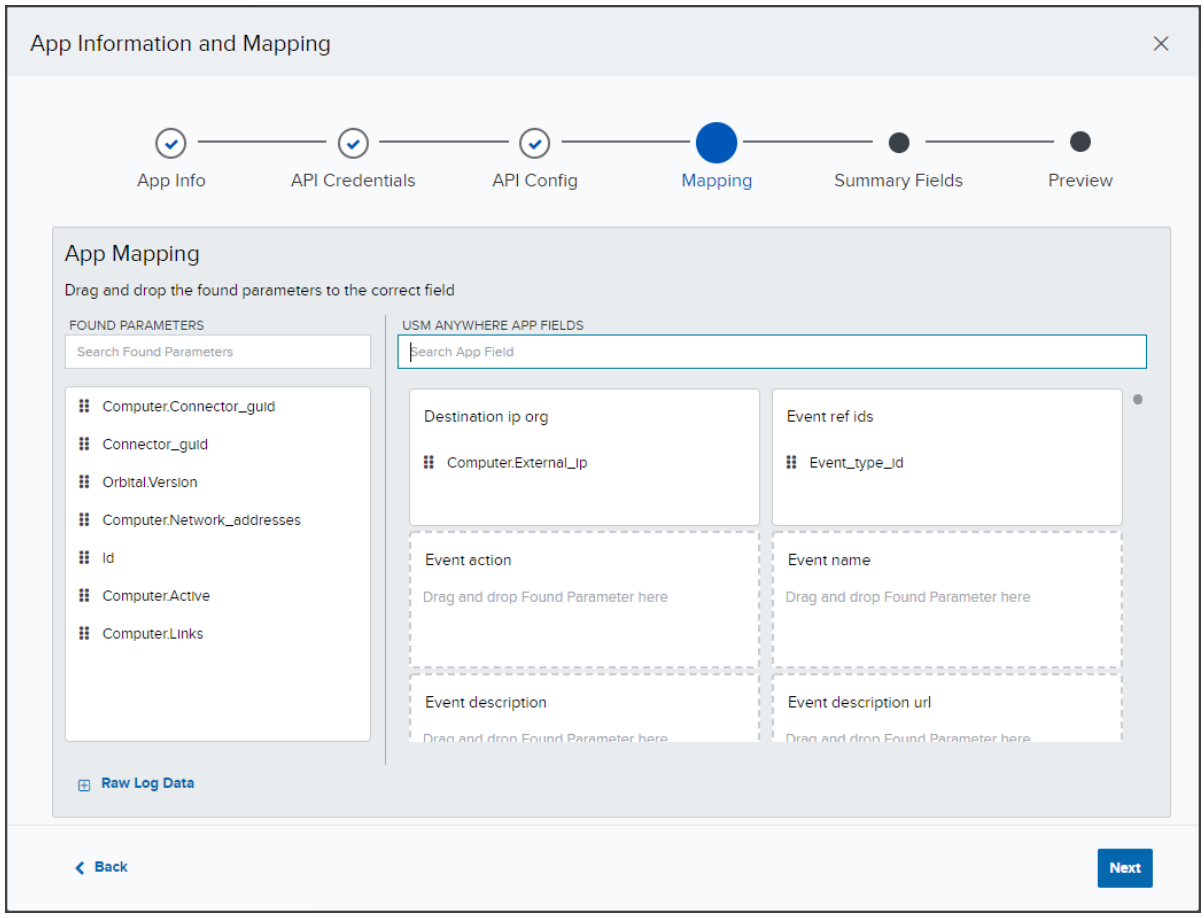
   Click **Next** to continue.

5. The custom template already contains most of the API configuration your custom BlueApp will need to communicate with your third party.
   Check the template specifications to see whether there is any additional configuration information you must to enter manually to prepare your advanced BlueApp to sync with your third-party application.

   Important: While the template comes prepopulated with as much configuration as possible, if there are any fields you want to be able to filter against you must manually ensure that they are configured here under Params.

   Click **Next** to continue.

6. USM Anywhere uses the configuration details from the previous two steps to connect with your third party and extract data fields found in the logs they send. In addition, the custom template is configured with many of the mappings you will need between the third-party application's data fields and fields in USM Anywhere.
   Review the mappings populated by the template. If necessary, you can adjust or further configure the mapping details by dragging and dropping from the detected fields to their matching fields in USM Anywhere.



