### Viewing Full User Details ................................................................. 227

### Events, Alarms, and Notifications Created When a User's Status Changes ........ 230

### Merging Users ........................................................................... 232

### Deleting Users .......................................................................... 235

### Importing Users from a CSV File .................................................... 237

#### Alarms Management ................................................................. 239

##### Alarms List View .................................................................. 240

##### Selecting Alarms in Alarm List View ...................................... 249

##### Searching Alarms .................................................................. 251

##### Viewing Alarm Details ........................................................... 259

##### Labeling the Alarms ............................................................... 271

##### Alarm Status ......................................................................... 274

##### Create Alarms Report ............................................................. 276

#### Events Management ................................................................. 278

##### Events List View .................................................................. 279

##### Searching Events .................................................................. 294

##### Viewing Event Details ............................................................ 308

##### Create an Events Report .......................................................... 323

##### Protecting Your Sensor's Performance with EPS Adaptive Response ....... 325

##### Raw Logs in Events ................................................................. 327

#### System Events Management ..................................................... 330

##### USM Anywhere System Events List View .................................. 331

##### Searching System Events .......................................................... 333

##### Viewing System Event Details .................................................. 337

##### Regular Events and System Events ........................................... 337

#### Console User Events on USM Anywhere ....................................... 353

##### USM Anywhere Console User Events List View ....................... 354

##### Searching Console User Events ................................................ 355

##### Viewing Console User Events Details ....................................... 360

#### Configuration Issues Management ........................................... 362

##### Configuration Issues List View ............................................... 363

##### Searching Configuration Issues ............................................... 366
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Configuration Issues Details</td>
<td>371</td>
</tr>
<tr>
<td>Create a Configuration Issues Report</td>
<td>372</td>
</tr>
<tr>
<td>List of Configuration Issues in USM Anywhere</td>
<td>373</td>
</tr>
<tr>
<td>USM Anywhere Scheduler</td>
<td>377</td>
</tr>
<tr>
<td>The Job Scheduler Page</td>
<td>377</td>
</tr>
<tr>
<td>USM Anywhere Scheduler Best Practices</td>
<td>379</td>
</tr>
<tr>
<td>Managing Jobs in the Scheduler</td>
<td>381</td>
</tr>
<tr>
<td>Scheduling Active Directory Scans from the Job Scheduler Page</td>
<td>388</td>
</tr>
<tr>
<td>Scheduling Asset Scans from the Job Scheduler Page</td>
<td>393</td>
</tr>
<tr>
<td>Scheduling Asset Groups Scans from the Job Scheduler Page</td>
<td>398</td>
</tr>
<tr>
<td>Scheduling User Discovery Jobs from the Job Scheduler Page</td>
<td>403</td>
</tr>
<tr>
<td>Scheduling Log Collection from the Job Scheduler Page</td>
<td>408</td>
</tr>
<tr>
<td>Rules Management</td>
<td>435</td>
</tr>
<tr>
<td>Orchestration Rules</td>
<td>436</td>
</tr>
<tr>
<td>Correlation Rules</td>
<td>497</td>
</tr>
<tr>
<td>Correlation Lists</td>
<td>500</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>509</td>
</tr>
<tr>
<td>About Vulnerability Assessment</td>
<td>510</td>
</tr>
<tr>
<td>System Settings for Authenticated Scans</td>
<td>513</td>
</tr>
<tr>
<td>Managing Credentials in USM Anywhere</td>
<td>518</td>
</tr>
<tr>
<td>Performing Vulnerability Scans</td>
<td>539</td>
</tr>
<tr>
<td>Viewing Vulnerabilities Scan Results</td>
<td>542</td>
</tr>
<tr>
<td>Searching Vulnerabilities</td>
<td>550</td>
</tr>
<tr>
<td>Viewing Vulnerabilities Details</td>
<td>556</td>
</tr>
<tr>
<td>Available Remediation Patches for Vulnerabilities</td>
<td>564</td>
</tr>
<tr>
<td>Labeling the Vulnerabilities</td>
<td>565</td>
</tr>
<tr>
<td>Create a Vulnerabilities Report</td>
<td>569</td>
</tr>
<tr>
<td>USM Anywhere Scans Best Practices</td>
<td>571</td>
</tr>
<tr>
<td>Open Threat Exchange® and USM Anywhere</td>
<td>575</td>
</tr>
<tr>
<td>About OTX</td>
<td>576</td>
</tr>
<tr>
<td>Using OTX in USM Anywhere</td>
<td>577</td>
</tr>
<tr>
<td>Entering Your OTX Key</td>
<td>581</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Editing Users</td>
<td>718</td>
</tr>
<tr>
<td>Managing Your Profile Settings</td>
<td>721</td>
</tr>
<tr>
<td>Deleting Users</td>
<td>729</td>
</tr>
<tr>
<td>Configuring Web UI Session Timeout</td>
<td>730</td>
</tr>
<tr>
<td>Using USM Anywhere for PCI Compliance</td>
<td>732</td>
</tr>
<tr>
<td>About PCI DSS</td>
<td>732</td>
</tr>
<tr>
<td>About USM Anywhere for PCI DSS</td>
<td>732</td>
</tr>
<tr>
<td>Working with Assets and PCI DSS</td>
<td>732</td>
</tr>
<tr>
<td>USM Anywhere Investigations</td>
<td>735</td>
</tr>
<tr>
<td>Investigations List View</td>
<td>736</td>
</tr>
<tr>
<td>Creating a New Investigation</td>
<td>737</td>
</tr>
<tr>
<td>Editing Investigations</td>
<td>739</td>
</tr>
<tr>
<td>Viewing Investigations Details</td>
<td>740</td>
</tr>
<tr>
<td>Deleting Investigations</td>
<td>752</td>
</tr>
<tr>
<td>Notification Rule for Investigations</td>
<td>753</td>
</tr>
<tr>
<td>System Status within USM Anywhere</td>
<td>755</td>
</tr>
<tr>
<td>USM Anywhere Network System</td>
<td>756</td>
</tr>
<tr>
<td>USM Anywhere System Monitor</td>
<td>757</td>
</tr>
<tr>
<td>USM Anywhere Log Collection</td>
<td>759</td>
</tr>
</tbody>
</table>
Introduction

This guide provides information for users of USM Anywhere who are responsible for monitoring network security, and identifying and addressing security threats in their environment. The guide also describes operations provided by the USM Anywhere web user interface (web UI), which is used to perform most USM Anywhere network security tasks after initial USM Anywhere deployment.

This guide includes these topics:

- Introduction
- Prerequisites and Requirements: Describes the target audience, recommended skills and background, and supported browsers for using the USM Anywhere web user interface to perform network security operations.
- USM Anywhere Network Security Concepts and Terminology: Describes key terms such as assets, threats, and vulnerabilities, and how USM Anywhere uses correlation rules to detect emerging threats.
- USM Anywhere Network Security Capabilities: Describes essential USM Anywhere security capabilities including asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and security information, and event management.
- USM Anywhere Web User Interface (UI): Describes key elements and navigation of the USM Anywhere web UI used to access and perform USM Anywhere network security monitoring and analysis operations.
- Using Multifactor Authentication: Describes multi-factor authentication (MFA), which is a method that grants access to the user. You need to configure MFA for your account.
- Getting Started with USM Anywhere: Describes typical security operations performed after initial USM Anywhere installation and configuration, including security operation best practices and workflow, verifying USM Anywhere operations, and establishing baseline network behavior.
- USM Anywhere Dashboards: Provides an overview of USM Anywhere dashboards.
- Asset Management: Describes operations to manage assets and asset groups. Includes topics such as asset creation and discovery, vulnerability scans, and asset monitoring and analysis.
- User Behavior Analytics: Provides information about how to identify malicious or compromised users, and enable you to better prioritize alarms with the addition of user data.
- Alarms Management: Provides information about alarms generated from events and OTX pulses, viewing and reviewing alarm information and field details, and suppressing alarms to remove noise in the system.
Introduction

- **Events Management**: Provides information on viewing, filtering, and sorting events, event and OTX field details, and analyzing events that generate alarms.

- **System Events Management**: Provides information on viewing, filtering, and sorting system events, which are the events generated within your environment.

- **Console User Events on USM Anywhere**: Provides information about the events that USM Anywhere generates when a user does a specific action in the user interface (UI).

- **Configuration Issues Management**: Provides information on viewing, filtering, and sorting configuration issues, and how to suppress them from the main view.

- **USM Anywhere Scheduler**: Describes the Job Scheduler page. This page provides a list of all jobs that are defined in your USM Anywhere environment.

- **Rules Management**: Describes how to create suppression and orchestration rules, and how USM Anywhere correlation rules work. This chapter also describes how Amazon Simple Notification Service (SNS) is integrated into USM Anywhere and how to manage AlienAppstm.

- **Vulnerability Assessment**: Describes how to perform vulnerability scans, view and understand scan results, and generate reports based on vulnerability scans.

- **Open Threat Exchange® and USM Anywhere**: Describes the open information-sharing and analysis network. OTX provides access to real-time information about issues and threats that may impact your organization, enabling you to learn from and work with others who have already experienced such attacks.

- **USM Anywhere Sensor Management**: Describes how to manage sensors within USM Anywhere.

- **The AWS Cloud Connector in USM Anywhere**: Describes how to manage Amazon Web Services (AWS) Cloud Connectors within USM Anywhere.

- **Subscription Management**: Describes license information, event data, and raw log data.

- **USM Anywhere Reports**: Describes reports displayed in USM Anywhere. You can find reports generated from your report creation feature; compliance templates based on alarms, vulnerabilities, and events collected in the system; and Event Type Templates based on event categorization by type of data source and by the most used data sources.

- **USM Anywhere User Management**: Describes USM Anywhere user authentication and role-based authorization, configuration of authorization for specific assets, and monitoring user activity.

- **Using USM Anywhere for PCI Compliance**: Describes USM Anywhere capabilities to manage PCI DSS requirements through assets, asset groups, and reports.

- **USM Anywhere Investigations**: Describes how to organize the information from your environment. You can link alarms, events, notes, and other files to their responses to have a complete view set of actions you have taken to address a particular threat.

- **System Status within USM Anywhere**: Describes the status of your environment. You have a system monitor page, if your role is Manager, a network settings page, and the log collection page.
Prerequisites and Requirements

The information in this guide is primarily targeted for security engineers, security analysts, and operators, IT managers and professionals, and system administrators, using the USM Anywhere product to provide network security within their own organization’s environment. We recommend you have knowledge of your organization’s network infrastructure and the networking technologies you use.

Recommended skills for users include the following:

- Basic TCP/IP networking knowledge and skills including IP addressing, DNS, switching, and routing.
- Basic familiarity with IT security concepts and associated skills, including threats, vulnerabilities, risk management, and security devices/applications.

Information provided in this guide assumes a customer has completed installation and configuration of USM Anywhere as described in the USM Anywhere Deployment Guide. In addition, users of this guide need the appropriate credentials to access USM Anywhere, and a web browser to access the USM Anywhere web UI through HTTPS.

Web Browsers Support

USM Anywhere works best in the latest desktop version of the following web browsers:

- Google Chrome
- Mozilla Firefox

USM Anywhere Network Security Concepts and Terminology

When working with USM Anywhere and using the USM Anywhere web UI to perform network security operations, it is important to understand a few basic USM network security concepts. First, a key principle of the USM system is that it monitors assets. Assets are all devices in an enterprise that have some value to the enterprise and, generally, that it is possible to monitor or gather information about, such as their status, health or availability, configuration, activity, or events. The value comprises either the cost of the device itself, or the value of the data that is stored on the device or travels through the device.

- An asset is defined as a unique IP address
- Assets are organized into networks based on IP addressing
- Networks are organized into locations, based on their geographical location
Typically, at least one USM Anywhere Sensor is used to monitor one geographically self-contained location. If several locations are used by an enterprise, each location is monitored with at least one USM Anywhere Sensor, which sends information to USM Anywhere about assets that are in the same location. AlienApps are used in the USM Anywhere Sensor to extract and normalize data from different data sources into standard-format events. USM Anywhere provides a wide assortment of integrations that can be used to collect events for most commonly encountered data sources.

USM Anywhere includes correlation rules for identifying important events or patterns of events within large volumes of data. Alarms are generated by an explicit call within the rules, either orchestration or correlation rules. Correlation rules detect threats and are continuously provided as part of the AT&T Alien Labs™ Security Research Team. Information about specific threats is obtained from sources such as those reported by AT&T Alien Labs™ Threat Intelligence Subscription and AT&T Alien Labs™ Open Threat Exchange® (OTX™). For example, OTX provides indicators of compromise and notifications of malicious hosts, which can link assets by their vulnerabilities to specific threats and notification about events that involve known or suspect malicious hosts. USM Anywhere can also perform scans which identify assets' vulnerabilities to specific and identified threats.

See Rules Management for more information.

