# Contents

AlienApps Overview ........................................................................................................... 5

AlienApps UI ..................................................................................................................... 7
  My Apps ....................................................................................................................... 7
  Available Apps ........................................................................................................... 9

AlienApps and Data Sources ............................................................................................ 12
  Auto Discovered Data Sources ................................................................................... 12
  Not Auto Discovered Data Sources ........................................................................... 12
  The AlienVault Generic Data Source ......................................................................... 13

Assign Assets to AlienApps ............................................................................................... 13
  AlienApps Supported Log Formats ............................................................................ 15

AlienApps Parser Syntax .................................................................................................... 16

Advanced AlienApps .......................................................................................................... 19
  AlienApp for AT&T Cybersecurity Forensics and Response ....................................... 21
  AlienApp for Box ......................................................................................................... 63
  AlienApp for Carbon Black EDR .................................................................................. 74
  AlienApp for Check Point ........................................................................................... 86
  AlienApp for Cisco AMP ............................................................................................. 93
  AlienApp for Cisco ASA ............................................................................................. 98
  AlienApp for Cisco Umbrella ...................................................................................... 106
  AlienApp for Cloudflare .............................................................................................. 124
  AlienApp for ConnectWise ......................................................................................... 138
  AlienApp for Fortinet FortiGate ............................................................................... 150
  AlienApp for Fortinet FortiManager ......................................................................... 156
  AlienApp for G Suite ................................................................................................. 163
  AlienApp for GSG Select ........................................................................................... 166
AlienApps Overview

AlienApps 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 AlienApps, you can monitor more of your security posture directly within USM Anywhere, including your cloud services like Microsoft Office 365 and Google G Suite. AlienApps 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 AlienApps for different data sources. In addition to translating raw log data into normalized events for analysis by USM Anywhere, some AlienApps 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.

AlienApps 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 a third-party vendor for immediate action. AlienApps with orchestration features are called Advanced AlienApps.
**Edition:** Some of the Advanced AlienApps are only available in the Standard and Premium editions of USM Anywhere. The following AlienApps are not available in the USM Anywhere Essentials edition:

- AlienApp for AT&T Cybersecurity Forensics and Response
- AlienApp for Carbon Black EDR
- AlienApp for Check Point
- AlienApp for Cisco AMP
- AlienApp for Cisco ASA
- AlienApp for Cisco Umbrella
- AlienApp for ConnectWise
- AlienApp for Fortinet FortiGate
- AlienApp for Fortinet FortiManager
- AlienApp for GSG Select
- AlienApp for Jira
- AlienApp for Microsoft Defender ATP
- AlienApp for Palo Alto Networks PAN-OS
- AlienApp for ServiceNow
- AlienApp for SpyCloud Dark Web Monitoring
- AlienApp for Zscaler

See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.
AlienApps UI

Go to Data Sources > AlienApps to open the AlienApps main page. Through this page, you can enable AlienApps, 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 AlienApps.
- **Events By Data Source**: Events correlated by AlienApps. The size of the bubbles depends on the number of issues.

You can see your apps in a list view (fullscreen) 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the AlienApp.</td>
</tr>
<tr>
<td>Sensors</td>
<td>Name of the sensor where the AlienApp has been configured.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the AlienApp.</td>
</tr>
<tr>
<td>Consumption</td>
<td>Data received by the AlienApp since deployment.</td>
</tr>
<tr>
<td>Sources</td>
<td>Number of data sources.</td>
</tr>
<tr>
<td>Data Last Consumed</td>
<td>Data received by the AlienApp since last consumption.</td>
</tr>
</tbody>
</table>

On either view, you can use the filters or search for a specific AlienApp.
You can click a tile to open the specific page for that AlienApp. Sometimes, at the bottom of the tile, you see information about the status of that AlienApp, as shown in the screenshot. You can click the tile to configure the needed data. See Advanced AlienApps 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 AlienApps in ascending or descending order.
- Search for an AlienApp by its name.
- Choose whether or not to include auto-discovered AlienApps
- Filter the AlienApps by these categories:
  - Cloud platform
  - Collection
  - Monitoring
  - Networking
  - Notification
  - Response
  - Security
  - Server

  The number between brackets displayed next to each filter indicates the number of total AlienApps 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 AlienApps and go to the previous or next pages.
AlienApps and Data Sources

AlienApps 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 AlienApps 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).

Auto Discovered Data Sources

In USM Anywhere, many AlienApps 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. USM Anywhere clearly indicates whether an AlienApp can auto-discover its data source in the user interface (UI). You can also use this list to find out if a data source is auto-discovered.

Not Auto Discovered Data Sources

Not all AlienApps accept hints, because some syslog messages only contain generic data. For hints to work, syslog messages must contain unique information. For this reason, USM Anywhere can neither automatically identify those data sources nor ready their syslog data. These AlienApps require a manual association between the asset forwarding the syslog messages and the AlienApp. See Assign Assets to AlienApps for detailed instructions.

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

**Important:** Assigning an AlienApp to an asset disables the usage of hints; therefore, only the assigned AlienApps are used to parse and normalize a log message. If you assign an AlienApp to an asset and that asset produces log messages to be processed by other AlienApps, you must manually assign each AlienApp, including the auto-discovered AlienApps, to the asset.
The AlienVault Generic Data Source

Occasionally, a log line cannot be matched by any AlienApps. 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 AlienVault 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 AlienVault Generic Data Source in the USM Anywhere User Guide for more information.

Assign Assets to AlienApps

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

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

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

**Important:** Assigning an AlienApp to an asset disables the usage of hints; therefore, only the assigned AlienApps are used to parse and normalize a log message. If you assign an AlienApp to an asset and that asset produces log messages to be processed by other AlienApps, you must manually assign each AlienApp, including the auto-discovered AlienApps, to the asset.

To assign an asset to an AlienApp

1. Go to Data Sources > AlienApps > Available Apps.
2. Look for the AlienApp 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 AlienApps Supported Log Formats for more information.

8. Click the ✔️ icon to confirm.

9. Click Done.

To remove an asset from an AlienApp

1. Go to Data Sources > AlienApps > Available Apps.
2. Look for the AlienApp 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 > AlienApps > Available Apps.
2. Look for the AlienApp 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.

AlienApps Supported Log Formats

Some AlienApps 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.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEF</td>
<td>ArcSight Common Event Format</td>
<td>CEF:Version</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
<td>2,398778306028,eni-abc,1.1.1.1,2.2.2.2,52392,443,6,11,1935,1461792267,1461792322,ACCEPT,OK</td>
</tr>
<tr>
<td>GELF</td>
<td>Graylog Extended Log Format</td>
<td>{ &quot;version&quot;: &quot;1.1&quot;, &quot;host&quot;: &quot;example.org&quot;, &quot;short_message&quot;: &quot;A short message&quot;, &quot;level&quot;: 5, &quot;_some_info&quot;: &quot;foo&quot; }</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
<td>{&quot;DateTime&quot;:1438189080000,&quot;UsersName&quot;:&quot;Dev&quot;,&quot;UsersEmail&quot;:&quot;<a href="mailto:dev@blah.com">dev@blah.com</a>&quot;,&quot;IP Address&quot;:&quot;1.1.1.1&quot;,&quot;Action&quot;:&quot;Test&quot;}</td>
</tr>
</tbody>
</table>
### Log Formats Supported by AlienApps (Continued)

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Sample Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key-Value</td>
<td>A key and value pair</td>
<td>id=&quot;0001&quot; severity=&quot;info&quot; name=&quot;http access&quot; action=&quot;pass&quot; method=&quot;GET&quot; srcip=&quot;1.1.1.1&quot; dstip=&quot;2.2.2.2&quot; user=&quot;myuser&quot;</td>
</tr>
<tr>
<td>LEEF</td>
<td>Log Event Extended Format</td>
<td>LEEF:Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LEEF:0</td>
</tr>
<tr>
<td>RegEx</td>
<td>Regular Expression</td>
<td>sshd[1097]: Failed password for invalid user from 1.1.1.1 port 43312 ssh2</td>
</tr>
<tr>
<td>Split</td>
<td>The fields are separated using a character other than comma</td>
<td>200</td>
</tr>
<tr>
<td>W3C</td>
<td>Extended Log File Format from W3C</td>
<td>#Fields: time cs-method cs-uri</td>
</tr>
<tr>
<td></td>
<td></td>
<td>00:34:23 GET /foo/bar.html</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
<td>&lt;Root&gt;&lt;EventID&gt;90060&lt;/EventID&gt;&lt;Priority&gt;4&lt;/Priority&gt;&lt;Message&gt;Application - End&lt;/Message&gt;&lt;Category&gt;AUDIT&lt;/Category&gt;&lt;/Root&gt;</td>
</tr>
</tbody>
</table>

### AlienApps Parser Syntax

AlienApps 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:
The following table includes each field and its description that a parser uses:
## Fields and Description Used by a Parser

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the parser.</td>
</tr>
<tr>
<td>type</td>
<td>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.</td>
</tr>
<tr>
<td>version</td>
<td>Version of the parser.</td>
</tr>
<tr>
<td>enrichmentScript</td>
<td>Specify the Lua script used to process a log line.</td>
</tr>
<tr>
<td>device</td>
<td>Data source that is sending the logs.</td>
</tr>
<tr>
<td>vendor</td>
<td>Data source vendor.</td>
</tr>
<tr>
<td>deviceType</td>
<td>Data source type (for example, firewall, router).</td>
</tr>
<tr>
<td>parentName</td>
<td>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.</td>
</tr>
<tr>
<td>parentVersion</td>
<td>Version of the parent parser.</td>
</tr>
<tr>
<td>app</td>
<td>Name displayed under Data Sources &gt; AlienApps.</td>
</tr>
<tr>
<td>hints</td>
<td>References to unique information within a syslog message that identify the data source sending the logs. AlienApps that contain hints will process the message when the information in the log message matches the criteria set within the parser. See AlienApps and Data Sources for more information.</td>
</tr>
<tr>
<td>highlight_fields</td>
<td>The most important fields shown in the principal event view.</td>
</tr>
<tr>
<td>properties</td>
<td>This field describes the different properties of the parser, depending on the type.</td>
</tr>
<tr>
<td>dictionaries</td>
<td>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.</td>
</tr>
<tr>
<td>tags</td>
<td>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.</td>
</tr>
<tr>
<td>rules</td>
<td>For regular expression (regex)-type parsers, there is a set of rules with these fields:</td>
</tr>
<tr>
<td></td>
<td>* name: name of the rule</td>
</tr>
<tr>
<td></td>
<td>* contains: pre-match filter</td>
</tr>
<tr>
<td></td>
<td>* regex: regular expression</td>
</tr>
<tr>
<td></td>
<td>* tags: tags to capture</td>
</tr>
</tbody>
</table>
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 AlienApps

Some AlienApps provide orchestration to automate your security operations, therefore they are called Advanced AlienApps. For example, if USM Anywhere finds data associated with a malicious website, orchestration rules might stipulate for this information be sent to a third-party application for immediate action. Both the AlienApp for Carbon Black EDR and the AlienApp for Cisco Umbrella provide this functionality.