- **Found Parameters:** Fields on the left are extracted from logs fetched from your third-party application.
- **USM Anywhere App Fields:** Fields on the right are the standard USM Anywhere data labels.

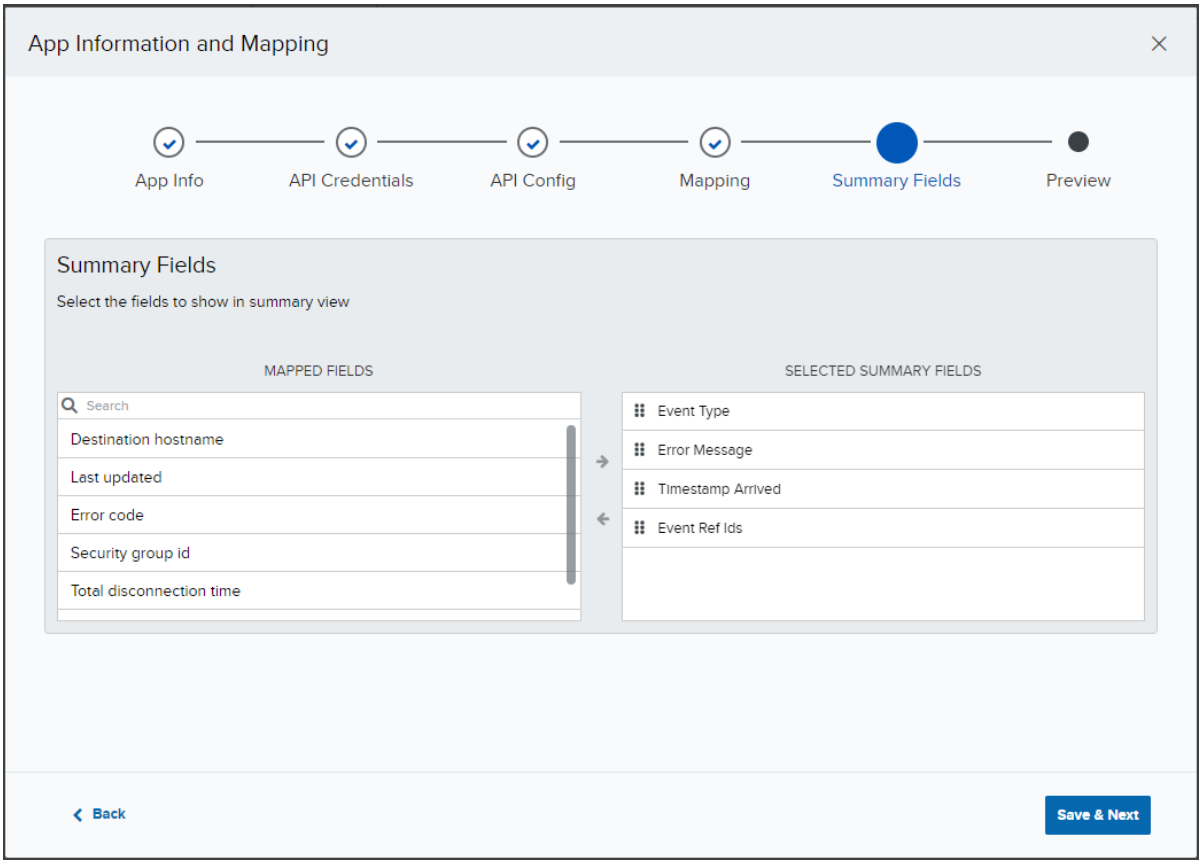
Note: You can map multiple found parameters to the same USM Anywhere app field.

See Event Keys for detailed definitions of the standard USM Anywhere data fields to help you match the extracted fields with those from USM Anywhere.

Click **Next** to continue.