USM Anywhere Network Security Capabilities

AlienVault USM Anywhere provides five essential security capabilities in a single SaaS platform, giving you everything you need to detect and respond to threats and manage compliance. As a cloud-based security solution, you can scale your threat detection and response capabilities as your hybrid environment changes.
The USM Anywhere cloud security management platform receives continuous updates from the AT&T Alien Labs™ Security Research Team. This team analyzes the different types of attacks, emerging threats, suspicious behavior, vulnerabilities, and exploits that they uncover across the entire threat landscape.

USM Anywhere supplements the Security Research Team with data from AT&T Alien Labs™ Open Threat Exchange® (OTX™). OTX is the largest and most authoritative crowd-sourced threat intelligence exchange in the world.

Here is a brief description of the essential functions that USM Anywhere provides:

- **Asset Discovery** is an essential security capability of USM Anywhere, which discovers assets in your environment, detects changes in assets, and discovers malicious assets in the network.

- **Vulnerability Assessment**, which is done in authenticated state, identifies vulnerabilities or compliance by comparing the installed software on assets with a database of known vulnerabilities. Vulnerability scans can be performed manually or scheduled to be performed periodically.

- **Intrusion Detection** monitors network traffic for malicious activity, monitors system log messages, and monitors user activity. Intrusion detection for USM Anywhere consists of network-based intrusion detection (NIDS) components.

  HIDS can be used to spot problems on host endpoints, and can include file integrity monitoring, rootkit and registry checks. NIDS passive sniffing interfaces can analyze network payload data to monitor for potentially malicious activity.

- **Behavioral Monitoring** identifies suspicious behavior and potentially compromised systems. USM Anywhere provides continuous monitoring of services run by particular systems. Data used for behavioral monitoring and analysis is collected from network devices and user behavior. USM Anywhere has access to logs in the cloud (Azure: Monitor, AWS: CloudTrail, S3, ELB) and VMware logs.

- **SIEM and Log Management** correlates and analyzes security event data and respond. USM Anywhere SIEM draws intelligence from different sources including the Alien Labs Threat Intelligence Subscription and OTX. Correlation rules, created by the Security Research Team, are used to identify patterns associated with malicious activity. OTX threat data provides IP reputation information and OTX pulses, which consist of Indicators of Compromise (IOCs) that identify a specific threat.

All of USM Anywhere's various security operation features and functionality are accessible from the USM Anywhere web UI.

**USM Anywhere Data Security**
As a security-first organization, AT&T Cybersecurity makes your data protection and privacy a top priority. USM Anywhere architecture and processes are designed to protect your data in transit and at rest.

Data Collection

All data sent from the USM Anywhere Sensor deployed in your on-premises or cloud environment to the USM Anywhere service in the AT&T Cybersecurity Secure Cloud is encrypted and transferred over a secure TLS 1.2 connection. Each sensor generates a certificate to communicate with the USM Anywhere service. This means that all communication is uniquely encrypted between each sensor and USM Anywhere.

All forensic data (raw logs) is backed up on an hourly basis. The data collected in USM Anywhere is secured using AES-256 encryption for both hot (online) storage and cold (offline) storage.

Data Access

Your data in USM Anywhere is treated as highly confidential, and only a select few AT&T Cybersecurity staff members have access. This group of employees uses multi-factor authentication (MFA) to access the AT&T Cybersecurity Secure Cloud. Strict internal controls and automation enable support for the service while minimizing administrative access.

AT&T Cybersecurity also has a formal information security program that implements various security controls to the National Institute of Standards Technology (NIST) Cyber Security Framework. Key controls include: Inventory of Devices, Inventory of Software, Secure Configurations, Vulnerability Assessment, and Controlled Use of Administrative Privileges. Additionally, AT&T Cybersecurity conducts security self-assessments on a regular basis.

Cold Storage Data Integrity

USM Anywhere offers secure long-term log retention, known as cold storage. By default, USM Anywhere stores all data associated with a customer’s subdomain in cold storage for the life of the active USM Anywhere subscription at no additional charge, while AT&T TDR for Gov customer data are kept for three years or longer (if requested).

**Important:** The retention period set on the license (30-days standard or 90-days standard) only applies to regular events. The retention policy for system events is 30 days and for user activities is 180 days, while the user activities related to investigations never expire.

USM Anywhere uses a write once, read many (WORM) approach in log storage to prevent log data from being modified or otherwise tampered with. You can download your raw logs at any time. If you do not renew your subscription, AT&T Cybersecurity will keep the raw logs for 14 days after your subscription expires, giving you a grace period to restart your service. Within the 14 days, no data is collected until your license is reactivated. Therefore, data is lost between license expiration and reactivation. After 14 days, your data will be destroyed.
End-of-Contract Shut Down

If your subscription expires and you decide not to renew, your USM Anywhere instance will be decommissioned 14 days after the expiration. All data, including asset information, orchestration rules, user credentials, events and vulnerabilities (hot storage), and raw logs (cold storage), will be destroyed.

Business Continuity Plan

To ensure business continuity, USM Anywhere executes a backup procedure 2 times a day, encrypts the data, and stores it for 15 days. The Recovery Point Objective (RPO) is up to 12 hours and the Recovery Time Objective (RTO) is approximately an hour, depending on the size of the data being restored.

Password Policy

USM Anywhere stores user credentials as salted hashed passwords using a Java library called StrongPasswordEncryptor, which is an industry standard library for securing passwords.

Keep in mind these points when you are logging in:

- USM Anywhere requires all passwords to have a minimum length of 8 characters and a maximum length of 128 characters.
- The password must contain numerical digits (0-9).
- The password must contain uppercase letters (A-Z).
- The password must contain lowercase letters (a-z).
- Special characters, such as hyphen (-) and underscore (_), are supported but optional.

**Note:** USM Anywhere passwords expire after 90 days. When your password expires, USM Anywhere enforces a password change when you next log in to the system using the current (now expired) password. A new password must be different from the previous four passwords.

A user account is locked for 30 minutes after 3 failed login attempts within 15 minutes.

USM Anywhere Log Data Enhancement

When evaluating threats to your systems, the more complete and clear the context of an incident is, the more accurate and efficient USM Anywhere can be in identifying and responding to those threats. Log data is one of the key sources of this threat data context, providing a tremendous amount of information about network events. Every network connection, authentication request, file transfer, and privilege escalation generates a log message.
However, many of these log messages were not originally designed to be used for security purposes. There are no official standards for log contents (although there are best practices); therefore, log message content is often inconsistent and incomplete.

For example, look at a typical log message generated by an authentication event:

```json
{
    "outcome" : "Allow",
    "type" : "Authentication",
    "source" : "13.107.4.50",
    "destination" : "10.60.5.94",
    "time" : "2018-10-17T19:03:26+00:00"
}
```

This message is brief and doesn’t provide enough context for incident analysis. USM Anywhere can improve that context by normalizing and enriching the data provided in the log message.

Data Normalization

The first step USM Anywhere takes when it analyzes your system logs is to normalize them so that all incoming data uses the same terminology. In this context, normalization means mapping it to a standard terminology. For example, a vendor may use the terms “outcome” or “result” to describe the success or failure of the authentication attempt. USM Anywhere normalizes these two different attributes, replacing them with a single, standard term. Likewise, things like source, source_ip, client, client_ip all need to be mapped to the same set of terminology so events from different vendors can be used for correlation and alarm generation.

The following is an example of how normalization works. Note that USM Anywhere preserves the original log message as a best practice in case you need to share it with a vendor or need to refer to the original alert. This means that the normalization phase of message processing likely increases the size of the log message by around 100%.

```json
{
    "log" : "{
        "outcome" : "Allow",
        "type" : "Authentication",
        "source" : "13.107.4.50",
        "destination" : "10.60.5.94",
        "time" : "2018-10-17T19:03:26+00:00"
    },
    "source_address" : "13.107.4.50",
    "destination_address" : "10.60.5.94",
    "event_outcome" : "ALLOW",
    "event_name" : "Authentication",
    "timestamp_occurred" : "2018-10-17T19:03:26+00:00"
}
```
Data Enrichment

Normalization enables you to analyze all the log messages USM Anywhere receives. Given the incomplete nature of so many log messages, it also makes sense to use this same process to add valuable information to the log messages, which helps USM Anywhere perform better incident detection.

Data enrichment is the process by which that valuable information is added to log messages. The USM Anywhere infrastructure has a large amount of contextual data about the network and systems that it can attach to the log messages to fill in the gaps and enhance threat detection. It also has access to many databases of things like the location of specific IP addresses, device types, and threats it can also leverage.

These are examples of information that can be added through data enrichment:

- Device identity
- Geolocation
- Collection details and flags

Device Identity

Most servers rely on Dynamic Host Configuration Protocol (DHCP) for dynamic IP address allocation. From a security point of view, this means that identifying and containing threats is much more difficult. By the time a system is identified as compromised, it may be on the network in a completely different place with a completely different IP address. To address that problem, USM Anywhere uses the network context it has to collect and include the media access control (MAC) address, fully qualified domain name (FQDN), and a unique identifier for the system, depending on which are known:

```
"source_asset_id" : "f8ebb373-b551-43d0-a628-a00771b5d0c1",
"source_mac" : "98:01:A7:B4:D8:47",
"destination_fqdn": "ip-10-6-255-129.ec2.internal",
"source_fqdn": "ip-10-6-2-102.ec2.internal",
```

Geolocation

Knowing where your network connections are terminating is important when deciding if traffic should be permitted, blocked, or more carefully monitored. Geolocation can play a role in deciding if a given incident is worthy of more attention. USM Anywhere augments logs with geolocation information of source and destination. In the following example, this data enables an operator to quickly determine that this particular destination is probably not an issue:

```
"destination_address" : "10.60.5.94",
"destination_name" : "AD Server",
"destination_asset_id" : "8cdf98a1-533d-9ec2-b5bc-3424caecf15",
```
"destination_organisation" : "Microsoft Azure",
"destination_city" : "Redmond",
"destination_fqdn" : "ad.alienvault.com",
"destination_hostname" : "ad",
"destination_organisation" : "Microsoft Azure",
"destination_latitude" : "47.6801",
"destination_longitude" : "-122.1206",
"destination_region" : "WA",
"destination_country" : "US",
"destination_country_registered" : "US",

Collection Details and Flags

USM Anywhere also includes some additional information about how the log message was acquired and processed. This information is included to give the security analyst and correlation algorithms insight into the source of the log, when a sensor received it, and how it was processed. For example, was_fuzzied = true means that the log message was received from a source that USM Anywhere doesn't have a specialized plug-in for and, therefore, it may not have normalized all the fields. If the log is key to an investigation, the operator should look at the original log message and ensure nothing was overlooked.

Impact on Log Storage

Because USM Anywhere adds data to log messages, the size of the original log message inevitably grows. Very sparse messages can grow as much as 1,860%. However, the messages themselves are still relatively small, typically growing from less than 250 B to as much as 2.6 KB, adding up over time. The good news is that the amount of metadata added is stable, which means it doesn't grow much larger or shrink in size for different event classes. So with careful planning, storage use can still be quite predictable. For larger events (for example, events coming from network-based intrusion detection systems [NIDS] and Amazon Web Services [AWS]), the percentage goes down significantly since the messages start out quite large. However, for small events such as the one in the previous example, it can have a noticeable impact on the total amount of data stored.

These are some syslog- and AWS-heavy data points for planning purposes:

Syslog-heavy deployment

From a sample size of 599,979 events

- **Total size including enriched data in bytes**: 1,612,790,164  
- **Total size of just log data in bytes**: 145,781,057  
- **Average log size in bytes**: 243  
- **Average log size with enriched data**: 2,688  
- **Increase in size**: 1106%

AWS-heavy deployment
From a sample size of 500,000 events

- **Total size including enriched data in bytes**: 1,934,740,282
- **Total size of just log data in bytes**: 711,502,141
- **Average log size in bytes**: 1,423
- **Average log size with enriched data**: 3,868
- **Increase in size**: 272%

**What Happens When You Reach the Tier Limit?**

If you find yourself running into problems with inadequate storage space, your first step should be to review your logging strategy with AT&T Cybersecurity Technical Support or your service provider. It may be that you don’t need to send as many logs as you are. However, it's better to err on the side of logging too much rather than logging too little, since lost logs can't be recovered and security investigations can lead in unexpected directions.

**Important:** Tier options do not have unlimited processing power, memory allotment, or disk input/output (I/O) speeds. In addition to storage per month, your deployment size’s impact on any of these factors will influence which tier option is right for your environment. AT&T Cybersecurity recommends pre-deployment sizing discussions with your sales representative to help select the right tier for you.

When approaching your monthly storage limit in USM Anywhere, you have two choices: rely on transient mode, or actively prune your consumption with event filters. See [Reaching the Monthly Usage Limit](#) in the USM Anywhere User Guide for more information.