**Edition:** Advanced AlienApps are available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.
For orchestration to work, USM Anywhere must connect to the third-party applications through their REpresentational State Transfer (REST) API. You need to configure each of your AlienApps separately. Find configuration instructions for the different AlienApps in these links:

- Configuring the AlienApp for AT&T Cybersecurity Forensics and Response
- Configuring the AlienApp for Box
- Configuring the AlienApp for Carbon Black EDR
- Configuring the AlienApp for Check Point
- Configuring the AlienApp for Cisco AMP
- Configuring the AlienApp for Cisco ASA
- Configuring the AlienApp for Cisco Umbrella
- Configuring the AlienApp for Cloudflare
- Configuring the AlienApp for ConnectWise
- Configuring the AlienApp for Fortinet FortiGate
- Configuring the AlienApp for G Suite
- Configuring the AlienApp for GSG Select
- Configuring the AlienApp for Jira
- Configuring the AlienApp for McAfee ePO
- Configuring the AlienApp for Microsoft Defender ATP
- Configuring the AlienApp for Office 365
- Configuring the AlienApp for Okta
- Configuring the AlienApp for Palo Alto Networks PAN-OS
- Configuring the AlienApp for Salesforce
- Configuring the AlienApp for ServiceNow
- Configuring the AlienApp for Sophos Central
- Configuring the AlienApp for SpyCloud Dark Web Monitoring
- Configuring the AlienApp for Zscaler
AlienApp for AT&T Cybersecurity Forensics and Response

The AlienApp for AT&T Cybersecurity Forensics and Response enables you to automate intrusion detection and response activities between USM Anywhere and your asset host systems. This AlienApp 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 AlienApp for AT&T Cybersecurity Forensics and Response is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for AT&T Cybersecurity Forensics and Response

To use the AlienApp for AT&T Cybersecurity 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 also supports credentials for Cisco IOS to support authenticated scans on those devices. This credential type is not used by the AlienApp for AT&T Cybersecurity Forensics and Response.

### Manage Credentials for Your Assets

Before you use the AlienApp for AT&T Cybersecurity 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 do not connect or the asset does not 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**.

![Credential Table]

<table>
<thead>
<tr>
<th>Asset</th>
<th>Type</th>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>credentials-name-2-master1</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-2-master2</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-3-master1</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-3-master2</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-4-master1</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-4-master2</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-5-master1</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-5-master2</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-6-master1</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-6-master2</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
</tbody>
</table>
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**

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

- **Cisco IOS Enable Password**: Use this option only for vulnerability scans on Cisco IOS devices.

  This requires level 15 privileges, similar to root, for running a vulnerability scan.

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

3. At the bottom of the dialog box, enter part of the asset name in the field.
   
   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.
After you select the asset, the dialog box displays the item at the top. If needed, you can enter text for another asset name and select it to assign multiple assets for the credential set.

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 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 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.
3. In the Choose Credentials drop-down list, select the credentials to use.
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 AlienApp 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.

3. In the dialog box, 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 group name, click the ✗ icon and select Assign Credentials.
3. In the Choose Credentials drop-down list, select the credentials to use.

![Assign Credentials to Asset Group]

Choose Credentials
Credentials will be applied to current members of this Asset Group and Assets added to the group later. Asset can be added automatically via Asset Group Rules or manually by adding Assets to Asset Group.

Credentials assigned directly to an Asset have higher priority than those assigned to an Asset Group.

credentials-name-1_d4dd-exec2

Edit Credentials
Create New Credentials

Note: If the needed credentials do not already exist, you can select Create New Credentials to define them in USM Anywhere. Select Edit Credentials if you want to modify any information.

4. Click Save.
Using the AlienApp for AT&T Cybersecurity Forensics and Response Actions

With the AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response actions to gather forensic information or make system changes on assets monitored in USM Anywhere.

Important: Running the AlienApp for AT&T Cybersecurity Forensics and Response actions requires that the target assets have assigned credentials that are suitable for administrative access to the host. See Configuring the AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response actions.

Forensic Profile Actions

The AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response also provides actions to launch a simple execution of that function. The table below describes what each action does:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Networking</td>
<td>Executes the Disable Networking enforcement function on the interfaces currently connected to the selected asset</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Get Active Directory Information</td>
<td>Executes the Get Active Directory (AD) Assets data collection function</td>
<td>Scheduled Job</td>
</tr>
<tr>
<td>Get Established Connections</td>
<td>Executes the Get Established Connections data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Get Users</td>
<td>Executes the Get Users data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Get Logged On Users</td>
<td>Executes the Get Logged On Users data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Get Processes with Hashes</td>
<td>Executes the Get Processes with Hashes data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Availability</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get Running Services</td>
<td>Executes the Get Running Services data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Get System Info</td>
<td>Executes the Get System Info data collection function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Executes the Shutdown enforcement function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Set Registry Key to String</td>
<td>Executes the Set Registry Key to String enforcement function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Set Registry Key to DWORD</td>
<td>Executes the Set Registry Key to DWORD enforcement function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
<tr>
<td>Launch Query</td>
<td>Executes the specified data collection or enforcement function</td>
<td>AlienApp for AT&amp;T Cybersecurity Forensics and Response page Event or Alarm Scheduled Job Orchestration Rule</td>
</tr>
</tbody>
</table>

See Defining a Launch Query Action
Running an Action

The AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response

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

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.

### AlienApp for AT&T Cybersecurity Forensics and Response App

<table>
<thead>
<tr>
<th>Collect Logs</th>
<th>Actions</th>
<th>Rules</th>
<th>Scheduling</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Registry Key to String</td>
<td>Sets a registry key to a String value</td>
</tr>
<tr>
<td>Get Established Connections</td>
<td>Retrieves a list of the opened connections with information about the port and the address involved.</td>
</tr>
<tr>
<td>Get Logged On Users</td>
<td>List the Logged On Users.</td>
</tr>
<tr>
<td>Get Processes With Hashes</td>
<td>Get the list of processes running in the system and the associated hash</td>
</tr>
<tr>
<td>Full Forensic Info</td>
<td>Get complete forensic info from an asset</td>
</tr>
<tr>
<td>Get Running Services</td>
<td>Get the list of services running in the system</td>
</tr>
<tr>
<td>Basic Forensic Info</td>
<td>Get basic forensic info from an asset</td>
</tr>
<tr>
<td>Get Registry Key to DWORD</td>
<td>Sets a registry key to a DWORD value</td>
</tr>
<tr>
<td>Disable Networking</td>
<td>Disable networking</td>
</tr>
<tr>
<td>Moderate Forensic Info</td>
<td>Get moderate forensic info from an asset</td>
</tr>
<tr>
<td>Get Users</td>
<td>List the local accounts in the system including privileges and last time they logged in</td>
</tr>
<tr>
<td>Launch Query</td>
<td>Launches a query or action against an asset</td>
</tr>
<tr>
<td>Get System Info</td>
<td>Gets information about the system including the Operating System version, Network interfaces and hostnames</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down the system.</td>
</tr>
</tbody>
</table>
This opens the Select Action dialog box.

7. If needed, select the sensor on which the AlienApp 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, AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response** for more information.
<table>
<thead>
<tr>
<th>System function</th>
<th>Collected data</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get System Info</td>
<td>Information about the target system, including the operating system version,</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>Windows</em></td>
<td>network interfaces, and hotfixes.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td>To execute this function using the Launch Query action, specify <code>getSystemInfo</code> as</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Users</td>
<td>A list of the local accounts in the target system, including privileges and the</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>Windows and Linux</em></td>
<td>last login time.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td>To execute this function using the Launch Query action, specify <code>getUsers</code> as</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td>the Query parameter.</td>
<td>Get Users</td>
</tr>
<tr>
<td>Get Running Services</td>
<td>A list of all currently running services on the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>Windows and Linux (non-RHEL)</em></td>
<td>To execute this function using the Launch Query action, specify <code>getRunningServices</code> as</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td>the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get Running Services</td>
</tr>
<tr>
<td>Get Running Services RedHat Linux</td>
<td>A list of all currently running services on the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>RHEL only</em></td>
<td>To execute this function using the Launch Query action, specify <code>getRunningServices.rhel</code> as the</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td>Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get Running Services</td>
</tr>
<tr>
<td>Get Services</td>
<td>A list of all services on the target system.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td><em>Windows</em></td>
<td>To execute this function using the Launch Query action, specify <code>getServices</code> as</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td>the Query parameter.</td>
<td></td>
</tr>
<tr>
<td>Get SMB Sessions</td>
<td>Information about the Server Message Block (SMB) sessions that are currently</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>Windows</em></td>
<td>established on the target system.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td>To execute this function using the Launch Query action, specify <code>getSMBSessions</code> as the Query parameter.</td>
<td></td>
</tr>
<tr>
<td>Get TCP Listening Ports</td>
<td>A list of the listening TCP ports on the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><em>Windows and Linux</em></td>
<td>To execute this function using the Launch Query action, specify <code>getTCPListeningPorts</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Get UDP Listening Ports</td>
<td>A list of the listening UDP ports on the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td>Windows and Linux</td>
<td>To execute this function using the Launch Query action, specify getUDPListeningPorts as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Established Connections</td>
<td>A list of the opened connections on the target system, including information about the port and the address.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td>Windows and Linux</td>
<td>To execute this function using the Launch Query action, specify getEstablishedConnections as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get Established Connections</td>
</tr>
<tr>
<td>Get Installed Applications</td>
<td>A list of the applications installed on the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td>To execute this function using the Launch Query action, specify getInstalledApplications as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get Installed Applications</td>
</tr>
<tr>
<td>Get Logged On Users</td>
<td>A list of the user accounts that are currently logged in to the target system.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td>To execute this function using the Launch Query action, specify getLoggedOnUsers as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get Logged On Users</td>
</tr>
<tr>
<td>Get Network Configuration</td>
<td>A list of the active network interfaces on the target system and their properties, including IP addresses and DHCP information.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td>To execute this function using the Launch Query action, specify getNetConfig as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Antivirus</td>
<td>Information about antivirus tools installed on the target system, including the status.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td>To execute this function using the Launch Query action, specify getAntivirus as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Get Start Up Items</td>
<td>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 <code>getStartUpItems</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get All Start Up Items</td>
<td>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 <code>getStartUpItemsAll</code> as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Processes</td>
<td>A list of processes running on the target system. To execute this function using the Launch Query action, specify <code>getProcesses</code> as the Query parameter.</td>
<td>Basic Forensic Info</td>
</tr>
<tr>
<td><strong>Windows and Linux</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Processes With Hashes</td>
<td>A list of processes running on the target system, along with the associated hash. To execute this function using the Launch Query action, specify <code>getProcessesWithHashes</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Shares</td>
<td>A list of the shared folders on the target system. To execute this function using the Launch Query action, specify <code>getShares</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Mapped Drives</td>
<td>A list of the mapped drives on the target system. To execute this function using the Launch Query action, specify <code>getMappedDrives</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Get Scheduled Tasks</td>
<td>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 <code>getScheduledTasks</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows and Linux</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Scheduled Jobs</td>
<td>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 <code>getScheduledJobs</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Installed Hotfixes</td>
<td>A list of the hotfixes installed on the target system. To execute this function using the Launch Query action, specify <code>getInstalledHotfixes</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Recent USB Drives</td>
<td>A list of the USB devices recently used on the target system. To execute this function using the Launch Query action, specify <code>getRecentUSBDrives</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Shadow Copies</td>
<td>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 <code>getShadowCopies</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Restore Points</td>
<td>A list of the restore points available on the target system. To execute this function using the Launch Query action, specify <code>getRestorePoints</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Get Prefetch Files</td>
<td>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 <code>getPrefetchFiles</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get DNS Cache</td>
<td>A list of the contents of the DNS client cache on the target system. To execute this function using the Launch Query action, specify <code>getDNSCache</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Failed DNS</td>
<td>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 <code>getFailedDNS</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get EventLog Info</td>
<td>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 <code>getEventLogInfo</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Firewall Config</td>
<td>The firewall configuration on the target system. To execute this function using the Launch Query action, specify <code>getFirewallConfig</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Audit Policy</td>
<td>The local audit policy information on the target system. To execute this function using the Launch Query action, specify <code>getAuditPolicy</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get IE History</td>
<td>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 <code>getIEHistory</code> as the Query parameter.</td>
<td>Moderate Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Get Typed URLs</td>
<td>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 <code>getTypedURLs</code> as the Query parameter.</td>
<td>Moderate Forensic Info Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Event Tracing for Windows (ETW) Sessions</td>
<td>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 <code>getETWSessions</code> as the Query parameter.</td>
<td>Moderate Forensic Info Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Windows Defender Information</td>
<td>Information about Windows Defender on the target system. To execute this function using the Launch Query action, specify <code>getWindowsDefenderStatus</code> as the Query parameter.</td>
<td>Moderate Forensic Info Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Drivers</td>
<td>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 <code>getDrivers</code> as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Recently Created Files</td>
<td>A list of files created on the target system within the last 24 hours. To execute this function using the Launch Query action, specify <code>getRecentlyCreatedFiles</code> as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Recent DLLs</td>
<td>A list of DLLs created on the target system within the last 24 hours. To execute this function using the Launch Query action, specify <code>getRecentDLLs</code> as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Recent Links</td>
<td>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 <code>getRecentLinks</code> as the Query parameter.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System function</td>
<td>Collected data</td>
<td>Actions</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Get Recent Executables Windows</td>
<td>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.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Compressed Files Windows</td>
<td>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.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Encrypted Files Windows</td>
<td>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.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Downloads Windows</td>
<td>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.</td>
<td>Full Forensic Info</td>
</tr>
<tr>
<td>Get Windows Defender Detections Windows</td>
<td>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.</td>
<td>Full Forensic Info</td>
</tr>
</tbody>
</table>
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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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**

The AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity Forensics and Response**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp 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.