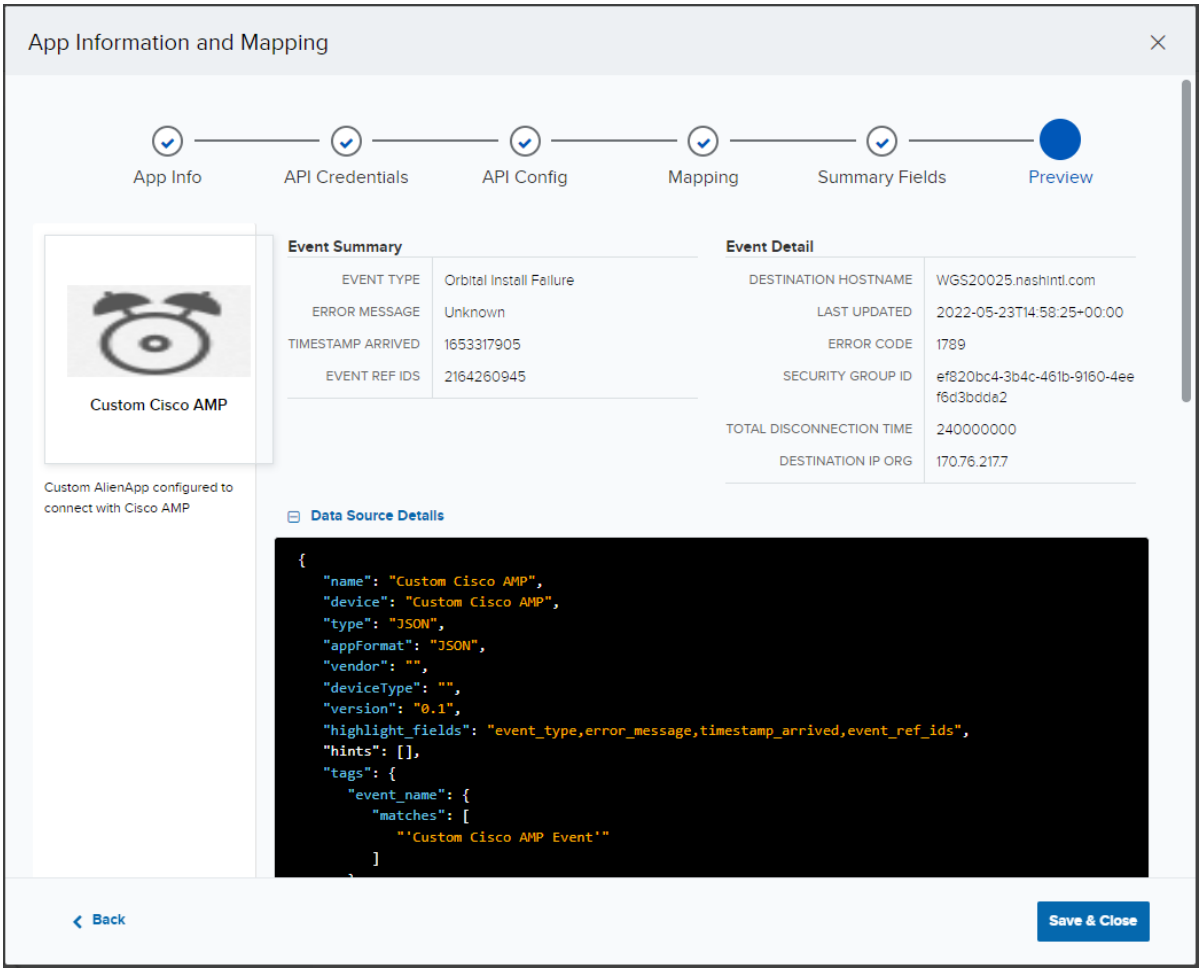
Important: In order for USM Anywhere to complete the field mapping configuration there must be sufficient events present for the product to map with. If you receive an "Events not found" error at this stage, you may have to stop configuration at this step and generate some events before resuming the configuration.

7. Select which log fields to include in the Event Details for events your new advanced BlueApp will generate.



Click **Save & Next** to continue.

8. Use the Preview screen to review your custom advanced BlueApp's configuration.



   You can use the Back button to navigate to any previous page and make changes.

9. Once you have finished all of the configuration steps for your custom advanced BlueApp, click **Save & Close** to create it.
   It will now be available to you under the My Apps tab of USM Anywhere.

Guides for Custom Advanced BlueApp Configuration

In addition to the many BlueApps offered by USM Anywhere, LevelBlue offers you the option of configuring an advanced BlueApp custom to your resources and the way you use them. With custom BlueApps, you can better monitor activity in your environment according to your needs.