AT&T Cybersecurity strives to guarantee that no data is lost, even when you're facing inadequate storage space or processing power. Because of this, USM Anywhere always makes data storage a top priority. When you exceed your data tier, or are projected to far exceed your tier, your system tries to store as much data as possible, even if functionality must be reduced to preserve the data. For instance, if you find that you are over your data tier, you may find that your USM Anywhere has paused correlation, asset counters, and more. All functionality is restored once your USM Anywhere is no longer experiencing resource limitations.

**Transient Mode**

USM Anywhere calculates how much space you have consumed and projects how much you will consume during the month. If consumption exceeds the monthly capacity, transient mode is automatically turned on. When transient mode is turned on, it's important to understand the following:

- All events are still stored within cold storage. Transient mode does not affect cold storage.
- All events are still correlated. You will not miss any alarms being generated because of transient mode.
• Alarms, vulnerabilities, and configuration issues will still be generated and stored. You will not miss any security issues because of transient mode.

• All events are dropped before persisting into hot storage. Therefore, while you will see alarms, you will not see the events that generated them. Additionally, you will not be able to see new events within your events view.

Event Filtering
If you want to be proactive with your data consumption, consider reducing the amount of data stored by using filters. Event filtering enables packets to be dropped before they enter correlation and persistence and consume any of the monthly storage allotment. Filtering enables you to define a set of rules for fields, which, when matched, are dropped. This enables you to easily pick certain types of packets that you don't want to enter the system. When filtering, it's important to realize the impact:

• Filtered events are not stored within cold storage.
• Filtered events are not correlated. Alarms are not generated off filtered events.
• Filtered events are dropped from going into hot storage. You will not see them within your events view.

When using filters, it's important to make sure that you're precisely defining the criteria for events to be dropped. If the filter rule is too broad, there is a chance you may drop packets that you are interested in keeping.

Is There Any Way of Freeing Space?
If you are in transient mode and wish to free up space to allow for more events, you can purge the last 7 days of events. This only affects events and doesn't purge any alarms that they generated. Additionally, the purge does not affect any events that are in cold storage. Purging removes those events from hot storage, and you will not see them within your events view.

Compliance Considerations for Filtering and Purging
It's important to remember that most security compliance regimes require the storage of 90 days of logs. Therefore, purging logs may put you in violation of your compliance regulations. It is also important to understand if there are any compliance implications to filtering out data as well. For example, if a filter restricts the amount of data logged by a system under Payment Card Industry (PCI) or similar requirements, it's important to check with your compliance team first.

USM Anywhere Web User Interface (UI)
The USM Anywhere web user interface (UI) provides access to all the tools and capabilities that USM Anywhere makes available for managing the security of your organization’s network and the devices in it. From the USM Anywhere web UI, you can view all essential information about network devices, applications, user activity, and network traffic in your environment. You can
begin monitoring information coming from devices and then go about defining orchestration rules to fine tune the behavior of your system. USM Anywhere includes by default correlation rules to alert you of potential security issues and vulnerabilities.

The USM Anywhere web UI runs in a standard web browser. Your system administrator can provide the web address and credentials to log in and access the features and functions appropriate to your role in your organization’s security operation.

When you first log in, the USM Anywhere web UI displays the main window.

By default, the web UI displays a collection of high-level graphs and charts summarizing activity in your organization’s network. From this main window, you can select different menu options or click other links and buttons.

**Important:** You can also load the configured default landing page by clicking the logo of USM Anywhere located in the upper-left corner of the page.

Callouts on the screen identify the main navigable elements and selections that are provided consistently through the web UI.

**Primary menu**

Provides access to the main functions or operations of USM Anywhere. These include:
• Dashboards. Display of lots of charts, tables, and graphs. There are dashboards that will be displayed depending on the sensor you have installed; there are also dashboards related to the AlienApp you have configured and that will be visible if you have data for them. See USM Anywhere Dashboards for more information.

• Activity. Display providing search, sorting, filtered selection, and visualization of Alarms and Events. See Alarms Management and Events Management for more information.


• Reports. Provides display and management of reports which are the result of export data that you can find in assets, asset groups, alarms, events, vulnerabilities, and configuration issues. You can also choose the format of the report (PDF and CSV). There are also Compliance and Event Type Templates. See USM Anywhere Reports for more information.


• Investigations. Provides options to organize the information from your environment. See USM Anywhere Investigations for more information.

• Settings. Provides options to view and manage credentials and system events. There are administration options which let you manage users and asset fields, display the system status, schedule jobs, validate your OTX key, and manage orchestration rules. You can also display the data about your subscription and connect your USM Anywhere to USM Central environments.

**Secondary Menu**

Provides access to the system configuration, the user profile information, the help link, and the bookmarked items:

• Bookmarks. The ⭐ icon enables you to see and access alarms, events, or assets that you (or another user) bookmarked for easy access. The number on the icon indicates the number of items bookmarked.

• Help. The 💡 icon includes the these options:
  • Documentation: Links to online documentation
  • Support: Links to the AT&T Cybersecurity Support page
  • Forums: Links to the AT&T Cybersecurity Success Center

• Feedback. The 🗣 icon provides a direct communication with the USM Anywhere team.
Profile Settings. The icon shows your profile settings. You can change your email, full name, update your password, enable **multi-factor authentication** (MFA) for the account, select your default landing page after you have logged in, configure an interval for auto-refreshing the dashboards and alarms pages, and the configuration of receiving alarm notifications. See Managing Your Profile Settings for more information.

The remainder of this guide describes best practices in performing common network security operations and provides step-by-step instructions for performing specific tasks. Following sections also describe the USM Anywhere web UI from which you can monitor network security and access all of USM Anywhere’s security operation features and functionality.

**Using Multifactor Authentication**

To protect your USM Anywhere account, enable multifactor authentication (MFA). MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account. In USM Anywhere, MFA provides a layered defense of two independent credentials: what you know (your user account name and password) and what you have (security token on your personal device).

To use multifactor authentication in USM Anywhere, you must have a mobile device that supports an Authenticator app. AT&T Cybersecurity recommends the [Google Authenticator app](https://play.google.com/store/apps/details?id=com.google.androidＲesession), which is available for iOS and Android devices. Google Authenticator implements two-step verification services using the Time-based One-Time Password (TOTP) algorithm and HMAC-based One-time Password Algorithm (HOTP) for authentication.

**Configuring MFA for Your Account**

Before you set up MFA for your account, you must install the Authenticator app on your device.
To configure MFA for your account

1. In the lower-left corner of the USM Anywhere web user interface (UI), click the icon and select **Profile Settings**.
2. Select **Enable multi-factor authentication** and click **Save**.

3. Click the icon and select **Logout**.

4. Click **Login**.

5. On the login page, enter your user account/password and click **Login**. USM Anywhere displays the multifactor authentication page to prompt you to complete your MFA configuration. The displayed page provides a unique QR code that is used by the Authenticator app to retrieve a verification code.
6. Open the Authenticator app on your device.
7. Scan the QR code using the Authenticator app.
8. Enter the one-time passcode in the text box of the USM Anywhere and click Verify Code and Login.

Changing Your Authentication Device

In the event that you lose or change your mobile device, there is a function to reset the MFA for your user account. Another user in your USM Anywhere environment can edit your user account to reset the QR code used to pair the device with your account.

To change your authentication device

1. Go to Settings > Users.
2. Click the icon of the user to which you want to reset the MFA account. Your role must be Manager.
3. Click **Reset Multi-factor Authentication**.

A message displays at the top of the page to inform you about the success of the MFA reset request.

4. Click **Cancel**.

After the reset, USM Anywhere displays the multifactor authentication page at your next login. Follow the same steps to set up the authentication with the new device.
Getting Started with USM Anywhere

This section details typical security operations performed after the system installation, initial deployment, and configuration of USM Anywhere.

The section includes several chapters for explaining these security operations. There is a chapter which describes how essential is the review of some of the overall best practices that many organizations follow in implementing and then maintaining network security operations in their environments.

Another chapter is about the significance of having a good network security monitoring system which can discover things every day that provide value to security efforts.

You can also find in this section, a chapter which describes a best practice workflow for using USM Anywhere to perform operations during the entire Security Monitoring and Management lifecycle.

You can also find information about how you can use the USM Anywhere web UI to verify that it is operating properly after the basic installation and configuration of your USM Anywhere system.

Finally, in this section, there is a chapter on which you will find how you could establish a Baseline Network Behavior for what constitutes normal behavior in your network. Through this baseline, you could evaluate results and filter out the noise to identify and filter out right away some false positives.

This section includes the following topics:

- USM Anywhere Network Security Best Practices .............................................................. 27
- Expectations of Security Monitoring .................................................................................. 28
- Workflow of the USM Anywhere Event Process ................................................................ 28
- Verifying USM Anywhere Operation .................................................................................. 29
- Establishing Baseline Network Behavior ............................................................................ 31
- Start Using USM Anywhere ............................................................................................... 32
USM Anywhere Network Security Best Practices

Providing strong and effective security for an organization's network, IT infrastructure, and environment requires some forethought and planning. If you are now tasked with monitoring, managing, or maintaining network security operations within your organization, after USM Anywhere has already been deployed, many of the planning steps and decisions may have already been made. In any case, it is worth reviewing some of the overall best practices that many organizations follow in implementing and then maintaining network security operations in their environments. This is the general process:

- **Determine** the scope of your network security operation, the range of networks and sub-networks to be covered, and the network devices or assets (host servers, applications, fire-walls, routers, and switches) to be protected.

- **Assess** risk, determine what is most important to protect, and determine the type of network security you need to provide. Identify specific threats and vulnerabilities you need to address. Also determine specific regulatory compliance and other business standard requirements you need to meet.

- **Define and determine** security team roles, permissions, tasks and responsibilities, and implement authentication and authorization to support USM Anywhere security operations. Also determine notification and escalation strategy for emails, ticket handling, incident response, and compliance documentation requirements.

- **Develop a plan** for initial implementation and rollout of network security operations, plus planned updates and enhancements, based on priorities. Take into account the time and resources required for monitoring, incident analysis and response, compliance reporting, and record-keeping, plus subsequent updates to address additions or changes in the environment, as well as new threats and vulnerabilities.

- **Deploy and run** USM Anywhere to monitor and analyze the behavior of the environment. Use dashboards, reports, and other features of the USM Anywhere web UI to examine events, network traffic, alarms, and notifications. Establish baseline behavior, identify threats and vulnerabilities, and eliminate or reduce false positives and other noise from normal, benign behavior. After establishing a baseline, you can use various tools provided within the USM Anywhere web UI to investigate alarms and suspicious events, identify threats and vulnerabilities, and continue monitoring your network for attacks, intrusions, or any other type of malicious and potentially damaging behavior.

- **Make continuous security lifecycle improvements** and perform regular maintenance: new asset discovery and risk assessments, new vulnerability and thread detection, compliance reporting, backup and archival record-keeping.

- **Incident Response.** Develop and implement processes and procedures for Incident Response (IR) to provide special event and incident handling. Detect anomalies and suspect behavior; investigate, identify, and isolate threats, intrusions, or attacks; eradicate, remediate, or mitigate threats; conduct post-incident, post-mortem reviews to identify improvements to security processes and practices.
Expectations of Security Monitoring

Security monitoring is often about monitoring often-overlooked things such as host, device, and application vulnerabilities, because those are typically the same things that attackers will leverage against you later in carrying out attacks or attempting unauthorized access to data or resources. A good network security monitoring system discovers things every day that provide value to security efforts. USM Anywhere can help to locate or identify:

- Misconfigured systems.
- Hosts that have fallen off the radar of asset management.
- Systems compromised by opportunistic malware or other attacks by malicious software.
- Inappropriate or unauthorized access of sensitive data or resources from both internal and external parties; for example, detecting websites that should be blocked at the proxy server, but were not.

USM Anywhere priorities for network security operations are determined primarily by correlation rules. The rules link events together into meaningful bundles and turn data into useful information. Correlation is a function of USM Anywhere, which configures automated analysis of correlated events for identifying potential security threats and produces alerts to notify recipients of immediate issues. You can also create orchestration and suppression rules to secure your network security operations.

Workflow of the USM Anywhere Event Process

After USM Anywhere is installed in your environment, events start flowing through the system, so you can start gaining visibility into the type of events that are occurring, what natural or non-threatening activity is taking place, and what activity can be a possible attack. USM Anywhere also begins collecting other information about your network and various network devices such as firewalls, routers and switches, servers, and applications. In addition, it is discovering and determining possible vulnerabilities and threats to your environment.

The following illustration details a high level view of events and other information from your network environment as it is collected or generated by the USM Anywhere Sensors and Agents, and then delivered to the USM Anywhere for processing and storage.
USM Anywhere Sensor combines asset discovery, vulnerability assessment, threat detection, and behavioral monitoring to provide full situational awareness. USM Anywhere Sensor is the front-line security module of the USM Anywhere platform and provides detailed visibility into your environment, vulnerabilities, attack targets and vectors, and services.