![Query field](image)

---

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

### Scheduling a Forensics and Response Job

The AlienApp for AT&T Cybersecurity 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 Managing Jobs in the Scheduler in the USM Anywhere Deployment Guide for more information about working with scheduled jobs.
To schedule a Forensics and Response job

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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. If needed, select the sensor on which the AlienApp is enabled to display more options.
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 **Hour**, **Day**, **Week**, **Month**, or **Year**.

   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.

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 (default is Coordinated Universal Time [UTC]).

12. Click **Save**.
Launching a Forensics and Response Action from an Event or Alarm

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.

Malware Infection
Downloader
10 minutes ago

Select Action Create Rule

Alarm Details

<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATUS</td>
<td>Open</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>Malware</td>
</tr>
<tr>
<td>SUBCATEGORY</td>
<td>Downloader</td>
</tr>
<tr>
<td>MALWARE FAMILY</td>
<td>Blackbeard</td>
</tr>
<tr>
<td>HTTP HOSTNAME</td>
<td>qwertyport.com</td>
</tr>
<tr>
<td>SENSOR</td>
<td>VmWareSensor VMware</td>
</tr>
<tr>
<td>LABELS</td>
<td></td>
</tr>
<tr>
<td>INVESTIGATIONS</td>
<td></td>
</tr>
</tbody>
</table>
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

The AlienApp for AT&T Cybersecurity 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 AlienApp for AT&T Cybersecurity 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** and select **Response Action Rules**. Then click **Create 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

The AlienApp for AT&T Cybersecurity Forensics and Response translates the data it retrieves into normalized events for analysis. After you enable this AlienApp, 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 AlienApp for AT&T Cybersecurity 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 **AT&T Cybersecurity 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.
AlienApp for Box

The AlienApp 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 AlienApp for Box does the following:

- The AlienApp 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 AlienApp 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 AlienApp for Box also provides advanced security orchestration to launch or automate user-initiated actions against threats detected in your Box environment.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Box

Connected through the Box application programming interface (API), the AlienApp 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 AlienApp for Box. The USM Anywhere Sensor you want to use for the AlienApp for Box must have outbound connectivity to `api.box.com` on port 443.

**To enable the AlienApp to connect to the Box API**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp 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 appears, 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 AlienApp 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.
AlienApp for Box Orchestration

With the collection of your Box Enterprise account activities through the configured AlienApp 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 AlienApp may produce.

Examples of Alarms Generated from Box Data

<table>
<thead>
<tr>
<th>Intent</th>
<th>Strategy</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Compromise</td>
<td>Credential Abuse</td>
<td>Authentication to Box from a known malicious host</td>
</tr>
<tr>
<td>Ransomware Infection</td>
<td></td>
<td>Multiple uploads with known ransomware extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ransomware decryption instructions file upload</td>
</tr>
<tr>
<td>Exploitation &amp; Installation</td>
<td>Malware Infection</td>
<td>Executable downloaded from Box followed by malware activity</td>
</tr>
<tr>
<td>Delivery &amp; Attack</td>
<td>Brute Force Authentication</td>
<td>Successful login after a brute-force attack</td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td></td>
<td>Password spraying against Box</td>
</tr>
<tr>
<td>Known Malicious Infrastructure</td>
<td></td>
<td>File sent to a known malicious host</td>
</tr>
<tr>
<td>Reconnaissance &amp; Probing</td>
<td>Brute Force Authentication</td>
<td>Multiple login failures</td>
</tr>
<tr>
<td>Environmental Awareness</td>
<td>Access Control Modification</td>
<td>Two-factor authentication disabled</td>
</tr>
<tr>
<td>Account Manipulation</td>
<td></td>
<td>Multiple user accounts deleted</td>
</tr>
<tr>
<td>Anomalous User Behavior</td>
<td></td>
<td>Admin login from an unknown device</td>
</tr>
<tr>
<td>Credential Abuse</td>
<td></td>
<td>User login from two different countries in a short period</td>
</tr>
<tr>
<td>Defense Evasion - Cover Tracks</td>
<td></td>
<td>User account created and deleted in short period</td>
</tr>
<tr>
<td>Defense Evasion - Disabling Security Tools</td>
<td></td>
<td>Box security policy deleted</td>
</tr>
</tbody>
</table>
Examples of Alarms Generated from Box Data (Continued)

<table>
<thead>
<tr>
<th>Intent</th>
<th>Strategy</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Infection</td>
<td>Box detected a malicious file upload</td>
<td></td>
</tr>
<tr>
<td>Sensitive Data Disclosure</td>
<td>Box support access granted</td>
<td></td>
</tr>
</tbody>
</table>

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

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 AlienApp 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 AlienApp 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Box User</td>
<td>Run this action to inactivate the user account in Box.</td>
</tr>
<tr>
<td>Create Box Task</td>
<td>Run this action to create a task on a file in Box.</td>
</tr>
</tbody>
</table>

Note: Before launching a Box response action, you must have enabled and connected the AlienApp for Box to your Box Enterprise account. See Configuring the AlienApp 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 AlienApp 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 your 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 AlienApp for Box, select the sensor that you want to use for the action.
5. In the App Action list, select **Create Box Task**.

   This displays the options for the selected action. You must complete all the fields.

   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

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** and select **Response Action Rules**. Then click **Create 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.
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**.
AlienApp for Carbon Black EDR

The AlienApp 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 AlienApp combines USM Anywhere advanced threat detection and the ability to automatically isolate compromised systems with Carbon Black EDR.

**Edition:** The AlienApp for Carbon Black EDR is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Collecting Logs from Carbon Black EDR

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

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 AlienApp 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](https://cybersecurity.att.com/pricing) for instructions.

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

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

**Assign Assets to the AlienApp**

To help AlienApp 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 AlienApp

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.
AlienApp for Carbon Black EDR Orchestration

With the AlienApp 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 AlienApp 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 AlienApp for Carbon Black EDR orchestration actions require that the AlienApp is enabled on a deployed USM Anywhere Sensor with a configured integration to the Carbon Black EDR API. See Configuring the AlienApp 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 AlienApp 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 table below lists the available actions from the AlienApp.

**Actions for the AlienApp for Carbon Black EDR**

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolate hosts from an alarm</td>
<td>Run this app action directly from an alarm to send a request to Carbon Black EDR to isolate the associated endpoint(s).</td>
</tr>
<tr>
<td>Isolate hosts from an orchestration rule</td>
<td>Run this app 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.</td>
</tr>
</tbody>
</table>

**To view information about these actions in USM Anywhere**

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.
Configuring the AlienApp for Carbon Black EDR

When the AlienApp 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 AlienApp for Carbon Black EDR Orchestration for more information about the orchestration actions supported by the AlienApp 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 AlienApp for Carbon Black EDR.

To acquire the API token for Carbon Black EDR

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 AlienApp for Carbon Black EDR in USM Anywhere.

To enable the Carbon Black API connection

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 appears, 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.

### Launching a Carbon Black EDR Action from an Alarm

When you review the information in the Alarm Details, you can easily launch an action to send a request to Carbon Black EDR to isolate a compromised host. If you want to apply an action to similar events that occur in the future, you can also create an orchestration rule directly from the alarm.

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

   ![Select Action](image)

   - **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:

   ![Action Initiated](image)

   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

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 AlienApp for Carbon Black EDR must be enabled and configured. See Configuring the AlienApp 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**.

  ![Create rule for similar alarms](image)

- **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** and select **Response Action Rules**.
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

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 AlienApp 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 AlienApp 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.

### AlienApp for Check Point

The AlienApp for Check Point enables you to automate threat detection and response activities between USM Anywhere and Check Point. The AlienApp 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 AlienApp for Check Point is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

### Configuring the AlienApp for Check Point

#### Role Availability

- Read-Only
- Analyst
- Manager

### AlienApp for Check Point Requirements

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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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:](image) 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 appears, 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 AlienApp 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 AlienApp to the asset representing the Check Point device or management server’s IP address in USM Anywhere. If the AlienApp isn't assigned to any assets, the Check Point events will be handled by the AlienVault Generic Data Source, which will result in some of the data from the log not being properly parsed or associated with the AlienApp.

See [Assign Assets to AlienApps](#) for instructions on how to assign your assets to AlienApp for Check Point.
AlienApp for Check Point Orchestration

The AlienApp 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 AlienApp for Check Point orchestration actions to enforce protection based on the information associated with the event or alarm. The table below lists the available actions from the AlienApp.

**Actions for the AlienApp for Check Point**

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a threat indicator using a destination IP address</td>
</tr>
<tr>
<td>Add a threat indicator using a source IP address</td>
</tr>
<tr>
<td>Add a threat indicator using a destination domain</td>
</tr>
<tr>
<td>Add a threat indicator using a source domain</td>
</tr>
<tr>
<td>Add a threat indicator using a file hash</td>
</tr>
<tr>
<td>Add a threat indicator using a URL</td>
</tr>
<tr>
<td>Tag a destination IP address from an alarm, event, or rule in the UI</td>
</tr>
<tr>
<td>Tag a source IP address from an alarm, event, or rule in the UI</td>
</tr>
</tbody>
</table>

**To view information about these actions in USM Anywhere**

1. In USM Anywhere, go to *Data Sources > AlienApps*.
2. Click the *Available Apps* tab.
3. Search for the AlienApp, 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.
Launching a Check Point Response Action

When you review the information in the Alarm Details, Event Details, or Vulnerability Details pages, you can easily launch an action to set an indicator or tag the event in Check Point. If you want to apply an action to similar events that occur in the future, you can also Creating Check Point Response Action Rules directly from an action applied to an alarm, event, or vulnerability.

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 tag the alarm destination host or source host.
6. Enter the Check Point 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 Check Point Response Action Rules

Use the AlienApp 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.
AlienApp for Cisco AMP

The AlienApp for Cisco Advanced Malware Protection (AMP) enables you to automate threat detection and response activities between USM Anywhere and Cisco AMP. The AlienApp for Cisco AMP 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.

**Edition:** The AlienApp for Cisco AMP is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Cisco AMP

**Role Availability**

- **Read-Only**
- **Analyst**
- **Manager**

To use the AlienApp for Cisco Advanced Malware Protection (AMP) in USM Anywhere, you first need to log in to Cisco AMP to create the API credentials.

**To get the API credentials from Cisco AMP**

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

**Connecting the Cisco AMP App in USM Anywhere**

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

**To enable the AlienApp for Cisco AMP**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp API endpoints.
6. Enter your information into the following fields:
   - Client ID
   - API Key

7. In the **Event Type ID** field, you can specify the event types (separated by a comma) you want the AlienApp for Cisco AMP to collect.

   When the Event Type ID field is left blank, AlienApp for Cisco AMP collects all event types. See the [Cisco AMP documentation](#) for more details on event types.

8. Click **Save**.

9. Verify the connection.

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

   If the 🔄 icon appears, 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 AMP connection.

### AlienApp for Cisco AMP Orchestration

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use the information to trigger actions in your Cisco Advance Malware Protection (AMP) environment. Rather than manually isolating or unisolating hosts, you can use the AlienApp for Cisco AMP response actions to automatically respond to events detected in your USM Anywhere environment to isolate potential threats. The table below lists the available actions from the AlienApp.