The custom BlueApp feature is quite powerful, unlocking the ability to import events from almost any product or service that uses a REST API. To make this configuration process easy and approachable, LevelBlue offers configuration guides for the most oft-requested custom BlueApps, providing clear guidance on the exact configurations needed to set up authentication of your custom BlueApp.

https://intercom.help/usm-anywhere/en/articles/7061412-custom-alienapp-configuration-guides

Before getting started, you will need to ensure that you are able to generate the required authentication information from the application or service for which you are trying to create an application. The configuration guides LevelBlue provides endeavor to document the highest level of security available when connecting to your third party resource. For that reason, LevelBlue recommends that you follow the documented authentication configuration when setting up your custom BlueApp.

Note: If you don't find a guide for the application you need there, you can request one by following the instructions here.

To use a configuration guide to create your custom BlueApp

1. Go to https://intercom.help/usm-anywhere/en/articles/7061412-custom-alienapp-configuration-guides.
2. In the Configuration Guide list, locate the BlueApp template you want to follow and select it.
3. Open the PDF link on the Configuration Guide page for your selected BlueApp and save the file for your reference.
4. Within USM Anywhere, navigate to **Data Sources > BlueApps > Custom Apps**.
5. Select **Add Custom App** to begin creating a new custom BlueApp.
6. Follow the guidelines to configure each step of your custom BlueApp.
   The guide is designed to offer you the most security and robust functionality available. For that reason, we recommend following the configuration in the guide exactly as it is presented unless your environment necessitates that you make a change.
   - **App Info:** Provide a unique name, logo, and description for your custom BlueApp.
   - **API Credentials:** Configure your custom BlueApp with secure credentials to your third party resource.

- **API Configuration:** Represent the API configuration your custom BlueApp should expect from your third party resource.
- **Field Mapping:** Map important fields from your third party resource's API to their matching fields within USM Anywhere.
- **Summary Fields:** Select which fields will appear in the details page of events generated from your new custom BlueApp.

7. Once you have finished all of the configuration steps for your custom BlueApp, click **Save & Close** to create it.
   It will now be available to you under the My Apps tab of USM Anywhere.

Request for a New BlueApp or Update to an Existing BlueApp

LevelBlue builds or updates BlueApps at the request of customers for products and devices available to the general public. To take advantage of this, customers must have an active LevelBlue Support and Maintenance contract.

Important: This policy does not apply to BlueApps for custom software or devices.

See this list of BlueApps for information on the BlueApps included in USM Anywhere.

Before Submitting Your Request

The more information you can provide, the faster LevelBlue can build the BlueApp and the more accurate it will be. A complete request must include the following information:

- Product's vendor, model, and version.
- A description of the device and how you will connect to it, including the data acquisition method.
  This needs to be explained in great detail, these examples are not all inclusive: Syslog, Database, SNMP, Flat File, OSSEC Agent.

  Note: BlueApp development does not include DB query development or third party tool implementation that may be needed for log data extraction such as LogBinder.

- A description of the formatting of the logs. Select from the list of current BlueApps Supported Log Formats.

  Important: All syslog messages must conform with the RFC 3164 standard, which recommends the message to have three parts: PRI, HEADER, and MSG.

- A description of how you use the product, including which messages and which fields inside those messages provide the most relevance to your business.

  You may also want to consider using the product's default log settings in defining which fields to log. However, if a product has a particular logging configuration that you want the BlueApp to support, you should include that in your request.

- Specific log samples or database dumps from the relevant device. Your sample must contain at least 100 lines or 2 MB of data. The best way to collect log sample is to download the raw logs generated by the LevelBlue Generic Data Source on the asset receiving this log. See how to download raw logs from USM Anywhere.

  Important: When submitting log samples, all Personal Identifiable Information (PII) such as Social Security number, credit card numbers, or medical information must be removed or obfuscated from the samples.

- For best results, exclude any extraneous *noise* from the log samples, while still retaining all the data needed to differentiate the various events you want to capture with the BlueApp.
- If you need information other than the date, source, destination, username, and protocol extracted from the logs, specify this in your request, and provide an example. This helps us test the BlueApp to make sure it can successfully extract that data.
- Use case for the new BlueApp and the business value of the application or device to your organization. This information helps us assign a priority to your request.

After you have collected the information, click here to submit your request.