USM Anywhere Sensor receives data and other activity or status information from devices and normalizes the information into a standardized event format. USM Anywhere Sensor then sends the normalized event to USM Anywhere, which tries to match every event with an asset or a user, enrich the event with environmental data where possible, and saves it.

**Note:** To protect the health of your system, USM Anywhere monitors the rate of events being sent to your sensor. If that rate, measured in events per second (EPS), threatens to impact your sensor's capacity your EPS will be throttled. Throttling allows your system to take more time to process events coming in, without risking event loss. USM Anywhere will generate an event when EPS throttling is engaged. See [Protecting Your Sensor's Performance with EPS Throttling](#) for more details about when EPS is engaged and how it works.

USM Anywhere provides a unified management interface through the web UI that combines security automation, and AT&T Alien Labs™ Open Threat Exchange® correlation intelligence from the AT&T Alien Labs™ Security Research Team to correlate data, spot anomalies, reduce risk, and improve operational efficiency.

Correlation can be done logically, where events can be compared to patterns and multiple conditions can be connected by using logical operators such as OR and AND. After events are processed and correlated, USM Anywhere performs risk analyses and triggers an alarm if the risk of the event is high enough.

### Verifying USM Anywhere Operation

After the basic installation and configuration of your USM Anywhere system is completed, you can use the [USM Anywhere web UI](#) to verify that it is operating properly.

The following process describes tasks you can perform to verify basic operations, also walking you through information available from the primary menu options.
1. When you first launch the USM Anywhere web UI, it displays the main dashboards page. This high-level view of summary information shows the overall state of your network, so you can get an immediate indication of the levels of events and alarms occurring in your environment.

2. Confirm that security events are being collected, and populating the USM Anywhere correctly. To see events, go to Activity > Events. On this page, any normalized log event, or any other event received or generated by any USM Anywhere Sensor at the application, system, or network level, will show in the display, unless a suppression event has filtered it out.

You can also search for and filter out specific events using time ranges and other search criteria. Click a specific event row to display additional information for the selected event, in a dialog box. You can view and examine full details about an event, in a full browser window, by clicking the event, and then clicking Full Detail. Use this link to see all the information about the event such as the details of the event, the related assets, the source and destination IP addresses, and the log of the event.

3. Confirm that USM Anywhere is creating alarms and the alarms are displaying correctly. The USM Anywhere generates alarms from correlation rules. To see alarms in your system, go to Activity > Alarms.

By default, the middle portion of the page provides a graphical representation of current alarms being generated in your environment. Blue circles indicate the number of alarms in a category that are displaying at a particular time. A bigger circle indicates a higher number of alarms. Alarms are prioritized by categories that reflect typical methods used by attackers. See Viewing Alarm Details for more information on alarm categorization.

You can also search for and filter out specific alarms using time ranges and other search criteria. Click a specific alarm row to display additional information for the selected alarm, in a dialog box. You can view and examine full details about an alarm, in a full browser window, by clicking the alarm, and then clicking Full Detail. Use this link to see all the information about the alarm such as the events that triggered the alarms, source and destination IP addresses, and the recommended actions to be done.
Establishing Baseline Network Behavior

When you first start using USM Anywhere, it is a good idea to let it run for a few days to determine which events and alarms you can consider "noise" and which ones to investigate further. By noise, we mean false positives that obscure true positives. Because no system is perfect, you must ensure that you have actionable alarms and useful reports, not hundreds of things to review. What you learn from the baseline collection and the evaluation of those events helps you create orchestration and suppression rules that tell USM Anywhere what is important or not. Alarms are also created from correlation rules, which are created by the AT&T Alien Labs™ Security Research Team.

See Rules Management for more information.

Baselining

To be able to tune the system, you need to create a baseline for what constitutes normal behavior in your network. This is called baselining. The alarms and events generated during this initial period represent currently normal behavior, in other words, a snapshot in time. Of course, there may be things you want to filter out right away. But in general, you should resist the temptation and wait until you have had a chance to observe any patterns in your network.

Evaluating Results

After you collect these data points, you need to start making decisions about them, based on these criteria:

- Which events have value and applicability to my system?
- Which events have to do with network policy and therefore are not potential threats?
- Was the rule properly assessed?
- Which events have value for reporting?
- Who should receive notification when this event occurs?

Answering these questions for the first time is best done in a group setting with the relevant stakeholders. In subsequent iterations of this process, usually only the analysts participate, because the fundamental questions for each event can be applied through taxonomy. Because AT&T Cybersecurity releases new signatures frequently, this decision making process will be a recurring event.

Filtering Out the Noise

You may want to identify and filter out right away some false positives. One example might be an alarm indicating scanning of hosts in the network. Such an alarm could be legitimate if performed by an internal network mapper. On the other hand, it may be currently benign, but may also be a precursor to a real attack. USM Anywhere treats both events equally.

If you examine an alarm and you determine that the event that triggered it was noise, not a real threat, consider taking these steps:

1. Create an orchestration rule that prevents USM Anywhere from processing new events from the source. For example, let’s say that USM Anywhere properly detected vulnerability scanning coming from an internal scanner but such events do not interest you, because the internal vulnerability scanner is controlled by your environment. See Orchestration Rules for more information.

2. If not interested in specific alarms, you can do:
   - Reconfigure the external data source to not send such events.
   - Use a rule to discard such events.
3. Suppress all occurrences of the alarm from USM Anywhere. See Creating Suppression Rules from the Alarms Page for information on how to do this.

Start Using USM Anywhere

After you have initialized your new USM Anywhere Sensor and you have configured it in the Setup Wizard, you can start using it. See these links for more information:

- USM Anywhere Deployment Process
- Completing the AWS Sensor Setup
- Completing the Azure Sensor Setup
- Completing the GCP Sensor Setup
- Completing the Hyper-V Sensor Setup
- Completing the VMware Sensor Setup

Once you click the Start Using USM Anywhere button, the page for entering the login and the password displays:

[Login page]

Keep in mind these points when you are logging in:

- USM Anywhere requires all passwords to have a minimum length of 8 characters and a maximum length of 128 characters.
- The password must contain numerical digits (0-9).
- The password must contain uppercase letters (A-Z).
- The password must contain lowercase letters (a-z).
- Special characters, such as hyphen (-) and underscore (_), are supported but optional.

**Note:** USM Anywhere passwords expire after 90 days. When your password expires, USM Anywhere enforces a password change when you next log in to the system using the current (now expired) password. A new password must be different from the previous four passwords.
The messages you can have are these:

- Password successfully updated. Please log in with your new password.
- Your session has expired.
- The username or password you entered is incorrect.
- The server responded incorrectly.
- There was an error with your security token. Try refreshing your page or contact support.

There are three roles in USM Anywhere:

- **Read-Only**: You can access views and search the system, but cannot make system changes that impact other users.
- **Analyst**: You can view and search the system, schedule jobs, launch actions, configure rules, and configure asset credentials. But you cannot add or modify sensor configurations; configure credentials for AlienApp, notification apps, and threat intelligence integrations; or add users.
- **Manager**: This role enables analyst permissions, and enables you to add or modify sensor configurations; configure credentials for AlienApps, notification apps, and threat intelligence integrations; and add users.

**Important**: There is a maximum number of sessions per user. Users whose role is Manager can log in to USM Anywhere from up to three different browsers at the same time. Users whose role is Analyst or Read-Only can log in to USM Anywhere from up to two different browsers at the same time.

See [USM Anywhere User Management](#) for all the information related to users.
The first view of the USM Anywhere web UI is a set of dashboards. These dashboards provide overall visibility into the activity on your network and display various network security metrics.

Note: USM Anywhere also makes available several reports that you can display. These reports provide detail on various aspects of USM Anywhere network security. For more information on reports, see USM Anywhere Reports.

This topic discusses these subtopics:

- Refreshing and Filtering Data from the USM Anywhere Dashboards .................................................. 35
- Exporting Data from the USM Anywhere Dashboards ............................................................... 36
- Executive Dashboard .................................................................................................................. 37
Refreshing and Filtering Data from the USM Anywhere Dashboards

USM Anywhere gives you the option of refreshing dashboards automatically in a period of time that you can configure.

You can also filter your search in the upper left corner of the dashboards page. When you select one or more filters, the dashboard restricts the views to the selected filters. If you export the dashboard as an HTML report, it preserves the selected filters. See Exporting Data from the USM Anywhere Dashboards for more information.

Refreshing Dashboards

You can configure a period of time for refreshing the data on your dashboards. See Managing Your Profile Settings for more information.

Following the name of the dashboard, you can click the icon to stop the auto-refresh countdown and refresh the page manually.

There is an auto-refresh countdown that refreshes the page at a regular interval. The number inside the blue circle indicates the remaining time until the next refresh. See Managing Your Profile Settings to configure this interval.

General Filters

All dashboards include two filters:
**Last 24 Hours**

Use this filter for identifying data created during the last hour, last 24 hours, last 7 days, or last 30 days. You can also configure your own period of time by clicking the **Custom Range** option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select **AM** or **PM**.

**All Assets**

Use this filter for searching data according to assets. You can search by all assets or by asset groups.

**To apply one or more filters to a dashboard**

1. Select the dashboard on which you want to display data.
2. Select the filter. You can select both filters option.
3. Click **Apply**.

**Widgets Filters**

There are some widgets that include the 👇 icon to filter data on that widget. Use this filter for identifying data created during the last hour, last 24 hours, last 7 days, or last 30 days.

---

**Exporting Data from the USM Anywhere Dashboards**
USM Anywhere enables you to export data from the dashboards as an HTML report.

**To export data as a report**

1. Display the dashboard you want to have a report.
2. Click **Generate Report** at the upper right-hand corner of the page.
3. Enter a title for your report.
4. (Optional.) Enter a report description.
5. Click **Print**.
   
   A dialog box opens to configure the options of the report that you are going to print.
6. Click **Save** in case you want to print your report or save it as PDF.

**Executive Dashboard**

The executive dashboard provides a visual display of important security metrics with the goal of giving an at-a-glance view into performance across your security program.
This dashboard offers widgets that detail all aspects of your environment. You can click these widgets, taking you to the detailed information page, and enabling you to drill down into the data even more. Use the executive dashboard to check the information included in your environment, detect possible problems, and decide the solutions that are better at every moment.

You can filter data included in the widgets by clicking the icon. See Refreshing and Filtering Data from the USM Anywhere Dashboards for more information.

You can clone and customize your executive dashboard to meet your specific needs. See Clone the Executive Dashboard for more information.

You can also export data from the dashboard as an HTML report. See Exporting Data from the USM Anywhere Dashboards for more information.

The executive dashboard includes these separate sections:

- **Executive Summary**: Provides several widgets with general information. These widgets are platform updates, threat metrics, security funnel, number of AT&T Alien Labs™ Open Threat Exchange® (OTX™) pulse hits, data source usage, alarms cycle time, and vulnerabilities remediation time by severity. See Executive Summary Section inside the Executive Dashboard for more information.

- **Investigations**: Provides several widgets related to investigations. These widgets are the number of investigations, average time to close an investigation, and top severity closed investigations. See Investigations Section inside the Executive Dashboard for more information.

- **Alarms**: Provides several widgets related to alarms. These widgets are alarms summary, opened investigations by intent, alarms by severity, alarms method by strategy, and alarms method by intent. See Alarms Section inside the Executive Dashboard for more information.

- **Vulnerability Assessment**: Provides several widgets related to vulnerabilities. These widgets are scan jobs history, number of vulnerabilities, and the top five vulnerable assets by score. See Vulnerability Assessment Section inside the Executive Dashboard for more information.

- **Events**: Provides several widgets related to events. These widgets are events trend and top 10 generating data sources. See Events Section inside the Executive Dashboard for more information.

**Executive Summary Section inside the Executive Dashboard**

This section shows the related actions that occur in your environment.
Widgets in Executive Summary Section inside the Executive Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Updates</td>
<td>Total number of updates that a logged-in user has made on orchestration rules, dashboard, views, plugin updates, and assets.</td>
</tr>
<tr>
<td>Threat Metrics</td>
<td>Total number of updates that a logged-in user has made on alarms, investigations, vulnerabilities, configuration issues, and users.</td>
</tr>
<tr>
<td>Security Funnel</td>
<td>Total number of events tied to alarms and the alarms tied to investigations.</td>
</tr>
<tr>
<td>Number of OTX Pulse Hits</td>
<td>Sankey diagram that displays the top AT&amp;T Alien Labs™ Open Threat Exchange® (OTX™) indicators or pulses found on alarms.</td>
</tr>
<tr>
<td>Data Source Usage</td>
<td>Graph that displays the number of events ingested in USM Anywhere per individual data source.</td>
</tr>
</tbody>
</table>
Widgets in Executive Summary Section inside the Executive Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Cycle Time</td>
<td>Graph that displays the alarm remediation and response. It shows how long it took to respond to a threat and how long it took to resolve the alarm.</td>
</tr>
<tr>
<td>Vulnerabilities Remediation Time by Severity</td>
<td>Graph that displays the number of open vulnerabilities by severity over time.</td>
</tr>
</tbody>
</table>

Investigations Section inside the Executive Dashboard

This section displays information about the investigations you have created. The investigations organize the information from your environment and enables you to manage and coordinate incident response activities. See USM Anywhere Investigations for more information.