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

#### Actions for the AlienApp for Cisco AMP

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolate Hosts Using FileHash</td>
<td>Run this action to isolate a host based on the FileHash identified.</td>
</tr>
<tr>
<td>Isolate Hosts Using Source IP</td>
<td>Run this action to isolate a host based on the source IP address identified.</td>
</tr>
<tr>
<td>Isolate Hosts Using Destination IP</td>
<td>Run this action to isolate a host based on the destination IP address identified.</td>
</tr>
</tbody>
</table>
Actions for the AlienApp for Cisco AMP (Continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unisolate Hosts Using FileHash</td>
<td>Run this action to unisolate a host based on the FileHash identified.</td>
</tr>
<tr>
<td>Unisolate Hosts Using Source IP</td>
<td>Run this action to unisolate a host based on the source IP address identified.</td>
</tr>
<tr>
<td>Unisolate Hosts Using Destination IP</td>
<td>Run this action to unisolate a host based on the destination IP address identified.</td>
</tr>
</tbody>
</table>

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

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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.

Launching a Cisco AMP Response Action

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

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to have your Cisco Advanced Malware Protection (AMP) instance to isolate or unisolate a host. If you want to apply an action to similar events that occur in the future, you can also create an orchestration rule after you apply the action.

To launch a Cisco AMP 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 AMP Action**.
5. Modify the information for the action for the following fields:
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 AMP Response Action Rules**

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

You can create orchestration rules in USM Anywhere that automatically trigger a Cisco Advanced Malware Protection (AMP) 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 AMP 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 AMP 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 AMP 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**.

### AlienApp for Cisco ASA

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

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

### Configuring the AlienApp for Cisco ASA

To use the AlienApp for Cisco Adaptive Security Appliance (ASA) in USM Anywhere, you need to perform the following steps in your Cisco ASA environment:
- Download and install the Cisco ASA Representational State Transfer (REST) API agent.
- Enable the REST API agent.
- Create a Cisco ASA user profile with a privilege level of 15 to be able to communicate with USM Anywhere.

**To install and configure the Cisco ASA REST API agent**

1. Follow the steps listed in *Install and Configure the ASA REST API Agent and Client* from the Cisco 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 AlienApp for Cisco ASA in USM Anywhere**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp API endpoints.

6. Enter the Cisco 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 ASA REST APIs, a ✓ icon displays in the Health column.

   If the ✗ icon appears, 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 ASA connection.
Forward Cisco ASA Syslog Messages to USM Anywhere

To fully integrate USM Anywhere with the AlienApp for Cisco ASA, you need to configure syslog forwarding in the Cisco 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 AlienApp to the asset representing the Cisco ASA device or management server’s IP address in USM Anywhere. If the AlienApp isn’t assigned to any assets, the Cisco ASA events will be handled by the AlienVault Generic Data Source, which will result in some of the data from the log not being properly parsed or associated with the AlienApp.

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

AlienApp for Cisco ASA Orchestration

With the AlienApp for Cisco 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 table below lists the available actions from the AlienApp.

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Source IP Address</td>
<td>Run this action to tag the source IP address in Cisco ASA from a rule, action, or event.</td>
</tr>
<tr>
<td>Tag Destination IP Address</td>
<td>Run this action to tag the destination IP address in Cisco ASA from a rule, action, or event.</td>
</tr>
</tbody>
</table>

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.
Launching a Cisco ASA Response Action

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 Cisco Adaptive Security Appliance (ASA) instance to create a new incident case based on that item. If you want to apply an action to similar events that occur in the future, you can also create an orchestration rule after you apply the action.

When reviewing an alarm originated from a Cisco ASA event, should you conclude that the Cisco ASA user account has been compromised, you can launch an action to inactivate the Cisco 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 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 ASA Action and enter the Cisco ASA Group Name and Group Description.
   
   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.

To launch a Cisco ASA action for an alarm

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

You can create orchestration rules in USM Anywhere that automatically trigger a Cisco 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 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 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 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 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 ASA cases.

Rule Condition

Select from property values below to create a matching condition. Learn more about creating rules.

<table>
<thead>
<tr>
<th>Property</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Type</td>
<td>Equals</td>
<td>system_event</td>
</tr>
<tr>
<td>Object type</td>
<td>Equals</td>
<td>AssetVulnerabilityStatus</td>
</tr>
</tbody>
</table>

CURRENT RULE

(packet_type == 'system_event' AND object_type == 'AssetVulnerabilityStatus')
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**.
AlienApp 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 AlienApp 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 AlienApp leverages two features from Cisco Umbrella:

- **Amazon Simple Storage Service (S3) log management**: The AlienApp collects Cisco Umbrella logs through an Amazon S3 bucket.
- **Enforcement API**: The AlienApp sends response actions to Cisco Umbrella based on the malicious records identified by USM Anywhere.

All three new Cisco Umbrella packages, *DNS Security Essentials*, *DNS Security Advantage*, and *Secure Internet Gateway (SIG) Essentials*, support both features. Therefore, AlienApp 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 AlienApp, you need to have the Platform package.

**Edition:** The AlienApp for Cisco Umbrella response actions are available in the Standard and Premium editions of USM Anywhere.

See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.
Collecting Logs from Cisco Umbrella

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 AlienApp for Cisco Umbrella provides a full scope of data and analysis within USM Anywhere.

**Important:** The AlienApp 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 the vendor website for more information about the Cisco Umbrella product packages.

**Amazon S3 Log Management**

Before the 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 article [https://support.umbrella.com/hc/en-us/articles/231248448-Cisco-Umbrella-Log-Management-in-Amazon-S3#self-bucket](https://support.umbrella.com/hc/en-us/articles/231248448-Cisco-Umbrella-Log-Management-in-Amazon-S3#self-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 10 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.

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. Select the USM Anywhere 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, `dnslogs/`).

10. For the Source Format option, select `raw`.

11. For the Plugin option, select `Cisco Umbrella`.

12. In the Schedule section, specify when USM Anywhere runs the job:
   
   a. Select the increment as **Hour, Day, Week, Month, or Year**.
   
   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.

   ```plaintext
   +-----------------------------+
   | Schedule                   |
   +-----------------------------+
   | Week                       |
   +-----------------------------+
   | Monday                     |
   | Tuesday                    |
   | Wednesday                  |
   | Thursday                   |
   | Friday                     |
   | Saturday                   |
   +-----------------------------+
   ```
Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.

![Schedule](image)

- **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 (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.

**AlienApp for Cisco Umbrella Orchestration**

With the AlienApp 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 AlienApp 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 AlienApp to send response actions, you must have a Cisco Umbrella package that supports the Enforcement API. See [the vendor website](https://www.cisco.com) for more information about the Cisco Umbrella product packages.

**Important:** Using the AlienApp for Cisco Umbrella orchestration actions requires that the AlienApp is enabled on a deployed USM Anywhere Sensor with a configured integration to your Cisco Umbrella account. See [Configuring the AlienApp for Cisco Umbrella](https://www.cisco.com) 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 AlienApp for Cisco Umbrella orchestration actions to enforce protection based on domains associated with the event or alarm. The table below lists the available actions from the AlienApp.

### Actions for the AlienApp for Cisco Umbrella

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report names found on an alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Report by a HTTP hostname found on an event</td>
<td>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.</td>
</tr>
<tr>
<td>Report by an URL found on an event</td>
<td>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.</td>
</tr>
<tr>
<td>Report by a DNS record found on an event</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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.
Configuring the AlienApp for Cisco Umbrella

When the AlienApp 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 AlienApp for Cisco Umbrella Orchestration for more information about the orchestration actions supported by the AlienApp 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 AlienApp.