---

Role Availability

Read-Only

Analyst

Manager

---

INVESTIGATIONS

Number Of Investigations

Average Time To Close An Investigation

Top Severity/Count Investigations:

<table>
<thead>
<tr>
<th>Title</th>
<th>Severity</th>
<th>Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA Inv 3</td>
<td>Medium</td>
<td>Environmental Awareness</td>
</tr>
<tr>
<td>QA Investigation 10</td>
<td>Medium</td>
<td>Exploitation &amp; Initial</td>
</tr>
<tr>
<td>Net Inv 1</td>
<td>Critical</td>
<td>System Compromise</td>
</tr>
<tr>
<td>QA Inv 2</td>
<td>Critical</td>
<td>Exploitation &amp; Initial</td>
</tr>
<tr>
<td>QA Investigation 8</td>
<td>Critical</td>
<td>Delivery &amp; Attack</td>
</tr>
</tbody>
</table>
Widgets in the Investigations Section inside the Executive Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Investigations</td>
<td>Number of all investigations in your environment. The options are open, in review, and closed.</td>
</tr>
<tr>
<td>Average Time to Close an Investigation</td>
<td>Graph that displays, in days, the average time to close an investigation, from the moment is opened to the moment is closed.</td>
</tr>
<tr>
<td>Top Severity Closed Investigations</td>
<td>Displays a list of the top closed investigations by severity.</td>
</tr>
</tbody>
</table>

Alarms Section inside the Executive Dashboard

![Role Availability](image) Read-Only Analyst Manager

This section displays information related to the detected alarms in your environment. These widgets include the results of the USM Anywhere correlation engine and the value of mapping those into actionable groups based on the risk factor. See Alarms Management for more information.
Widgets in the Alarms Section inside the Executive Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Summary</td>
<td>Graph that displays the number of alarms that you have in your environment on a monthly basis and their current status. The options are open, suppressed, closed, and total.</td>
</tr>
<tr>
<td>Opened Investigations by Intent</td>
<td>Pie chart displaying the opened investigations correlated by intent.</td>
</tr>
<tr>
<td>Alarms by Severity</td>
<td>Alarms correlated by severity (critical, high, medium, and low) and related to a range of dates. The size of the bubbles depends on the number of issues.</td>
</tr>
</tbody>
</table>
Widgets in the Alarms Section inside the Executive Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms Method by Strategy</td>
<td>Method name with count of number of alarms under that method. The data are in tabular format.</td>
</tr>
<tr>
<td>Alarms Method by Intent</td>
<td>Method name with count of number of alarms under that method. The data are in tabular format.</td>
</tr>
</tbody>
</table>

Vulnerability Assessment Section inside the Executive Dashboard

This section provides you with a way to understand your assets' exposure and measure the remediation cycle. See Vulnerability Assessment for more information.

Widgets in the Vulnerability Assessment Section inside the Executive Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Jobs History</td>
<td>Graph that displays the total number of asset scans on each day in the current month to identify vulnerabilities.</td>
</tr>
<tr>
<td>Number of Vulnerabilities</td>
<td>Total number of vulnerabilities in your environment.</td>
</tr>
<tr>
<td>Top 5 Vulnerable Assets by Score</td>
<td>List of the top five vulnerable assets ordered by score.</td>
</tr>
</tbody>
</table>
Events Section inside the Executive Dashboard

This section displays the security refinement you get when using USM Anywhere, and how it relates to different data sources on your network. See Events Management for more information.

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events Trend</td>
<td>Graph that displays the number of events ingested in USM Anywhere on hourly basis.</td>
</tr>
<tr>
<td>Top 10 Generating Data Sources</td>
<td>List of the top 10 generating data sources based on the number of events ingested.</td>
</tr>
</tbody>
</table>

Actions on the Executive Dashboard

When you open the executive dashboard, there is an Action button in the upper right side of the page.
This button includes these options:

- **Create New Dashboard**: Creates a new dashboard. You can customize your own dashboard with the widgets and content you need. See USM Anywhere Custom Dashboards for more information.

- **Clone Dashboard**: Clones the executive dashboard and you can edit it and customize your own dashboard with the widgets and content you need. See Clone the Executive Dashboard for more information.

Clone the Executive Dashboard

USM Anywhere enables you to clone the executive dashboard and customize the cloned dashboard with the widgets and content you need.

**To clone the Executive Dashboard**

1. Go to **Dashboards > Executive**.
2. Click **Actions > Clone Dashboard**.

   The new dashboard displays in the navigation menu, below Custom Dashboards.
To edit your cloned executive dashboard

1. In the navigation menu, click your cloned executive dashboard.

2. Click **Actions > Edit Dashboard**.

   The Edit Executive Dashboard dialog box opens.
To change the name of your cloned executive dashboard

1. In the navigation menu, click your cloned executive dashboard.
2. Click Actions > Edit Dashboard.

The Edit Executive Dashboard dialog box opens.
3. Modify the title of the dashboard.
4. Click **Save**.

**To change the group name of your cloned executive dashboard**
1. In the navigation menu, click your cloned executive dashboard.
2. Click **Actions > Edit Dashboard**.
   
   The Edit Executive Dashboard dialog box opens.
3. Click the icon next to the group name you want to change.

4. Modify the group name.

5. Click icon to save the group name or the icon to cancel the change.

6. Click Save.

To remove a group of your cloned executive dashboard

1. In the navigation menu, click your cloned executive dashboard.

2. Click Actions > Edit Dashboard.

   The Edit Executive Dashboard dialog box opens.
3. Click the **Remove Group** link next to the group name you want to remove.
4. Click **Save**.

**To modify the widget order of your cloned executive dashboard**

1. In the navigation menu, click your cloned executive dashboard.
2. Click **Actions > Edit Dashboard**.

   The Edit Executive Dashboard dialog box opens.
3. Click the icon and drag the widget to the desired place.

4. Click **Save**.

**To modify the widget row height of your cloned executive dashboard**

1. In the navigation menu, click your cloned executive dashboard.
2. Click **Actions > Edit Dashboard**.
   
   The Edit Executive Dashboard dialog box opens.
3. Click one of these icons and change the widget row height. The values are small, medium, and large.

4. Click Save.

To delete a widget of your cloned executive dashboard

1. In the navigation menu, click your cloned executive dashboard.
2. Click **Actions > Edit Dashboard**.

   The Edit Executive Dashboard dialog box opens.
3. Click the icon next to the widget you want to delete.

4. Click **Save**.

To add a widget in your cloned executive dashboard

1. In the navigation menu, click your cloned executive dashboard.
2. Click **Actions > Edit Dashboard**.

   The Edit Executive Dashboard dialog box opens.
3. Click the **Add Widget** link in the group where you want to add the widget.
4. Select the data you want to add to that widget.
5. Click **Save**.
USM Anywhere includes a set of dashboards that display data collected from your network. Dashboards are visible if you have data for them. Sometimes it takes a few minutes for the dashboards to display.

**Note:** There are dashboards related to the AlienApp you have configured, which are visible if you have data for them. See USM Anywhere AlienApps™ 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.

Dashboards include widgets with important information about your environment. You can find different types of widgets. There are lists, graphs, pie charts, total numbers of a feature or element, and some other ways of presenting the data to have a valuable and quick view of your environment.

Some of the widgets include a filter that you can use to select a predefined range between Last Hour, Last 24 Hours, Last 7 Days, or Last 30 Days. Click the icon to use this filter.

**AlienVault Agent Dashboard**

This dashboard will have data when your environment has deployed agents on the assets. See The AlienVault Agent for more information.
**DEPLOYED AGENTS**

<table>
<thead>
<tr>
<th>Agent Platform</th>
<th>WINDOWS</th>
<th>LINUX</th>
<th>MACOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Agent Version**

- New Version Available: 1
- Current Version: 0

**Agent Status**

- Online: 1
- Offline: 0

**Alarms By Intent**

- System Compromise
- Exploitation & Installation
- Delivery & Attack
- Reconnaissance & Probing
- Environmental Awareness

**Activity**

**Count/Time**

- Last 24 Hours
- Graph showing the number of events over a period of time.

**Top Event Names**

<table>
<thead>
<tr>
<th>EVENT NAME</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset heartbeat</td>
<td>6</td>
</tr>
<tr>
<td>Crypto Miner process detected</td>
<td>4</td>
</tr>
<tr>
<td>Info Heartbeat</td>
<td>4</td>
</tr>
<tr>
<td>Information Gathering tool detected - nmap</td>
<td>4</td>
</tr>
</tbody>
</table>

**File Integrity Monitoring - Top Action**

No data available.

**File Integrity Monitoring - Top File Path**

No data available.

---

**Widgets in the AlienVault Agent Dashboard**

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Platform</td>
<td>Total number of assets with a deployed agent by platform, Windows, macOS, and Linux.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>Total number of agents with the current version installed, and the total number of agents that can be updated to new version using the Update and Troubleshoot AlienVault Agents.</td>
</tr>
<tr>
<td>Agent Status</td>
<td>Total number of agents that are online and offline.</td>
</tr>
<tr>
<td>Alarms By Intent</td>
<td>Alarms are correlated by intent and related to a range of dates. The size of the bubbles depends on the number of issues.</td>
</tr>
<tr>
<td>Count/Time</td>
<td>Graph that shows the number of events over a period of time.</td>
</tr>
<tr>
<td>Top Event Names</td>
<td>List of the top events related to the agent.</td>
</tr>
<tr>
<td>File integrity Monitoring – Top Action</td>
<td>Pie chart displaying, in percentages, the top actions based on integrity changes on those systems.</td>
</tr>
<tr>
<td>File Integrity Monitoring – Top File Path</td>
<td>List of the top file path based on integrity changes on those systems.</td>
</tr>
</tbody>
</table>
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Amazon DynamoDB dashboard. This dashboard displays data when the Amazon Web Services (AWS) CloudTrail data source has been configured and includes Amazon DynamoDB events.

## Widgets in the DynamoDB Dashboard

<table>
<thead>
<tr>
<th><strong>Widgets</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Events By Name</td>
<td>List of events by name.</td>
</tr>
<tr>
<td>Access Control</td>
<td>Pie chart displaying, in percentages, the authentication and access control for DynamoDB.</td>
</tr>
<tr>
<td>Top Tables/Streams</td>
<td>List of the top DynamoDB streams.</td>
</tr>
<tr>
<td>Actions</td>
<td>List of actions supported by Amazon DynamoDB.</td>
</tr>
<tr>
<td>Top Users</td>
<td>List of the Amazon DynamoDB top users.</td>
</tr>
<tr>
<td>User Activity</td>
<td>Users related to their implied activity, which can be create, read, update and delete (CRUD). The size of the bubbles depends on the number of issues.</td>
</tr>
</tbody>
</table>

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Amazon Simple Storage Service (S3) dashboard. This dashboard displays data when the Amazon Web Services (AWS) CloudTrail data source has been configured and receives s3.amazonaws.com events.
### Widgets in the Amazon S3 Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events By Name</td>
<td>List of events by name.</td>
</tr>
<tr>
<td>Top Buckets</td>
<td>Top of Amazon S3 resources that can store objects from different S3 storage tiers.</td>
</tr>
<tr>
<td>Top Users</td>
<td>List of the Amazon S3 top users.</td>
</tr>
<tr>
<td>Access Control</td>
<td>Pie chart displaying, in percentages, the authentication and access control for Amazon S3.</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>Pie chart displaying, in percentages, the authentication mode for Amazon S3.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Pie chart displaying, in percentages, the authentication type for Amazon S3.</td>
</tr>
<tr>
<td>Actions</td>
<td>List of actions supported by Amazon S3.</td>
</tr>
<tr>
<td>User Activity</td>
<td>Users related to their implied activity, which can be create, read, update and delete. The size of the bubbles depends on the number of issues.</td>
</tr>
</tbody>
</table>

### Amazon VPC Flow Logs Dashboard

The Amazon Virtual Private Cloud (VPC) Flow Logs dashboard only displays events from Amazon VPC Flow Logs when the Amazon VPC Flow Logs data source is used. See [Collect Amazon CloudWatch Logs](#) and [Example: Creating a Suppression Rule for VPC Flow Logs](#) for more information.
Widgets in the AWS VPC Flow Logs Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events by outcome</td>
<td>Pie chart displaying, in percentages, the top AWS VPC Flow Logs events ordered by outcome.</td>
</tr>
<tr>
<td>Rejects by Protocol</td>
<td>Pie chart displaying, in percentages, the top AWS VPC Flow Logs events rejected by protocol.</td>
</tr>
<tr>
<td>Top Blocked Sources</td>
<td>List of the 10 top blocked sources from further access in order to prevent intrusions.</td>
</tr>
<tr>
<td>Top Blocked Destinations</td>
<td>List of the 10 top blocked destinations by AWS VPC Flow Logs.</td>
</tr>
<tr>
<td>Top Source Countries</td>
<td>List of the 10 top source countries.</td>
</tr>
<tr>
<td>Top Destination Countries</td>
<td>List of the 10 top destination countries.</td>
</tr>
</tbody>
</table>
Widgets in the AWS VPC Flow Logs Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Sources with Bad Reputation</td>
<td>List of the 10 top sources with bad reputation.</td>
</tr>
<tr>
<td>Flows Per Hour</td>
<td>Graph that displays the number of events accepted or rejected per hour during the last 24 hours.</td>
</tr>
</tbody>
</table>

AWS Dashboard

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Amazon Web Services dashboard. This dashboard displays data when the Amazon Web Services (AWS) CloudTrail data source has been configured.

USM Anywhere™

User Guide
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages by Source</td>
<td>List of the fifteen assets receiving the most messages.</td>
</tr>
<tr>
<td>Event Action: Create</td>
<td>Total number of assets created for the current day and for the current week.</td>
</tr>
<tr>
<td>Event Action: Update</td>
<td>Total number of assets updated for the current day and for the current week.</td>
</tr>
<tr>
<td>Widgets</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Action: Delete</td>
<td>Total number of assets deleted for the current day and for the current week.</td>
</tr>
<tr>
<td>Event Action: Read</td>
<td>Total number of assets read for the current day and for the current week.</td>
</tr>
<tr>
<td>Unauthorized Activity</td>
<td>List of the unauthorized activity that has been made on events.</td>
</tr>
<tr>
<td>Asset Instances by Type</td>
<td>List of asset instances ordered by type.</td>
</tr>
<tr>
<td>Messages by Outcome</td>
<td>Pie chart displaying, in percentages, the outcome for access control, which can be Allow or Deny.</td>
</tr>
<tr>
<td>Asset States</td>
<td>List of the state of the assets and the total number at each state.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Total number of assets having vulnerabilities, configuration issues, and alarms.</td>
</tr>
<tr>
<td>Asset Instances by Region</td>
<td>Total number of asset instances by region.</td>
</tr>
<tr>
<td>Latest Console Login</td>
<td>Date of the latest console login.</td>
</tr>
<tr>
<td>Account Vendors</td>
<td>Pie chart displaying, in percentages, the known vendor services in AWS.</td>
</tr>
<tr>
<td>User Actions</td>
<td>Users related to the implied action of the event, which can be create, read, update, and delete. The size of the bubbles depends on the number of issues.</td>
</tr>
<tr>
<td>Denied Activity</td>
<td>Sankey diagram which displays the source username, the event name, and the data in which the events were received.</td>
</tr>
</tbody>
</table>

AWS Load Balancer Dashboard

Depending on the USM™ Anywhere Sensor you have installed, the widgets might be visible in the Amazon Web Services (AWS) Load Balancer dashboard. This dashboard is active when the ELBAccess data source has been configured or your environment has the AWS Application Load Balancer installed. See Collect ELB Access Logs for more information.
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events by Outcome</td>
<td>Pie chart displaying, in percentages, the top AWS Load Balancer events ordered by outcome.</td>
</tr>
<tr>
<td>Events by Response Code</td>
<td>Pie chart displaying, in percentages, the main events by response code.</td>
</tr>
<tr>
<td>Events by TLS Version</td>
<td>Pie chart displaying, in percentages, the main events by Transport Layer Security (TLS) Version.</td>
</tr>
<tr>
<td>Events by Device</td>
<td>List of the main events by device.</td>
</tr>
<tr>
<td>HTTP 4xx Error Codes</td>
<td>Graph that displays the HTTP4xx error codes by periods of time.</td>
</tr>
<tr>
<td>Top URL with Errors</td>
<td>List of the top URL with errors.</td>
</tr>
<tr>
<td>HTTP 5xx Error Codes</td>
<td>Graph that displays the HTTP 5xx error codes by periods of time.</td>
</tr>
</tbody>
</table>
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Microsoft Azure dashboard. This dashboard displays data when the Azure Cloud data source has been configured.

**Widgets in the Azure Dashboard**

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages by Severity</td>
<td>Pie chart displaying, in percentages, the received messages by severity.</td>
</tr>
<tr>
<td>Activity by User</td>
<td>List of the top five users with the most activity.</td>
</tr>
<tr>
<td>Events by Provider</td>
<td>List of the events by provider.</td>
</tr>
<tr>
<td>Top Denied Users</td>
<td>List of the top denied users.</td>
</tr>
<tr>
<td>Events by Resource</td>
<td>List of the events by resource.</td>
</tr>
<tr>
<td>Unauthorized Activity</td>
<td>List of the unauthorized activity.</td>
</tr>
<tr>
<td>Number of VMs</td>
<td>Total number of virtual machines (VMs) installed.</td>
</tr>
<tr>
<td>VMs by OS</td>
<td>Total number of virtual machines (VMs) installed by operating system (OS).</td>
</tr>
<tr>
<td>VMs by Region</td>
<td>Total number of virtual machines (VMs) installed by region.</td>
</tr>
<tr>
<td>VMs by Size</td>
<td>Total number of virtual machines (VMs) installed by size.</td>
</tr>
</tbody>
</table>
Box Dashboard

The Box dashboard displays a summary of the events originating from Box logs. This option is visible if there are Box events. See The AlienApp for Box for more information.

Widgets in the Box Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>List of top events detected by Box</td>
</tr>
<tr>
<td>Box Activity</td>
<td>Graph that displays the activity in Box by periods of time</td>
</tr>
<tr>
<td>User Activity</td>
<td>List of the five users that have more activity in Box</td>
</tr>
<tr>
<td>Top File Names</td>
<td>List of the top five file names in Box</td>
</tr>
<tr>
<td>Login by Country</td>
<td>List of the top five logins in Box</td>
</tr>
<tr>
<td>Top Users With Failed Logins</td>
<td>List of the top five failed logins by user</td>
</tr>
</tbody>
</table>

The widgets might be visible in the Cisco AMP dashboard if there are Cisco AMP events. See AlienApp for Cisco Secure Endpoint for more information.
Widgets in Cisco AMP Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events over Time</td>
<td>Graphs that displays events over time.</td>
</tr>
<tr>
<td>Events by Name</td>
<td>Pie chart displaying, in percentages, the top events by name.</td>
</tr>
<tr>
<td>Threat Detected</td>
<td>Total of Cisco events with the name 'Thread Detected'.</td>
</tr>
<tr>
<td>Top Alarms</td>
<td>List of top alarms ordered by event name.</td>
</tr>
<tr>
<td>Multiple Infected Files</td>
<td>Total of multiple infected files.</td>
</tr>
<tr>
<td>Top Source</td>
<td>List of top sources.</td>
</tr>
<tr>
<td>Activity by Host</td>
<td>Top Cisco AMP activity by host.</td>
</tr>
<tr>
<td>Malicious Activity Detection</td>
<td>Total of malicious activity detected by Cisco AMP.</td>
</tr>
</tbody>
</table>

The widgets might be visible in the Cisco Meraki dashboard if there are Cisco Meraki events.
Widgets in Cisco Meraki Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count/Time</td>
<td>Graph that shows the number of issues over a period of time.</td>
</tr>
<tr>
<td>Top Device Categories</td>
<td>List of the top device categories on Cisco Meraki.</td>
</tr>
<tr>
<td>HTTP Hostname</td>
<td>Pie chart displaying, in percentages, the specific host names and IP addresses that are visited by clients on your network.</td>
</tr>
<tr>
<td>Top Categories</td>
<td>Total number of top supported syslog event types.</td>
</tr>
<tr>
<td>Reporting Device Hostname</td>
<td>List of reporting device hostnames.</td>
</tr>
</tbody>
</table>

Cisco Umbrella Dashboard

This option is visible if there are Cisco Umbrella events.

User Guide
**Widgets in Cisco Umbrella Dashboard**

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events By Action</td>
<td>Pie chart displaying, in percentages, the events detected by action.</td>
</tr>
<tr>
<td>Top Blocked Categories</td>
<td>Pie chart displaying, in percentages, the top blocked categories.</td>
</tr>
<tr>
<td>Number Of Events By Identity</td>
<td>Pie chart displaying, in percentages, the number of events by identity.</td>
</tr>
<tr>
<td>Top Domains</td>
<td>List of the top 5 popular domains in order of popularity.</td>
</tr>
<tr>
<td>Top Categories</td>
<td>List of the top 5 content categories on Cisco Umbrella.</td>
</tr>
<tr>
<td>Top Blocked Domains</td>
<td>List of the top 5 domains blocked by Cisco Umbrella.</td>
</tr>
<tr>
<td>Top Blocked Identities</td>
<td>List of the top 5 identities blocked by Cisco Umbrella.</td>
</tr>
<tr>
<td>Blocked Activity</td>
<td>Sankey diagram which displays the blocked activity detected by Cisco Umbrella.</td>
</tr>
</tbody>
</table>
The widgets might be visible in the Cloudflare dashboard if there are Cloudflare events. See the AlienApp™ for Cloudflare for more information.

### Widgets in Cloudflare Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Pie chart displaying, in percentages, the platforms detected by Cloudflare</td>
</tr>
<tr>
<td>Top Hostnames</td>
<td>List of the top hostnames on Cloudflare</td>
</tr>
<tr>
<td>Top Events</td>
<td>List of the top events detected by Cloudflare</td>
</tr>
<tr>
<td>TLS Version</td>
<td>Pie chart displaying, in percentages, the main events by Transport Layer Security (TLS) Version</td>
</tr>
<tr>
<td>TLS Cipher</td>
<td>Pie chart displaying, in percentages, the main events by Transport Layer Security (TLS) Cipher</td>
</tr>
</tbody>
</table>

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the BlackBerry Cylance dashboard. This dashboard displays data when the CylancePROTECT data source has been configured.
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices by platform</td>
<td>Pie chart displaying, in percentages, the connected devices by platform.</td>
</tr>
<tr>
<td>Stats</td>
<td>Total number of connected devices, threats, and devices with threats.</td>
</tr>
<tr>
<td>Top Exploits Attempts by Category</td>
<td>Pie chart displaying, in percentages, the top exploit attempts by category.</td>
</tr>
<tr>
<td>Top Users by Number of Threats</td>
<td>List of the top users by number of threats.</td>
</tr>
<tr>
<td>Top Devices by Number of Threats</td>
<td>List of the top devices by number of threats.</td>
</tr>
<tr>
<td>Top Exploits Attempts by Process</td>
<td>List of the top exploit attempts by process.</td>
</tr>
<tr>
<td>Top Exploits Attempts by Device</td>
<td>List of the top exploit attempts by device.</td>
</tr>
</tbody>
</table>
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the FireEye dashboard. This dashboard displays data when the Reporting Device Vendor field has the FireEye value.

### Widgets in the FireEye Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Types</td>
<td>List of alerts by type.</td>
</tr>
<tr>
<td>Severity</td>
<td>Pie chart displaying, in percentages, the detected severity.</td>
</tr>
<tr>
<td>Alerts by Device</td>
<td>Total number of alerts by device.</td>
</tr>
<tr>
<td>Top Sources</td>
<td>List of the top sources.</td>
</tr>
<tr>
<td>Top Ports</td>
<td>Pie chart displaying, in percentages, the top ports.</td>
</tr>
</tbody>
</table>

#### Alert Types
- malware-object
- domain-match
- web-infection
- malware-callback
- infection-match

#### Top Sources
1. NA-testing.fenotify-examples.com: 8
2. abc123.example.com: 3
3. dev0001sav02.example.com: 2
4. rescomp-09-497335.Stanford.RDU: 2

#### Top Malware
- FireEye-TestEvent SIG: 9
- Trojan.Generic:DNS: 7
- Malware Binary.URL: 2
- Trojan:Peake:2: 2
- Exploit:Browser: 1

#### Daily Activity Per Hour
- malware-object
- domain-match
- web-infection
- malware-callback
- infection-match
Widgets in the FireEye Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Destinations</td>
<td>List of the top destinations.</td>
</tr>
<tr>
<td>Top Malware</td>
<td>List of the top malware.</td>
</tr>
<tr>
<td>Last Alerts</td>
<td>List of the last-detected alerts.</td>
</tr>
<tr>
<td>Daily Activity Per Hour</td>
<td>Graph that displays the daily activity per hour.</td>
</tr>
</tbody>
</table>

FortiGate Dashboard

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Fortinet FortiGate dashboard. This dashboard displays data when the FortiGate data source has been configured.
Widgets in the FortiGate Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Pie chart displaying, in percentages, the actions supported by FortiGate.</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>List of the ten top intrusion prevention events.</td>
</tr>
<tr>
<td>Top Blocked Users</td>
<td>List of the five top blocked users by FortiGate.</td>
</tr>
<tr>
<td>Events by Severity</td>
<td>Pie chart containing percentage of FortiGate events by severity.</td>
</tr>
<tr>
<td>Applications</td>
<td>List of the ten top applications detected in the events.</td>
</tr>
<tr>
<td>Inbound Traffic Per Hour by Interface</td>
<td>Graph that displays the inbound traffic per hour and by interface.</td>
</tr>
<tr>
<td>Outbound traffic Per Hour by Interface</td>
<td>Graph that displays the outbound traffic per hour and by interface.</td>
</tr>
</tbody>
</table>

Google Cloud Platform Dashboard

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Google Cloud Platform dashboard. This dashboard displays data when the Google Cloud Audit data source has been configured.