**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:
   ```
Configuring the AlienApp for Cisco Umbrella Connection

After you create the Cisco Umbrella integration and copy the key value, you’re ready to establish the AlienApp for Cisco Umbrella connection in USM Anywhere. The USM Anywhere Sensor that you use to configure the AlienApp must have connectivity to the Umbrella Enforcement API at https://s-platform.api.opendns.com.

To enable the AlienApp for Cisco Umbrella

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 green icon displays in the Health column.

   If the red icon appears, 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.
Launching a Cisco Umbrella Action from an Alarm or Event

When you review the information in the Alarm Details or Event Details, you can easily launch an action to forward the associated domain information to Cisco Umbrella. If you want to apply an action to similar items that occur in the future, you can also create an orchestration rule directly from the alarm or event.

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.

---

Malware Infection
Downloader
10 minutes ago

Select Action  Create Rule

Alarm Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>High</td>
</tr>
<tr>
<td>STATUS</td>
<td>Open</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>Malware</td>
</tr>
<tr>
<td>SUBCATEGORY</td>
<td>Downloader</td>
</tr>
<tr>
<td>MALWARE FAMILY</td>
<td>Blackbeard</td>
</tr>
<tr>
<td>HTTP HOSTNAME</td>
<td>qwertyport.com</td>
</tr>
<tr>
<td>SENSOR</td>
<td>VmWareSensor</td>
</tr>
<tr>
<td></td>
<td>VMware</td>
</tr>
<tr>
<td>LABELS</td>
<td></td>
</tr>
<tr>
<td>INVESTIGATIONS</td>
<td></td>
</tr>
</tbody>
</table>
4. In the Select Action dialog box, select the Cisco Umbrella tile.

   ![Select Action dialog box with Cisco Umbrella tile selected]

   This displays the options for the selected response app. It automatically sets the App Action to Report names found on an alarm.

5. If you have more than one sensor installed, select the sensor where the AlienApp for Cisco Umbrella is enabled.

   ![Select Action dialog box with sensor and App Action options]

6. Click Run.

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

   ![Action Initiated dialog box with Cisco Umbrella and Report names found on an alarm]
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

The AlienApp 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 AlienApp for Cisco Umbrella must be enabled and configured for a deployed USM Anywhere Sensor. For more information, see **Configuring the AlienApp 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 AlienApp for Cisco Umbrella orchestration rule in USM Anywhere:

- **On the Rules tab of the AlienApp page**: This tab provides various tools that you can use to create and manage the orchestration rules that use the AlienApp 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 AlienApp 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** and select **Response Action Rules**. Then click **Create 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 > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 \[\text{icon}\] 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 \textbf{More} to display the optional multiple occurrence and window-length parameters.

\textbf{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:

• \textbf{AND}: Match all conditions
• \textbf{OR}: Match any one condition
• \textbf{AND NOT}: Exclude items matching all conditions after the first
• \textbf{OR NOT}: Include all items that do not match any conditions after the first

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

Click \textit{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.

\textbf{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.

\textbf{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**

<table>
<thead>
<tr>
<th>Role Availibility</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

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 AlienApp 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 AlienApp 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.
**AlienApp for Cloudflare**

The AlienApp 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 AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

**Configuring the AlienApp for Cloudflare**

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 AlienApp 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 AlienApp 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**

2. Copy the key value to be entered in USM Anywhere.
Enabling the AlienApp for Cloudflare API Connection

After you have your Cloudflare API key value, you're ready to enable the AlienApp for Cloudflare in USM Anywhere.

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 AlienApp 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 appears, 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.

**Scaling AlienApp 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 AlienApp 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 AlienApp 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 > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 **Settings > Scheduler**, enable the *Collect Cloudflare events* job that corresponds to that sensor.
9. Repeat step 4 through 8 to configure another 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

After you configure the AlienApp 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 AlienApp 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 AlienApp 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 AlienApp for Cloudflare.

**To verify the Cloudflare collection job**

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the **Filter by** option at the top of the list, enter **Cloudflare** to filter the displayed list for the Cloudflare App jobs.

![Job Scheduler](image-url)
Jobs that are currently enabled display the ☑ icon.

3. If the jobs for the sensor are not enabled, click the ☑ icon to toggle it.

<table>
<thead>
<tr>
<th>VMware</th>
<th>SpyCloud</th>
<th>Collect breach monitoring events</th>
<th>Collect breach monitoring events</th>
<th>Every day ...</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure</td>
<td>Cloudflare</td>
<td>Collect Cloudflare events</td>
<td>Collect Cloudflare events</td>
<td>Every 20 ...</td>
<td>-</td>
</tr>
<tr>
<td>VMware</td>
<td>Cloudflare</td>
<td>Collect Cloudflare events</td>
<td>Collect Cloudflare events</td>
<td>Every 20 ...</td>
<td>-</td>
</tr>
<tr>
<td>AWS-Sensor</td>
<td>Cloudflare</td>
<td>Collect Cloudflare events</td>
<td>Collect Cloudflare events</td>
<td>Every 20 ...</td>
<td>2 minutes ...</td>
</tr>
<tr>
<td>Hyper-V</td>
<td>Cloudflare</td>
<td>Collect Cloudflare events</td>
<td>Collect Cloudflare events</td>
<td>Every 20 ...</td>
<td>-</td>
</tr>
<tr>
<td>AWS-Sensor</td>
<td>Okta</td>
<td>Collect Okta events</td>
<td>Collect Okta events</td>
<td>Every 20 ...</td>
<td>4 minutes ...</td>
</tr>
</tbody>
</table>

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 AlienApp 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 AlienApp 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 > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, and then click the tile.
4. Click the **Rules** tab.

   **AlienApp for Cloudflare**
   
<table>
<thead>
<tr>
<th>Collect Logs</th>
<th>Actions</th>
<th>Rules</th>
<th>History</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Orchestration Rules</strong></td>
<td>USM Anywhere allows you to create and manage your own orchestration rules. Keep in mind that these rules verify whether they match with every new event coming into the system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Suggested Rules</strong></td>
<td>Filter all Cloudflare events with 200 OK status code</td>
<td>Reduces data consumption by filtering all Cloudflare events that have a 200 OK HTTP status code.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. 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 the suggested rule settings, if needed:

- Change the name of the rule.
- Add one or more Rule Condition items to narrow the scope for a matching event.
- Include a multiple occurrence parameter. (Click the More link to display the fields).

**Important:** If you choose to modify the conditions or occurrence parameters, 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.

7. Click **Save Rule**.

**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 Integration, Equals**, and **Cloudflare Enterprise Log Share Received** respectively, to create alarms that are specific to events from the AlienApp for Cloudflare.

AlienApp for Cloudflare Statistics

The AlienApp for Cloudflare presents a number of diagnostic statistics and related feedback, enabling you to assess the status of the AlienApp without having to delve into the sensor log.

The statistics reported on the AlienApp'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:

| Throttled Events | Approximately 9% of events are not being downloaded in order to maintain a maximum EPS of 1000 |

**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.

**Creating Cloudflare Response Action Rules**

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** and select **Response Action Rules**. Then click **Create 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 **delete** 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**.
Launching a Cloudflare Response Action

**Role Availability**  
[Read-Only] [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 AlienApp for Cloudflare response action to create a firewall action to block the suspicious upload.

The AlienApp 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Cloudflare action from an alarm</td>
<td>Run this action to create a Cloudflare firewall rule (Block, Challenge, JS Challenge, Allow, Log) from an alarm.</td>
</tr>
<tr>
<td>Create a Cloudflare action from an event</td>
<td>Run this action to create a Cloudflare firewall rule (Block, Challenge, JS Challenge, Allow, Log) from an event.</td>
</tr>
</tbody>
</table>

**Note:** Before launching a Cloudflare response action, you must have enabled and connected the AlienApp for Cloudflare to your Cloudflare Enterprise account. See Configuring the AlienApp 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 AlienApp 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 features 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.

   **To launch the Create Firewall Action for an event**

   1. Go to **Activity > Events**.
   2. Review the alarms generated on the Cloudflare events, and then click the event 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 AlienApp 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 features 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.
AlienApp for ConnectWise

Service management teams that use ConnectWise Manage can deploy and provision USM Anywhere through the ConnectWise Marketplace and manage those deployments for their customers. With configuration of the AlienApp 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 AlienApp for ConnectWise is available in the Standard and Premium editions of USM Anywhere.

It is also available when you sign up through the ConnectWise Marketplace and pay a monthly subscription to access an exclusive edition of USM Anywhere that is available only to ConnectWise MSP partners. After you complete the signup and registration process, follow the initial deployment process to activate and provision the USM Anywhere ConnectWise Edition instance (see USM Anywhere Deployment Process in the USM Anywhere Deployment Guide).

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

AlienApp for ConnectWise Requirements

Before you can configure and use the AlienApp 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 AlienApp for ConnectWise

When the AlienApp 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 AlienApp for ConnectWise Orchestration for more information about these AlienApp for ConnectWise response actions.

**Important:** Before you configure the AlienApp 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 AlienApp for ConnectWise Connection

To enable AlienApp for ConnectWise functions, you must configure a connection with your ConnectWise Manage environment and define the associated customer (managed company). This connection enables the AlienApp 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 appears, 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.
AlienApp for ConnectWise Orchestration

The AlienApp 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 table below lists the available actions from the AlienApp.

Actions for the AlienApp for ConnectWise

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add tickets to the Manage database</td>
<td>This action creates and updates the tickets from USM Anywhere alarms and vulnerabilities. USM Anywhere includes the <em>Update the Ticket database</em> job in the Scheduler, which executes this action every five minutes. When you configure the AlienApp for ConnectWise, this job is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Currently, configuration issues identified by USM Anywhere are not included in the job to create and update Manage service tickets.</td>
</tr>
<tr>
<td>Add configurations to the Manage database</td>
<td>This action updates the Configurations catalog in ConnectWise Manage to reflect the most recent asset scan by USM Anywhere. USM Anywhere includes the <em>Update Configurations catalog</em> job in the Scheduler, which executes this action every 60 minutes. When you configure the AlienApp for ConnectWise and select <strong>Automatically sync assets with Manage</strong>, this job is enabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If an asset that USM Anywhere previously discovered is no longer present in the most recent asset scan, the status changes to <em>inactive</em>. If it discovers the asset in another future scan, the status changes to <em>active</em>.</td>
</tr>
</tbody>
</table>

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 Managing Jobs in the Scheduler in the *USM Anywhere Deployment Guide* for more information.

**Important:** The AlienApp for ConnectWise must be enabled and connected to your Manage environment for successful execution of these jobs. See Configuring the AlienApp for ConnectWise for more information.
To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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.

**Accessing USM Anywhere Tickets in ConnectWise Manage**

With a successful connection to your ConnectWise Manage environment, the AlienApp 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 AlienApp 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.

<table>
<thead>
<tr>
<th>Configuration Name</th>
<th>Configuration Type</th>
<th>Status</th>
<th>Serial Number</th>
<th>Tag Number</th>
<th>Model Number</th>
<th>MAC Address</th>
<th>Site Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>License server</td>
<td>alien/vwzr/database</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>msnIX60</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>msnIX60+network/Use</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote - incfive</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-internal/108</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-internal/51</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-internal/201</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-internal/001</td>
<td>alien/vwzr/default</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote-internal</td>
<td>alien/vwzr/database</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

USM Anywhere and ConnectWise Manage UI Integration

With a successful connection to your ConnectWise environment, the AlienApp 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.
AlienApp for Fortinet FortiGate

The AlienApp for Fortinet FortiGate enables you to automate threat detection and response activities between USM Anywhere and the Fortinet FortiGate Next-Generation Firewall (NGFW). The AlienApp 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 AlienApp for Fortinet FortiGate 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.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Fortinet FortiGate

To use the AlienApp 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 all required values, 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 AlienApp in USM Anywhere.
Connecting the AlienApp for Fortinet FortiGate in USM Anywhere

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

To enable the AlienApp for Fortinet FortiGate

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp API endpoints.

6. Enter your information into the following fields:
   - FortiGate Firewall IP Address/Host Name
   - Port
   - 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 appears, 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 AlienApp 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 AlienApp has the same trusted certificate chain that are deployed on your firewall.

**AlienApp for Fortinet FortiGate Orchestration**

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 AlienApp 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 AlienApp for Fortinet FortiGate

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Source Address to Address Group</td>
<td>Run this action to add the source address to a group in your FortiGate environment.</td>
</tr>
<tr>
<td>Add Destination Address to Address Group</td>
<td>Run this action to add the destination address to a group in your FortiGate environment.</td>
</tr>
<tr>
<td>Add to Custom Category</td>
<td>Run this action to add the source address to a group in your FortiGate environment.</td>
</tr>
<tr>
<td>Add to Custom Category</td>
<td>Run this action to include the source address, destination address, or both to a custom group in your FortiGate environment.</td>
</tr>
</tbody>
</table>

**Note:** Before launching a FortiGate response action or creating a FortiGate response action rule, the AlienApp for Fortinet FortiGate must be enabled and connected to your FortiGate instance. See Configuring the AlienApp for Fortinet FortiGate for more information.

**To view information about these actions in USM Anywhere**

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.
Launching a FortiGate Response Action

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 an orchestration rule after you apply the action.

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

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 to create FortiGate cases.
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.

   ![Rule Condition](image)

   - 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**.

**AlienApp for Fortinet FortiManager**

The AlienApp for Fortinet FortiManager enables you to automate threat detection and response activities between USM Anywhere and the Fortinet FortiManager. The AlienApp 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 AlienApp for Fortinet FortiGate is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.
Warning: If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Fortinet FortiManager

To use the 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 AlienApp for Fortinet FortiManager in USM Anywhere

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

To enable the AlienApp for Fortinet FortiManager

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.
AlienApps 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 AlienApp 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. Click **Save**.

**Uploading a CA Certificate (Optional)**

If you leave the Require CA Certificate checkbox deselected, the AlienApp 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 AlienApp has the same trusted certificate chain that are deployed on your firewall.

**AlienApp for Fortinet FortiManager Orchestration**

As USM Anywhere surfaces events, alarms, and vulnerabilities, you can use 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 AlienApp for Fortinet FortiManager response actions to automatically manage your FortiManager firewall using information from your USM Anywhere environment.

**Example of alarms generated from the Fortigate AlienApp**

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Address to Static URL Filter</td>
<td>Run this action to add the source or destination address to a static URL filter in your FortiManager environment.</td>
</tr>
<tr>
<td>Add Address to Address Group</td>
<td>Run this action to add the destination address to a group in your FortiManager environment.</td>
</tr>
</tbody>
</table>
Example of alarms generated from the Fortigate AlienApp (Continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Custom Category</td>
<td>Run this action to add an address to a group in your FortiManager environment.</td>
</tr>
</tbody>
</table>

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, and then click the tile.
4. On the AlienApps page, click the **FortiManager** tile.
5. Click the **Actions** tab to display information for the supported actions.
6. Click the **History** tab to display information about the executed actions.

Launching a FortiManager Response Action

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

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 an orchestration rule](#) after you apply the action.

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**.
Creating FortiManager Response Action Rules

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 a 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 FortiManager cases.
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**.
AlienApp for G Suite

With the AlienApp 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 AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for G Suite

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

After you configure the connection between the AlienApp 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 AlienApp 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.
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 API console to support server-to-server interactions. For more information about server-to-server authentication in Google, refer to https://developers.google.com/accounts/docs/OAuth2ServiceAccount.

As you complete the following setup tasks, you must collect these items to complete the integration with the AlienApp for G Suite:

- Client identification (ID) for the service account
- User email for the login that you use to create the account
- 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 AlienApp for G Suite. Ask your Google administrator for these privileges.

First, create a service account. See the G Suite Administrator Help for instructions. Pay attention to these specifics:

- In Step 2: Enable the APIs, enable the Admin SDK.
- In Step 3: Create the service account, do the following:
  1. For key type, select **P12** and 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.
  3. Skip item 11-16 in the article and continue with the rest of this document.

Delegate domain-wide authority to the service account you just created. See the Google Identity Platform Guide for instructions. Pay attention to these specifics:

- In the One or More API Scopes field (step 6), enter https://www.googleapis.com/auth/admin.reports.audit.readonly and click Authorize.

⚠️ 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.
Connecting the AlienApp for G Suite

After you create the new service account in G Suite and enable the Admin 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 AlienApp for G Suite connection configuration might not be successful immediately if these resources are not yet accessible.

To enable the AlienApp for G Suite

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp.
   
   AlienApps 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 AlienApp API endpoints.

6. In the Service Client ID field, enter the unique 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. (Optional.) If using, click **Choose File** to upload the P12 private key file for the Google service
9. Click **Save**.

### AlienApp for GSG Select

The AlienApp for GSG Select 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 AlienApp for GSG Select can add the source or destination address to your blacklist.

**Edition:** The AlienApp for GSG Select is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

### Configuring the AlienApp for GSG Select

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

Before AlienApp for GSG Select can connect to USM Anywhere, you need to submit a Move, Add, Change, Delete (MACD) Change Request though the BusinessDirect Web Portal.
To acquire AT&T Global Security Gateway (GSG) Select 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-AlienApp 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 GSG Select API to USM Anywhere
1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.
   AlienApps 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 AlienApp 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 appears, 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.

**AlienApp for GSG Select Orchestration**

The AlienApp for GSG Select 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 AlienApp for GSG Select orchestration actions to enforce protection based on the information associated with the event or alarm.

**Actions for the AlienApp for GSG Select**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Blocked List</td>
<td>Add a source or destination to the Zscaler blocked list.</td>
</tr>
<tr>
<td>Add to Allowed List</td>
<td>Add a source or destination to the Zscaler allowed list.</td>
</tr>
<tr>
<td>Remove from Allowed List</td>
<td>Remove a source or destination from the Zscaler blocked list.</td>
</tr>
<tr>
<td>Add to Custom Category</td>
<td>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 <strong>Search for existing categories</strong> link to see if the IP address is currently associated with any categories. Click the <strong>URL Lookup</strong> 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.</td>
</tr>
</tbody>
</table>

**To view information about these actions in USM Anywhere**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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.
Launching a GSG Select Response Action

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to set an indicator or tag the event in Zscaler. 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 GSG Select 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 GSG Select 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.
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 GSG Select Response Action Rules

Use the AlienApp for GSG Select to access the GSG Select 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 GSG Select 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 GSG Select 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.

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Select from property values below to create a matching condition: Learn more about creating rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>![Add Condition] Add Group Of Conditions</td>
</tr>
<tr>
<td>Packet Type</td>
<td>Equals alarm</td>
</tr>
<tr>
<td>Category</td>
<td>Equals Malware</td>
</tr>
<tr>
<td>Malware Family</td>
<td>Equals FindPOS</td>
</tr>
</tbody>
</table>

**CURRENT RULE**