Role Availability

- Read-Only
- Analyst
- Manager

Activity By Project

- 98.3% sploitation-developer
- 14% 308/340/448/448
- 37% rloginPolicy 23093

Unauthorized Activity

Asset Instances By Type

No data available.

Asset States

No data available.

Asset Information

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Configuration Issues</th>
<th>Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Asset Instances By Region

No data available.
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages by Source</td>
<td>List of the top sources receiving the most messages.</td>
</tr>
<tr>
<td>Activity by Project</td>
<td>Pie chart displaying, in percentages, the top projects with the most activity.</td>
</tr>
<tr>
<td>Unauthorized Activity</td>
<td>List of the unauthorized activity.</td>
</tr>
<tr>
<td>Top Users</td>
<td>List of the top users.</td>
</tr>
<tr>
<td>Top Actions</td>
<td>Pie chart displaying the top actions in Google Cloud Platform.</td>
</tr>
<tr>
<td>Asset Instances by Type</td>
<td>List of assets instances ordered by type.</td>
</tr>
<tr>
<td>Messages by Outcome</td>
<td>Pie chart displaying, in percentages, the outcome for access control, which can be Allow or Deny.</td>
</tr>
<tr>
<td>Asset States</td>
<td>List of the state of the assets and the total number at each asset.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Total number of assets having vulnerabilities, configuration issues, and alarms.</td>
</tr>
<tr>
<td>Asset Instances by Region</td>
<td>Total number of assets instances by region.</td>
</tr>
</tbody>
</table>

**Google G Suite Audit Dashboard**

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Google G Suite audit dashboard. This dashboard displays data when the G Suite audit data source has been configured.

**USM Anywhere™ User Guide**
## Widgets in G Suite Audit Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Attempts</td>
<td>Pie chart displaying, in percentages, the successful and unsuccessful login attempts to G Suite Audit.</td>
</tr>
<tr>
<td>Failed Login By User</td>
<td>List of the failed login by user.</td>
</tr>
<tr>
<td>Login Failed Reasons</td>
<td>Pie chart displaying, in percentages, the reasons of the failed login.</td>
</tr>
<tr>
<td>Top Category</td>
<td>List of the top 5 G Suite Audit category.</td>
</tr>
<tr>
<td>Failed Login By Address</td>
<td>List of the 5 failed login in G Suite Audit by address.</td>
</tr>
<tr>
<td>Login By Country</td>
<td>List of the 5 login in G Suite Audit by country.</td>
</tr>
<tr>
<td>Recently Authorized Applications</td>
<td>List of the recently authorized applications by G Suite Audit.</td>
</tr>
<tr>
<td>Top Actions</td>
<td>List of the top 5 actions in G Suite Audit.</td>
</tr>
<tr>
<td>Login Activity</td>
<td>Graph that displays the successful and unsuccessful login attempts to G Suite Audit.</td>
</tr>
<tr>
<td>Authorized Applications</td>
<td>Sankey diagram which displays the authorized applications by G Suite Audit.</td>
</tr>
</tbody>
</table>

### Google G Suite Drive Dashboard

**Role Availability**

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

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Google G Suite Drive dashboard. This dashboard displays data when the G Suite Drive data source has been configured.
Widgets in the Google G Suite Audit Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>List of top events detected by Google G Suite Audit.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Pie chart displaying, in percentages the type of resource in Google G Suite Audit.</td>
</tr>
<tr>
<td>Top Category</td>
<td>List of the top Google G Suite Audit category.</td>
</tr>
<tr>
<td>User Activity</td>
<td>List of the 5 users that have more activity in Google G Suite Audit.</td>
</tr>
<tr>
<td>Top File Names</td>
<td>List of the top 5 file names in Google G Suite Audit.</td>
</tr>
<tr>
<td>Activity</td>
<td>Graph that displays the activity in Google G Suite Audit by periods of time.</td>
</tr>
</tbody>
</table>

McAfee ePO Dashboard

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the McAfee ePO dashboard. This dashboard displays data when the McAfee ePO data source has been configured. See The AlienApp™ for McAfee ePO for more information.

**TOP EVENTS**

- Dec 16 2016 - Jan 15 2017
  - 48.0% The update is running
  - 47.5% The update was successful
  - 2.3% file infected, No cleaner
  - 2.1% Other

**EVENT BY SEVERITY**

- Dec 16 2016 - Jan 15 2017
  - 95.7% Informational
  - 2.3% Major
  - 1.0% Minor
  - 0.4% Warning

**EVENTS BY ACTION**

- Dec 16 2016 - Jan 15 2017
  - 59.4% deleted
  - 21.0% blocked
  - 18.0% would deny execute

**TOP MALWARE FAMILIES**

<table>
<thead>
<tr>
<th>FAMILY</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESCAP list file</td>
<td>95</td>
</tr>
<tr>
<td>Protección estándar de antivirus</td>
<td>35</td>
</tr>
<tr>
<td>Protección común</td>
<td>10</td>
</tr>
<tr>
<td>Common Standard Protection</td>
<td>10</td>
</tr>
</tbody>
</table>

**TOP HOSTS**

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows/ePO</td>
<td>3,975</td>
</tr>
<tr>
<td>Drezet</td>
<td>160</td>
</tr>
</tbody>
</table>

**TOP USERS**

<table>
<thead>
<tr>
<th>Dec 16 2016 - Jan 15 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.0% SYSTEM</td>
</tr>
<tr>
<td>2.0% Drezet/Admistrator</td>
</tr>
<tr>
<td>0.5% Windows/ePO/Admistrator</td>
</tr>
</tbody>
</table>

**DAILY ACTIVITY PER HOUR**

- 2
- 1.5
- 1
- 0.5
- 0

6:00 PM | 8:00 PM | 10:00 PM | 12:00 AM | 2:00 AM | 4:00 AM | 6:00 AM | 8:00 AM | 10:00 AM | 12:00 PM | 2:00 PM | 4:00 PM
## Widgets in the McAfee ePO Dashboard

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>Pie chart displaying, in percentages, the top events detected by McAfee ePO.</td>
</tr>
<tr>
<td>Event by Severity</td>
<td>Pie chart containing percentage of McAfee ePO per severity.</td>
</tr>
<tr>
<td>Events by Action</td>
<td>Pie chart displaying, in percentages, the events detected by action.</td>
</tr>
<tr>
<td>Top Malware Families</td>
<td>List of the top malware families expressed in total numbers.</td>
</tr>
<tr>
<td>Top Hosts</td>
<td>List of top hosts expressed in total numbers.</td>
</tr>
<tr>
<td>Top Users</td>
<td>Pie chart containing percentage of McAfee ePO logs per user.</td>
</tr>
<tr>
<td>Daily Activity Per Hour</td>
<td>Graph that displays the daily activity of McAfee ePO per hour.</td>
</tr>
</tbody>
</table>

## Microsoft ATA Dashboard

The widgets might be visible in the Microsoft Advanced Threat Analytics (ATA) dashboard if there are Microsoft Advanced Threat Analytics events.
# Widgets in Microsoft ATA Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Activity</td>
<td>Graph that shows the number of events over a period of time.</td>
</tr>
<tr>
<td>Alarms Over Time</td>
<td>Graph that shows the number of alarms over a period of time.</td>
</tr>
<tr>
<td>Top Active Users</td>
<td>List of the Microsoft ATA top active users.</td>
</tr>
<tr>
<td>Top Applications</td>
<td>List of the ten top applications detected in the events.</td>
</tr>
<tr>
<td>Top Failures</td>
<td>List of the Microsoft ATA top failures.</td>
</tr>
<tr>
<td>Top Events by Severity</td>
<td>Pie chart containing percentage of Microsoft ATA events by severity.</td>
</tr>
<tr>
<td>Top Activity by Host</td>
<td>List of the Microsoft ATA top activity by host.</td>
</tr>
</tbody>
</table>

---

## MITRE ATT&CK Dashboard

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This dashboard includes the tactics and techniques to describe adversarial actions and behaviors. Techniques are specific actions an attacker might take, and tactics are phases of attacker behavior. See [MITRE ATT&CK](https://attack.mitre.org) and [Alarms List View](https://www.att.com) for more information.

### Note:
You can watch the [How to improve threat detection and response with the MITRE ATT&CK framework](https://www.att.com) customer training webcast on-demand to learn how to use MITRE ATT&CK within USM Anywhere.

---

# USM Anywhere™

## User Guide
Widgets in the MITRE ATT&CK Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Widgets</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>MITRE ATT&amp;CK</td>
<td>Table with Tactics and Techniques, see Alarms List View for more information.</td>
</tr>
<tr>
<td>Command and Control Top Assets</td>
<td>The command and control tactic represents how adversaries communicate with systems under their control within a target network.</td>
</tr>
</tbody>
</table>
## Widgets in the MITRE ATT&CK Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exfiltration Top Assets</td>
<td>Exfiltration refers to techniques and attributes that result or aid in the adversary stealing files and information from a target network.</td>
</tr>
<tr>
<td>Privilege Escalation Top Assets</td>
<td>Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network.</td>
</tr>
<tr>
<td>Lateral Movement Top Assets</td>
<td>Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems.</td>
</tr>
<tr>
<td>Credential Access Top Assets</td>
<td>Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment.</td>
</tr>
<tr>
<td>Discovery Top Assets</td>
<td>Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network.</td>
</tr>
<tr>
<td>Defense Evasion Top Assets</td>
<td>Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses.</td>
</tr>
<tr>
<td>Persistence Top Assets</td>
<td>Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.</td>
</tr>
<tr>
<td>Execution Top Assets</td>
<td>The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system.</td>
</tr>
<tr>
<td>Collection Top Assets</td>
<td>Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration.</td>
</tr>
<tr>
<td>Initial Access Top Assets</td>
<td>The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network.</td>
</tr>
</tbody>
</table>

### MobileIron Threat Defense Dashboard

**Role Availability**

- Read-Only
- Analyst
- Manager

The MobileIron Threat Defense dashboard is available when the MobileIron Threat Defense (MTD) source has been configured and includes MobileIron events. See AlienApp for MobileIron Threat Defense for more information.

### USM Anywhere™ User Guide
Widgets in the MobileIron Threat Defense Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Activity</td>
<td>Graph that shows the number of events over a period of time.</td>
</tr>
<tr>
<td>Top Alerts</td>
<td>Graph that shows the number of alarms over a period of time.</td>
</tr>
<tr>
<td>Top Event Types</td>
<td>Pie chart displaying, in percentages, the top events types related to the MTD.</td>
</tr>
<tr>
<td>Top Event Severities</td>
<td>Pie chart displaying, in percentages, the top events severities related to the MTD.</td>
</tr>
<tr>
<td>Events by Platform</td>
<td>Pie chart displaying, in percentages, the top events by platform related to the MTD.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Total number of assets having not upgraded Apple iOS, not upgraded Android, not upgradable iOS, and not upgradable Android.</td>
</tr>
<tr>
<td>Critical Events</td>
<td>Total number of critical MobileIron events.</td>
</tr>
</tbody>
</table>

depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the network-based intrusion detection system (NIDS) dashboard. This dashboard displays data when the AlienVault NIDS data source has been configured.
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Microsoft Azure Active Directory (AD) dashboard. This dashboard displays a summary of the events originating from the Azure AD logs, so your environment must have configured the Azure AD data source.