```
(packet_type == 'alarm' AND event_category == 'Malware' AND malware_family == 'FindPOS')
```

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.
AlienApp for Jira

The AlienApp 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 AlienApp 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 AlienApp for Jira connection to your Jira instance, you can simplify the response execution process for threats identified in USM Anywhere.

**Edition:** The AlienApp for Jira is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Jira

**Role Availability**

- Read-Only
- Analyst
- Manager

When the AlienApp 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 AlienApp for Jira Orchestration for more information about the response actions supported by the AlienApp for Jira.

**Important:** The AlienApp for Jira integration works with the Cloud deployment of Jira Service Desk and Jira Software. The Server deployment (self-managed) is not currently supported.

AlienApp for Jira Requirements

Before you configure the AlienApp 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 AlienApp 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 AlienApp 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 https://confluence.atlassian.com/cloud/api-tokens-938839638.html 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 AlienApp 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.
AlienApps 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 AlienApp API endpoints.

6. Specify the connection information for Jira:

   ![Configure API](image)

   - **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.

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 appears, 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.

AlienApp for Jira Orchestration

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 AlienApp 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 table below lists the available actions from the AlienApp.

**Actions for the AlienApp for Jira**

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new issue from an alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new issue from a vulnerability</td>
<td>Run this action to generate a new Jira issue directly from a vulnerability. This action is available when you launch a response action directly from a vulnerability.</td>
</tr>
<tr>
<td>Create a new issue from an event</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new issue from event based orchestration rule</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 AlienApp for Jira must be enabled and connected to your cloud-based Jira instance. See Configuring the AlienApp for Jira for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.

### AlienApp for Jira

<table>
<thead>
<tr>
<th>Collect Logs</th>
<th>Actions</th>
<th>Rules</th>
<th>History</th>
<th>Issues</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**History**

<table>
<thead>
<tr>
<th>EVENT ACTION</th>
<th>FINISHED</th>
</tr>
</thead>
<tbody>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 03:13 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 03:25 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 11:01 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 11:02 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 03:25 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 03:26 PM</td>
</tr>
<tr>
<td>apps_manager,worker main JOB</td>
<td>Wed Dec 11 2019, 03:27 PM</td>
</tr>
</tbody>
</table>

1-10 of 11

< Prev | 1 | 2 | Next >

### Launching a Jira Response Action

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can launch an action to send a request to your cloud-based Jira instance to create a new issue based on that item. If you want to apply an action to similar items that occur in the future, you can also create an orchestration rule directly from the applied action.

**Note:** Before launching a Jira response action, the AlienApp for Jira must be enabled and connected to your Jira instance. See Configuring the AlienApp 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 AlienApp for Jira, use the Select Sensor option to set the sensor that you want to use for the rule.

6. Define the information included in the new Jira issue:
   - **Summary**: 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.

7. 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 AlienApp for Jira.

8. 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.

9. 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

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.

Note: Before launching a Jira response action or creating a Jira orchestration rule, the AlienApp for Jira must be enabled and connected to your cloud-based Jira instance. For more information, see Configuring the AlienApp for Jira.

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.

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 and select Response Action Rules. Then click Create 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 AlienApp 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

After the AlienApp 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp 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 AlienApp 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.
AlienApp for McAfee ePO

The AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for McAfee ePO

The AlienApp 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 AlienApp 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 AlienApp for McAfee ePO uses SQL Server authentication over Windows Authentication.

Creating a Scheduler Job for McAfee ePO

The AlienApp 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 Managing Jobs in the Scheduler in the **USM Anywhere Deployment Guide** for more information about working with scheduled jobs.
To schedule a McAfee ePO job

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, and then click the tile.
4. Click the Scheduling tab.
5. Enable an existing job or click New Job.

This opens the Schedule New Job dialog box with the options defined for an AlienApp 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. 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.

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

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

**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 (default is Coordinated Universal Time [UTC]).

9. **Click Save.**

After the scheduled job runs, you should start seeing new events in USM Anywhere originating from the ePO server SQL database.

**AlienApp 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.

**Edition:** The AlienApp for Microsoft Defender ATP is available in the Standard and Premium editions of USM Anywhere.

See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.
Important: Because the AlienApp for Microsoft Defender ATP can only act on events received from Azure, you also need to configure log collection from Azure Event Hubs. See Collect Logs from Azure Event Hubs and follow the process documented on that page to set up Azure log collection.

Configuring the AlienApp for Microsoft Defender ATP

Before you configure the AlienApp 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

Important: Because the AlienApp for Microsoft Defender ATP can only act on events received from Azure, you also need to configure log collection from Azure Event Hubs. See Collect Logs from Azure Event Hubs and follow the process documented on that page to set up Azure log collection.

Microsoft Defender ATP Configurations

To set up the AlienApp 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. See the Microsoft Defender ATP setup documentation for full details on the steps.

To enable the AlienApp for Microsoft Defender ATP

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 appears, 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.

AlienApp for Microsoft Defender ATP Orchestration

The AlienApp 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 AlienApp for Microsoft Defender ATP orchestration actions to enforce protection based on the information associated with the event or alarm. The table below lists the available actions from the AlienApp.

### Actions for the AlienApp for Microsoft Defender ATP

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine a file</td>
<td>Quarantine the file that appears according to the rule, or the file in the event action, and delete it from the machine. The file name, file path, and the SHA1 of the file are displayed when this action is selected.</td>
</tr>
<tr>
<td>Isolate Machine by ID</td>
<td>Isolates the machine based on the details of the event or rule conditions.</td>
</tr>
<tr>
<td>Unisolate Machine by ID</td>
<td>Unisolates the machine based on the details of the event or rule conditions.</td>
</tr>
</tbody>
</table>
To view information about these actions in USM Anywhere

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.

Launching a Microsoft Defender ATP Response Action

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to set an indicator or tag the event in Microsoft Defender Advanced Threat Protection (ATP). If you want to apply an action to similar events that occur in the future, you can also Creating Microsoft Defender ATP Response Action Rules directly from an action applied to an alarm, event, or vulnerability.

To launch a Microsoft Defender ATP 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 Microsoft Defender ATP tile.
5. For the App Action, select the action you want to launch.
   - 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

Use the AlienApp 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.

![Rule Condition dialog box]

- 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.
AlienApp for Office 365

With the AlienApp 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 AlienApp 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 AlienApp for Office 365. You can use any deployed sensor for the AlienApp connection.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

AlienApp for Office 365 Requirements

Before you can configure and use the AlienApp for Office 365, you must make sure that your Microsoft Office 365 environment is set up to support Office 365 Management API calls through Microsoft Azure Active Directory (AD) and audit log search.

**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

AlienApp for Office 365 configuration includes creating an AD application in Azure AD. This application securely authenticates the AlienApp for Office 365 so that it can access and collect the data according to the services and permission levels that 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.

When Azure AD is associated with your Office 365 account, you can use the management portal in Azure to manage users, roles, and apps:

- If you already have an Azure subscription, follow Microsoft's instructions to associate your Office 365 subscription with it.
- If you do not have an Azure subscription, follow Microsoft's instructions to create one and associate your Office 365 subscription with it.

### Audit Log Search

Office 365 audit logging records almost every major 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. This can be used to compare the events generated in USM Anywhere using the AlienApp 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 logs actions performed by mailbox owners, delegates, and administrators. Mailbox auditing in Office 365 is not mandatory for log collection using the AlienApp for Office 365, but it is turned on by default starting in 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:

```powershell
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,UpdateInboxRule
```

**Configuring the AlienApp for Office 365**

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 AlienApp 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 dashboards become available in the Dashboards menu (according 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.

This integration requires connectivity between your USM Anywhere Sensor and the Office 365 Management Activity API. If you have an Azure Sensor deployed in your Azure subscription, you should use this sensor to configure the AlienApp. 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**

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Endpoint</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>443</td>
<td><a href="https://login.windows.net/">https://login.windows.net/</a></td>
<td>Authentication for your Office 365 account</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td><a href="https://manage.office.com/api/v1.0/">https://manage.office.com/api/v1.0/</a></td>
<td>Queries to retrieve log data from the Office 365 Management Activity API</td>
</tr>
</tbody>
</table>

Before you configure the AlienApp for Office 365, make sure that you have fulfilled the requirements in your Office 365 account for this integration.
To configure the AlienApp for Office 365

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, and then click the tile.
4. Click the Instructions tab.
5. Follow the instructions on the page to register the AlienApp for Office 365 in Azure, and then copy the Application (client) ID and Directory (tenant) ID.
   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 AlienApp.

   AlienApps 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 AlienApp API endpoints.
9. Enter the copied IDs in the Tenant ID and Application ID fields.
10. Click Save.
11. 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 appears, 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.

12. In the USM Anywhere main menu, go to **Settings > Scheduler** and search for the collection job for Office 365.

13. Enable the job if it is not already enabled.

**Important:** The AlienApp 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 AlienApp 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 AT&T Cybersecurity. You can observe the latency by comparing the Time Received ISO8601 and Time Created ISO8601 fields of an Office 365 event in USM Anywhere.
<table>
<thead>
<tr>
<th>APP ID</th>
<th>office-365</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS FUZZIED</td>
<td>false</td>
</tr>
<tr>
<td>CLOUD APP</td>
<td>office-365</td>
</tr>
<tr>
<td>TIME RECEIVED</td>
<td>Wed, Sep 05 2018, 11:20 AM AEST</td>
</tr>
<tr>
<td>WAS GUESSED</td>
<td>false</td>
</tr>
<tr>
<td>HAS ALARM</td>
<td>true</td>
</tr>
<tr>
<td>EVENT HASH</td>
<td></td>
</tr>
<tr>
<td>DATA SOURCE</td>
<td>Exchange</td>
</tr>
<tr>
<td>TIME RECEIVED ISO8601</td>
<td>2018-09-05T01:20:01.541Z</td>
</tr>
<tr>
<td>APP NAME</td>
<td>office-365</td>
</tr>
<tr>
<td>USED HINT</td>
<td>false</td>
</tr>
<tr>
<td>PACKET TYPE</td>
<td>log</td>
</tr>
<tr>
<td>SUPPRESSED</td>
<td>false</td>
</tr>
<tr>
<td>USER RESOURCE</td>
<td></td>
</tr>
<tr>
<td>REPORTING DEVICE VERSION</td>
<td>1</td>
</tr>
<tr>
<td>TRANSIENT</td>
<td>false</td>
</tr>
<tr>
<td>TIME CREATED ISO8601</td>
<td>2018-09-04T12:49:58.000Z</td>
</tr>
<tr>
<td>DATA SOURCE TYPE</td>
<td>Mail Server</td>
</tr>
<tr>
<td>NEEDS ENRICHMENT</td>
<td>true</td>
</tr>
<tr>
<td>IN ALARMS</td>
<td></td>
</tr>
</tbody>
</table>
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. For detailed information about log collection and aggregation by the Microsoft Activity API, refer to this Microsoft article.

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. For a table listing the time delays of different services in Office 365, refer to this Microsoft article. However, if you observe delays to be more than 5 days, it could indicate a potential issue. Microsoft advises to check the Service Health Dashboard or open a ticket with Microsoft support.

Office 365 UserLoggedIn Event Discrepancy

When using the AlienApp for Office 365, you may see successful login events when the user actually fails to log in. For example:

![UserLoggedIn Event Discrepancy Example](image-url)

- **USER**: [User Name]
- **PLUGIN**: Office 365 Azure AD [0.14]
- **SENSOR**: [Sensor Name]
- **AUTHENTICATION MODE**: Login:login
- **REQUEST USER AGENT**: [Agent Name]
- **SECURITY GROUP NAME**: A regular user.
- **APPLICATION**: AzureActiveDirectory
- **EVENT OUTCOME**: Success
- **AUDIT REASON**: User:AccountNotFound
- **DESTINATION FQDN**: office365.com
This is not a mistake in the AlienApp, 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-xxxxxxxxxxxxxx",
    "LogonError": "UserAccountNotFound"
}
```

AT&T Cybersecurity 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:

```
Data Source Plugin: Office 365 Azure AD  
Event Name: UserLoggedIn  
Audit Reason: [ No Value ]
```

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 AlienApp 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 AlienApp 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. AT&T Cybersecurity 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.
The AlienApp for Okta provides deep security monitoring for single sign-on (SSO) and multi-factor 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 AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

### Configuring the AlienApp for Okta

After you configure the connection between the AlienApp 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 AlienApp 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*.

![Create Token dialog box](image)

Okta generates the unique token and displays the value in the dialog box.

![Create Token dialog box](image)

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.

![Token list](image)
Enable the AlienApp for Okta API Connection

After you generate an Okta API token and copy the value, you’re ready to enable the AlienApp in USM Anywhere.

To enable the AlienApp for Okta

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

AlieanApps 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 AlienApp 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 appears, 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.
AlienApp for Palo Alto Networks PAN-OS

The AlienApp 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 AlienApp 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 AlienApp for Palo Alto Networks PAN-OS 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.

Warning: If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Collecting Logs from Palo Alto Networks

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. AlienApp 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. 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.

2. 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.

### AlienApp for Palo Alto Networks PAN-OS Orchestration

The AlienApp 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 AlienApp 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 AlienApp for Palo Alto Networks PAN-OS orchestration actions requires that the AlienApp is enabled on a deployed USM Anywhere Sensor with configured integration to your Palo Alto Networks product. See [Configuring the AlienApp 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 AlienApp for Palo Alto Networks PAN-OS orchestration actions to enforce protection based on the information associated with the event or alarm. The table below lists the available actions from the AlienApp.

### Actions for AlienApp for Palo Alto Networks PAN-OS

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Destination IP Address from Rule</td>
<td>Run this action to tag destination IP Address in the connected Palo Alto Networks device.</td>
</tr>
<tr>
<td>Tag Destination IP Address to Dynamic Address Group from Rule</td>
<td>Run this action to tag destination IP Address and add it to a Dynamic Address Group in the connected Palo Alto Networks device.</td>
</tr>
<tr>
<td>Tag Source IP Address from Rule</td>
<td>Run this action to tag source IP Address in the connected Palo Alto Networks device.</td>
</tr>
<tr>
<td>Tag Source IP Address to Dynamic Address Group from Rule</td>
<td>Run this action to tag source IP Address and add it to a Dynamic Address Group in the connected Palo Alto Networks device.</td>
</tr>
</tbody>
</table>
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 [[[Undefined variable Anywhere.AppsPaloAlto]]] 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.
Configuring the AlienApp for Palo Alto Networks PAN-OS

When the AlienApp 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 AlienApp for Palo Alto Networks PAN-OS, see AlienApp for Palo Alto Networks PAN-OS Orchestration.

**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 AlienApp 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.

AlienApp 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**

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 AlienApp 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 AlienApp 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 AT&T Cybersecurity Technical Support for assistance.

**To configure the connection for PAN-OS**

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp 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.

Configure API

<table>
<thead>
<tr>
<th>Sensor</th>
<th>VmWareSensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or hostname</td>
<td>IP address or hostname</td>
</tr>
<tr>
<td>Validate HTTPS host name</td>
<td></td>
</tr>
<tr>
<td>Require CA certificate</td>
<td></td>
</tr>
<tr>
<td>CA certificate</td>
<td>CA certificate</td>
</tr>
<tr>
<td>Admin Name</td>
<td>Admin Name</td>
</tr>
</tbody>
</table>

**API key**

![Change API key button]

7. Click **Save**.

**Uploading a CA Certificate**

If you leave the Require CA Certificate checkbox deselected, the AlienApp 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 AlienApp 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 AlienApp.

**Launching a Palo Alto Networks Action from an Alarm or Event**

When you review the information in the Alarm Details or Event Details, you can easily launch an action to send a tag request to the Palo Alto Networks PAN-OS API. If you want to apply an action to similar events that occur in the future, you can also create an orchestration rule directly from an 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Priority</strong></td>
<td>High</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Open</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>Malware</td>
</tr>
<tr>
<td><strong>Subcategory</strong></td>
<td>Downloader</td>
</tr>
<tr>
<td><strong>Malware Family</strong></td>
<td>Blackbeard</td>
</tr>
<tr>
<td><strong>HTTP Hostname</strong></td>
<td>qwertyport.com</td>
</tr>
<tr>
<td><strong>Sensor</strong></td>
<td>VmWareSensor</td>
</tr>
<tr>
<td><strong>VMware</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Labels</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Investigations</strong></td>
<td></td>
</tr>
</tbody>
</table>
4. In the Select Action dialog box, select the **Palo Alto** tile.

5. For the App Action, select the action you want to launch.
   
   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

Use the AlienApp 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** and select **Response Action Rules**. Then click **Create 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.

![Create Response Action Rule](image)

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.

![Rule Condition](image)

- 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**.
Viewing Alarms with Applied Palo Alto Response Actions

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 AlienApp for Palo Alto Networks PAN-OS executes a response action for an alarm, it automatically applies the Palo Alto label to it. You can select this label as a filter so that a page displays data for only the items related to an AlienApp for Palo Alto Networks PAN-OS response action.

To view alarms with applied Palo Alto 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 Palo Alto.

   ![Search & Filters panel with Labels filter]

   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.

AlienApp for Salesforce

The AlienApp 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 AlienApp for Salesforce is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** The AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Salesforce

To use the AlienApp 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 recommended 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 AlienApp 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.

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)


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. AT&T Cybersecurity 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 AlienApp for Salesforce**

1. In USM Anywhere, go to **Data Sources > AlienApps**.

2. Click the **Available Apps** tab.

3. Search for the AlienApp, 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 AlienApp.

AlienApps 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 AlienApp 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 AlienApp for Salesforce to collect.

The AlienApp 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, DocumentAttachmentDownloads, 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 appears, 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.
AlienApp for Salesforce Orchestration

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 AlienApp 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 table below lists the available actions from the AlienApp.

### Actions for the AlienApp for Salesforce

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Salesforce Case</td>
<td>Run this action to generate a new Salesforce case from an alarm, event, response action, or vulnerability.</td>
</tr>
</tbody>
</table>

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 AlienApp for Salesforce must be enabled and connected to your Salesforce instance. See [Configuring the AlienApp for Salesforce](#) for more information.

To view information about these actions in USM Anywhere

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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.
Launching a Salesforce Response Action

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 Salesforce instance to create a new incident case based on that item. If you want to apply an action to similar events that occur in the future, you can also create an orchestration rule after you apply the action. Salesforce events are updated on an hourly basis.

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

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**.
AlienApp for ServiceNow

Using the AlienApp for ServiceNow, you can streamline incident response activities by automatically opening ServiceNow incident tickets in response to threats detected by USM Anywhere. Upon execution of the action, USM Anywhere generates the ServiceNow issue ticket and populates the ServiceNow ticket's Short description and Description fields with details from USM Anywhere.

**Edition:** The AlienApp for ServiceNow is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.
Configuring the AlienApp for ServiceNow

To enable the AlienApp for ServiceNow actions within USM Anywhere, you must configure the AlienApp 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 AlienApp for ServiceNow Orchestration for more information about using this functionality.

AlienApp for ServiceNow Requirements

You or your ServiceNow administrator must create a user account in your ServiceNow instance to be used by the 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 Aggregate API. If you are using the ServiceNow Security Incident Response (SIR) application and want the AlienApp 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 AlienApp for ServiceNow to access your ServiceNow instance. See ServiceNow production 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 AlienApp for ServiceNow and the history are displayed in the USM Anywhere UI according to this username. By using an exclusive user account, this information will include only the information that is related to USM Anywhere Alarm, Vulnerability, and Event response.

If you are a service provider or enterprise that manages more than one USM Anywhere instance, you can configure the AlienApp 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 differentiate them in the ServiceNow UI and the history and incident information displayed in USM Anywhere reflects only that instance.

Before you configure the AlienApp 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 AlienApp to perform CRUD operations using the ServiceNow Table and Aggregate REST APIs.

To configure the connection

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp 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 appears, 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.

**AlienApp for ServiceNow Orchestration**

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 AlienApp 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 table below lists the available actions from the AlienApp.

**Actions for AlienApp for ServiceNow**

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new incident from an alarm</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new incident from a vulnerability</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new incident from an event</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new incident from event based orchestration rule</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 AlienApp for ServiceNow must be enabled and connected to your ServiceNow instance. See Configuring the AlienApp for ServiceNow for more information.
To view information about these actions in USM Anywhere

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.

Launching a ServiceNow Response Action

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 ServiceNow instance to create a new incident ticket based on that item.

Note: Before launching a ServiceNow response action, the AlienApp for ServiceNow must be enabled and connected to your ServiceNow instance. See Configuring the AlienApp for ServiceNow for more information.

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 AlienApp 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 AlienApp 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 AlienApp populates the name of the alarm, event, or vulnerability.

- **Description**: This field contains information used to respond to the incident. By default, the AlienApp 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

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.

<i>Note: Before creating a ServiceNow response action rule, the AlienApp for ServiceNow must be enabled and connected to your ServiceNow instance. See Configuring the AlienApp for ServiceNow for more information.</i>

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 <i>USM Anywhere User Guide</i> for more information about managing orchestration rules.

In the left navigation menu, go to Settings > Rules and select Response Action Rules. Then
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 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 AlienApp.

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. The field will suggest autocomplete options as you type the username.

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. In the confirmation dialog box, click **OK**.

**Managing Your ServiceNow Incidents**

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

After the AlienApp 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 > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp**.

   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.

---

**Notes**

**Watch list**

**Work notes list**

---

**USM Anywhere™ AlienApps™ Guide**
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 AlienApp 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 AlienApp 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.

<table>
<thead>
<tr>
<th>Sort By: Time Created</th>
<th>LABELS</th>
<th>ALARM STATUS</th>
<th>SOURCES</th>
<th>PRIORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Infection Malicious SSL Certificate 2 hours ago</td>
<td>ServiceNow</td>
<td>Open</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Network Access Control Modification AWS EC2 Security Group Modified 2 hours ago</td>
<td>ServiceNow</td>
<td>Open</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Malware Infection Malicious SSL Certificate 4 hours ago</td>
<td>ServiceNow</td>
<td>Open</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Brute Force Authentication Successful Authentication After Brute Force 18 hours ago</td>
<td>ServiceNow</td>
<td>Open</td>
<td></td>
<td>Medium</td>
</tr>
</tbody>
</table>
AlienApp for Sophos Central

The AlienApp 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 AlienApp 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 AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for Sophos Central

<table>
<thead>
<tr>
<th>Role Availability</th>
<th>Read-Only</th>
<th>Analyst</th>
<th>Manager</th>
</tr>
</thead>
</table>

With a configured connection between the AlienApp 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.

**Required Connectivity on the USM Anywhere Sensor**

An AlienApp operates through a deployed USM Anywhere Sensor. To use the AlienApp for Sophos Central, you must open the following ports on the sensor to support its functions.

<table>
<thead>
<tr>
<th>Port</th>
<th>Endpoint</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>api1.central.sophos.com/gateway/siem/v1/events</td>
<td>Collect event data from Sophos Central</td>
</tr>
<tr>
<td>443</td>
<td>api1.central.sophos.com/gateway/siem/v1/alerts</td>
<td>Collect alert data from Sophos Central</td>
</tr>
</tbody>
</table>
Configuration for the Sophos Central Connection

To enable AlienApp for Sophos Central functionality within USM Anywhere, you must configure the AlienApp by providing a valid Sophos Central API token. With a successful connection to your Sophos Central environment, the AlienApp 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.

Generate the API Token

As a Sophos Central administrator, you must create the API token to be used by the AlienApp for the connection to your Sophos Central data through the Sophos Central APIs. The token is valid for one year. To maintain the USM Anywhere connection, you will need to renew the token to extend its validity.

To add an API token for Sophos Central

1. Log in to your Sophos Central environment and select Global Settings.
2. In the Administration section of the page, click API Token Management.
3. On the top-right corner of the page, click Add Token.
4. Enter a name for the token, such as usm-anywhere.

   ![Add Token](image)

5. Click Save.

   Sophos Central displays a summary page for the generated token, including the URL and header information used to access the APIs with the token.

6. On the right of the API Access URL + Headers box, click Copy.
7. (Optional.) If needed, store the value in a secure location so that it is available for configuring the AlienApp for Sophos Central connection.

If you plan to immediately configure the AlienApp for Sophos Central connection on the same system, you can simply leave the value in your clipboard.

**Configure the AlienApp for Sophos Central Connection**

After you create the API token in Sophos Central, you can configure the connection within USM Anywhere.

**To enable the AlienApp for Sophos Central connection**

1. In USM Anywhere, go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab.
3. Search for the AlienApp, 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 AlienApp.

   AlienApps 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 AlienApp API endpoints.

6. Click **Change Sophos Central API Access URL + Headers**.
7. Enter the API token you copied from Sophos Central.
8. (Optional.) Modify the data options for log collection.
9. Select **Collect Sophos Central events** or **Collect Sophos Central alerts** to limit the data collection from your Sophos Central environment.

10. Click **Save**.

11. 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 appears, 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 AlienApp for Sophos Central Collection Jobs**

![Role Availability](image)

After you configure the AlienApp 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 AlienApp 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 AlienApp 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 AlienApp 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.

   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

AlienApp 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.
AlienApp for SpyCloud Dark Web Monitoring

The AlienApp 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. AT&T Cybersecurity provides this functionality at no additional cost through a partnership with SpyCloud, a pioneer in breach discovery. 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 AlienApp for SpyCloud Dark Web Monitoring.

**Edition:** The AlienApp for SpyCloud Dark Web Monitoring is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.

Configuring the AlienApp for SpyCloud Dark Web Monitoring

To enable AlienApp for SpyCloud Dark Web Monitoring functionality within USM Anywhere, you must configure the AlienApp by setting up your watchlist or connecting your SpyCloud-managed watchlist. After this configuration is complete, the AlienApp for SpyCloud Dark Web Monitoring queries the SpyCloud API every 24 hours for information regarding all watchlist items. 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 AlienApp operates through a deployed USM Anywhere Sensor. In order to use the AlienApp for SpyCloud Dark Web Monitoring, you must open the following ports on the sensor to support these functions.

<table>
<thead>
<tr>
<th>Port</th>
<th>Endpoint(s)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP, TCP port 53</td>
<td>8.8.8.8, 209.244.0.3, 64.6.64.6</td>
<td>Domain Name System (DNS) lookup to verify the domain</td>
</tr>
<tr>
<td>80, 443</td>
<td>Domain configured in the watchlist</td>
<td>Validate the verification marker of the domain</td>
</tr>
<tr>
<td>443</td>
<td>api.spycloud.io</td>
<td>Check the SpyCloud breach database</td>
</tr>
</tbody>
</table>
Configuration for SpyCloud Dark Web Monitoring

The AlienApp 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 AlienApp 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 AT&T Cybersecurity partnership with SpyCloud, complete the form on this page: https://www.alienvault.com/app/dark-web-monitoring/signup.

- **A valid SpyCloud customer API key** used to retrieve breach data from a watchlist managed in SpyCloud.
  
  When you use the SpyCloud API key method, you do not need to manually add domain or email addresses in USM Anywhere. The AlienApp 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 one domain, a list of up to 10 email addresses, or both. When combining both of 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 AlienApp 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 AlienApp for SpyCloud Dark Web Monitoring app action to collect historical breach events.

To configure a watchlist for the AlienApp for SpyCloud Dark Web Monitoring

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.

   ![Add Email dialog box]

   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 AlienApp 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.
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**.

```
Add Domain

Add your domain in the form example.org.

For each domain you add to the watchlist, you'll have to verify ownership. Until ownership verification is complete, you will not be able to view any data related to the domain.

Domain:

mycompany.com

Add  Cancel
```

This adds the domain to the watchlist, but it is not yet verified. Upon verification, the AlienApp 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.
When you have the information that you need, click **Verify Domain** to close the dialog box. This also executes a verification check that is successful if you have already completed the configuration, and an automated job that checks every six hours to verify the domain.

**Note:** The Add Domain function is disabled when you enter a SpyCloud API key. The AlienApp 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 AlienApp 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 AlienApp for SpyCloud Dark Web Monitoring app action to **collect historical breach events**.

**Important:** If you previously enabled the AlienApp 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 AlienApp for SpyCloud Dark Web Monitoring to your SpyCloud account

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.
   AlienApps 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 AlienApp 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 AlienApp 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 AlienApp, 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 appears, 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.

**Collecting Your Historical Breach Events**

Upon configuration of the AlienApp for SpyCloud Dark Web Monitoring, the SpyCloud Dark Web Monitoring scheduler job collects new records every 24 hours for all validated watchlist items. The AlienApp 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, and then click the tile.
4. Click the Actions tab.
5. Click Run to execute the action.

### AlienApp for SpyCloud Dark Web Monitoring

<table>
<thead>
<tr>
<th>Collect Logs</th>
<th>Actions</th>
<th>History</th>
<th>Domain Watchlist</th>
<th>Email Watchlist</th>
<th>Instructions</th>
</tr>
</thead>
</table>

**Actions**

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get historical breach records</td>
<td>Generate new events for historical breaches for verified watchlist domains and emails.</td>
</tr>
</tbody>
</table>

6. Verify the selected action type and action, and then click Run.

### Select Action

- **Action Type**: SpyCloud Dark Web Monitoring
- **Sensor**: USMA-51 (172.31.122.23)

**App Action**

Select the following:
- Get historical breach records

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source DNS Domain</td>
<td>Domain name associated with the breach record.</td>
</tr>
<tr>
<td>Event Ref Date</td>
<td>The date on which the record entered the SpyCloud systems, in ISO 8601 date-time format.</td>
</tr>
<tr>
<td>Source Username</td>
<td>Username associated with the breach record.</td>
</tr>
<tr>
<td>Source User Email</td>
<td>The email address associated with the breach record.</td>
</tr>
<tr>
<td>Public Breach</td>
<td>A true/false flag that indicates if the breach has been disclosed to the public.</td>
</tr>
<tr>
<td>Infected User</td>
<td>A true/false flag that indicates if the credentials were obtained by a keylogger.</td>
</tr>
<tr>
<td>Source ID</td>
<td>SpyCloud-generated numerical identifier for the breach in which the credentials were found.</td>
</tr>
<tr>
<td>Password Type</td>
<td>The password type identified in the breach record.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>List of one or more IP addresses in alphanumeric format (both IPv4 and IPv6 addresses are supported).</td>
</tr>
<tr>
<td>Sighting</td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Note:** The AlienApp for SpyCloud Dark Web Monitoring leverages the SpyCloud APIs to retrieve breach records. For more information about the attributes (data fields) it stores in these breach records, refer to the SpyCloud API documentation.
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.
   
   ![Data Source Integration](image)

   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.

### AlienApp for Zscaler

The AlienApp 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 AlienApp for Zscaler can add the source or destination IP address to the blacklist in the Zscaler Internet Access (ZIA) interface.

**Edition:** The AlienApp for Zscaler is available in the Standard and Premium editions of USM Anywhere. See [https://cybersecurity.att.com/pricing](https://cybersecurity.att.com/pricing) for more information about the features and support provided by each of the USM Anywhere editions.

**Warning:** If the AlienApp fails and you receive a message informing you that it has not been loaded, please contact AT&T Cybersecurity Technical Support to solve the problem.
Configuring the AlienApp for Zscaler

To configure the AlienApp 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 > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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 AlienApp.
   - AlienApps 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 AlienApp 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 appears, 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.

AlienApp for Zscaler Orchestration

The AlienApp 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 AlienApp for Zscaler orchestration actions to enforce protection based on the information associated with the event or alarm. The table below lists the available actions from the AlienApp.

### Actions for the AlienApp for Zscaler

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to Blocked List</td>
<td>Add a source or destination to the Zscaler blocked list.</td>
</tr>
<tr>
<td>Add to Allowed List</td>
<td>Add a source or destination to the Zscaler allowed list.</td>
</tr>
<tr>
<td>Remove from Allowed List</td>
<td>Remove a source or destination from the Zscaler blocked list.</td>
</tr>
<tr>
<td>Add to Custom Category</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Search for existing categories</strong> to see if the IP address is currently associated with any categories.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>URL Lookup</strong> 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.</td>
</tr>
</tbody>
</table>
To view information about these actions in USM Anywhere

1. In USM Anywhere, go to Data Sources > AlienApps.
2. Click the Available Apps tab.
3. Search for the AlienApp, 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.

Launching a Zscaler Response Action

When you review the information in the Alarm Details, Event Details, or Vulnerability Details, you can easily launch an action to set an indicator or tag the event in Zscaler. 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 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.
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 Zscaler Response Action Rules

Use the AlienApp 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.

## Request for a New AlienApp or Update to an Existing AlienApp

AT&T Cybersecurity builds or updates AlienApps at the request of customers for products and devices available to the general public. To take advantage of this, customers must have an active AT&T Cybersecurity Support and Maintenance contract.

**Important:** This policy does not apply to AlienApps for custom software or devices.

See this [list of AlienApps](#) for information on the AlienApps included in USM Anywhere.

### Before Submitting Your Request

The more information you can provide, the faster AT&T Cybersecurity can build the AlienApp 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 formatting of the logs. Select from the list of current AlienApps 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 AlienApp 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 AlienVault 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 AlienApp.

- 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 AlienApp to make sure it can successfully extract that data.

- Use case for the new AlienApp 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.