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets with Malware Activity</td>
<td>Total number of assets with malware activity for the current day and for the current week.</td>
</tr>
<tr>
<td>Top Categories</td>
<td>List of the top categories expressed in total numbers.</td>
</tr>
<tr>
<td>Top Signatures</td>
<td>List of the top NIDS signatures having more events.</td>
</tr>
<tr>
<td>Top Malware Families</td>
<td>List of the top malware families expressed in total numbers.</td>
</tr>
<tr>
<td>Top Malware Destination</td>
<td>List of the top malware ordered by destination country.</td>
</tr>
<tr>
<td>Top Categories/SubCategories</td>
<td>List of the top categories and subcategories expressed in total numbers.</td>
</tr>
<tr>
<td>Top Exploit Activity</td>
<td>List of the top exploit activity in your environment.</td>
</tr>
<tr>
<td>Top Malware</td>
<td>List of the top malware in your environment.</td>
</tr>
</tbody>
</table>
Widgets in the Office 365 Azure Active Directory Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Attempts</td>
<td>Pie chart displaying, in percentages, the successful and unsuccessful login attempts to Office 365 Azure Active Directory.</td>
</tr>
<tr>
<td>Failed Login By User</td>
<td>List of the 5 failed login by user.</td>
</tr>
<tr>
<td>Login Failed Reasons</td>
<td>Pie chart displaying, in percentages, the reasons of the failed login.</td>
</tr>
<tr>
<td>Top Events</td>
<td>List of top events detected by Office 365 Azure Active Directory.</td>
</tr>
<tr>
<td>Failed Login By Address</td>
<td>List of the 5 failed login in Office 365 Azure Active Directory.</td>
</tr>
<tr>
<td>Login By Country</td>
<td>List of the 5 login in Office 365 Azure Active Directory.</td>
</tr>
<tr>
<td>Login Activity</td>
<td>Graph that displays the successful and unsuccessful login attempts to Office 365 Azure Active Directory.</td>
</tr>
</tbody>
</table>

Depending on the USM Anywhere™ sensor you have installed, the widgets might be visible in the Microsoft OneDrive dashboard. This dashboard displays a summary of the events originating from the OneDrive logs, so your environment must have configured the Microsoft SharePoint data source and the OneDrive application.
Widgets in the Office 365 OneDrive Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>List of top events detected by Office 365 OneDrive.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Pie chart displaying, in percentages the type of resource in Office 365 OneDrive.</td>
</tr>
<tr>
<td>File Types</td>
<td>Pie chart displaying, in percentages the type of files in Office 365 OneDrive.</td>
</tr>
<tr>
<td>Activity</td>
<td>Graph that displays the activity in Office 365 OneDrive by periods of time.</td>
</tr>
<tr>
<td>Top User Agents</td>
<td>List of the top 5 user agents used by Office 365 OneDrive.</td>
</tr>
<tr>
<td>User Activity</td>
<td>List of the 5 users that have more activity in Office 365 OneDrive.</td>
</tr>
</tbody>
</table>

Office 365 SharePoint Dashboard

Depending on the USM Anywhere™ sensor you have installed, the widgets might be visible in the Microsoft SharePoint dashboard. This dashboard displays a summary of the events originating from the SharePoint logs, so your environment must have configured the Microsoft SharePoint data source and the SharePoint application.
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>List of top events detected by Office 365 SharePoint.</td>
</tr>
<tr>
<td>Resource Type</td>
<td>Pie chart displaying, in percentages the type of resource in Office 365 SharePoint.</td>
</tr>
<tr>
<td>File Types</td>
<td>Pie chart displaying, in percentages the type of files in Office 365 SharePoint.</td>
</tr>
<tr>
<td>Activity</td>
<td>Graph that displays the activity in Office 365 SharePoint by periods of time.</td>
</tr>
<tr>
<td>Top User Agents</td>
<td>List of the top 5 user agents used by Office 365 SharePoint.</td>
</tr>
<tr>
<td>User Activity</td>
<td>List of the 5 users that have more activity in Office 365 SharePoint.</td>
</tr>
</tbody>
</table>

**Okta Dashboard**

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

Depending on the USM Anywhere sensor you have installed, the widgets might be visible in the Okta dashboard. This dashboard displays data when the Okta data source has been configured. See The AlienApp™ for Okta for more information.
Widgets in the Okta Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events by Name</td>
<td>List of the ten top Okta events by name.</td>
</tr>
<tr>
<td>Failed Actions</td>
<td>List of the ten top failed actions related with Okta.</td>
</tr>
<tr>
<td>Event Outcome</td>
<td>Pie chart displaying, in percentages, the successful and failed event outcomes.</td>
</tr>
<tr>
<td>Top Users with Failed Actions</td>
<td>List of the top users with failed actions.</td>
</tr>
<tr>
<td>Top Applications</td>
<td>List of the ten top applications detected in the events.</td>
</tr>
<tr>
<td>Top Users</td>
<td>List of the ten top users in Okta.</td>
</tr>
<tr>
<td>Top Categories</td>
<td>List of the top Okta categories.</td>
</tr>
<tr>
<td>User Activity</td>
<td>Sankey diagram that displays the Okta user activity.</td>
</tr>
</tbody>
</table>

Open Threat Exchange Dashboard

The AT&T Alien Labs™ Open Threat Exchange® (OTX™) dashboard displays if raw pulse data points are received. See Open Threat Exchange® and USM Anywhere for more information.
Sometimes you may see the IP Reputation widgets contain data but the OTX Pulse widgets do not. This is because IP Reputation widgets include all suspicious IP addresses, but OTX Pulse widgets only contain data when the suspicious IP is reported as an IOC for a pulse. See About OTX for the difference between pulses and IP Reputation.

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Reputation Activity</td>
<td>Graph that displays the IP reputation activity.</td>
</tr>
<tr>
<td>IP Reputation by Activity</td>
<td>Pie chart displaying, in percentages, the IP Reputation by activity.</td>
</tr>
<tr>
<td>IP Reputation Activity By Data Source</td>
<td>Pie chart displaying, in percentages, the IP Reputation by data source.</td>
</tr>
<tr>
<td>OTX Activity</td>
<td>Graph that displays the OTX activity.</td>
</tr>
<tr>
<td>OTX Activity By Data Source</td>
<td>Pie chart displaying, in percentages, the OTX activity by data source.</td>
</tr>
<tr>
<td>Top OTX Pulse Indicators of Compromise</td>
<td>List of the top indicators of compromise that identify a specific threat.</td>
</tr>
<tr>
<td>Top Pulses</td>
<td>Top 5 Threat Events</td>
</tr>
<tr>
<td>Top Sources with OTX Pulse Activity</td>
<td>List of the top 5 source IPs, which are identified by OTX as potential malicious activity.</td>
</tr>
<tr>
<td>Top Destinations with OTX Pulse Activity</td>
<td>List of the top 5 destinations IPs, which are identified by OTX as potential malicious activity.</td>
</tr>
</tbody>
</table>

Overview Dashboard

This dashboard includes three separate sections.

SIEM Section
SIEM security intelligence combines and correlates collected logs and other data to find malicious patterns in network traffic and within host activity.
### Widgets in the SIEM Section

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>Total number of alarms for the current day and for the current week.</td>
</tr>
<tr>
<td>Alarms by Intent</td>
<td>Alarms correlated by intent and related to a range of dates. The size of the bubbles depends on the number of issues.</td>
</tr>
<tr>
<td>Top Alarms by Method</td>
<td>List of the top 5 alarms ordered by the method of attack or infiltration and including the total number of alarms.</td>
</tr>
<tr>
<td>Event Data Sources</td>
<td>Most seen data sources to normalize events.</td>
</tr>
<tr>
<td>Events Trend</td>
<td>Graph that displays the trend in events.</td>
</tr>
<tr>
<td>Sensor Activity</td>
<td>Top sensor activity by events and alarms.</td>
</tr>
</tbody>
</table>

### Asset Discovery Section

Asset Discovery discovers assets in your environment, detects changes in assets, and discovers malicious assets in the network.

### Widgets in the Asset Discovery Section

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Operating Systems</td>
<td>List of the top operating systems on assets.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Software Inventory refers to the total number of assets having software installed. Assets Discovered refers to the total number of assets discovered by the user.</td>
</tr>
<tr>
<td>Top Assets with Alarms</td>
<td>List of the top 5 assets having the most alarms.</td>
</tr>
</tbody>
</table>

### Vulnerability Assessment Section

Vulnerability Assessment identify vulnerabilities or compliance by comparing the installed software on assets with a database of known vulnerabilities.

---

1Some widgets include a filter. You can hover over the filter to see the details.
## Widgets in the Vulnerability Assessment Section

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets with Vulnerabilities</td>
<td>Total number of assets having vulnerabilities for the current day and for the current week.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Total number of vulnerabilities in your environment.</td>
</tr>
<tr>
<td>Vulnerabilities by Severity</td>
<td>Top vulnerabilities ordered by severity. See About Vulnerability Severity</td>
</tr>
<tr>
<td>Most Vulnerable Assets</td>
<td>List of most vulnerable assets.</td>
</tr>
</tbody>
</table>

### Palo Alto Networks Dashboard

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

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Palo Alto Networks dashboard. This dashboard displays data when the Palo Alto PAN-OS data source has been configured. See The AlienApp™ for Palo Alto Networks for more information.

---

**USM Anywhere™
User Guide**
Widgets in the Palo Alto Networks Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories</td>
<td>Pie chart displaying, in percentages, the Palo Alto Networks categories.</td>
</tr>
<tr>
<td>Applications</td>
<td>Pie chart displaying, in percentages, the Palo Alto Networks applications.</td>
</tr>
<tr>
<td>Threats</td>
<td>Pie chart displaying, in percentages, the threats detected by Palo Alto Networks.</td>
</tr>
<tr>
<td>Top Thread Users</td>
<td>List of the top thread users expressed in total numbers.</td>
</tr>
<tr>
<td>Outcomes</td>
<td>List of the top Palo Alto Networks outcomes expressed in total numbers.</td>
</tr>
<tr>
<td>Top Signatures</td>
<td>List of the top Palo Alto Networks signatures.</td>
</tr>
<tr>
<td>Top Malware</td>
<td>List of the top malware in your environment.</td>
</tr>
</tbody>
</table>

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the SonicWall dashboard. This dashboard displays data when the SonicWall data source has been configured.
Widgets in the SonicWall Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Policies</td>
<td>Pie chart displaying, in percentages the top ten SonicWall policies.</td>
</tr>
<tr>
<td>Severity</td>
<td>Pie chart displaying, in percentages the top event severity.</td>
</tr>
<tr>
<td>User Activity</td>
<td>Pie chart displaying, in percentages the top users by activity.</td>
</tr>
<tr>
<td>Top Categories</td>
<td>List of the top categories expressed in total numbers.</td>
</tr>
<tr>
<td>Top Events</td>
<td>List of the top SonicWall events expressed in total numbers.</td>
</tr>
<tr>
<td>Top Users</td>
<td>List of the top users expressed in total numbers.</td>
</tr>
<tr>
<td>Top Web Categories</td>
<td>List of the top web categories expressed in total numbers.</td>
</tr>
<tr>
<td>Top Source Countries</td>
<td>List of the top source countries expressed in total numbers.</td>
</tr>
<tr>
<td>Top Destination Countries</td>
<td>List of the top destination countries expressed in total numbers.</td>
</tr>
</tbody>
</table>

Sophos UTM Dashboard
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the Sophos Unified Threat Management (UTM) dashboard. This dashboard displays data when the Sophos UTM data source has been configured.

### Widgets in the Sophos UTM Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Pie chart displaying, in percentages, the actions supported by Sophos UTM.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Pie chart displaying, in percentages, the protocols used by Sophos UTM.</td>
</tr>
<tr>
<td>Top Blocked Categories</td>
<td>Pie chart displaying, in percentages, the top blocked categories.</td>
</tr>
<tr>
<td>Categories</td>
<td>List of top categories on Sophos UTM.</td>
</tr>
<tr>
<td>Content Categories</td>
<td>List of top content categories on Sophos UTM.</td>
</tr>
<tr>
<td>Top Blocked Hosts</td>
<td>List of top hosts blocked by Sophos UTM.</td>
</tr>
<tr>
<td>Traffic Per Hour</td>
<td>Graph that displays the traffic detected by Sophos UTM per hour during the last 24 hours.</td>
</tr>
<tr>
<td>Top Blocked Users</td>
<td>List of top users blocked by Sophos UTM.</td>
</tr>
</tbody>
</table>
Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the VMware dashboard. This dashboard displays data when the VMware application programming interface (API) data source has been configured.

### Widgets in the VMware Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Events</td>
<td>List of top events detected by VMware.</td>
</tr>
<tr>
<td>Events by Data Center</td>
<td>Pie chart displaying, in percentages, the VMware events by data center.</td>
</tr>
<tr>
<td>Events by Resource</td>
<td>List of VMware events by resource.</td>
</tr>
<tr>
<td>Logins by Country</td>
<td>List of logins detected by VMware by country.</td>
</tr>
<tr>
<td>User Activity</td>
<td>Pie chart displaying, in percentages, the VMware user by activity.</td>
</tr>
<tr>
<td>Top Denied Users</td>
<td>List of top denied users by VMware.</td>
</tr>
<tr>
<td>VMware Assets</td>
<td>Total number of VMware assets with alarms and total number of VMware assets.</td>
</tr>
</tbody>
</table>
### Widgets

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMs by OS</td>
<td>List of VMware assets by operating system (OS).</td>
</tr>
<tr>
<td>VMware Assets with Alarms</td>
<td>List of VMware assets with the number of detected alarms.</td>
</tr>
</tbody>
</table>

### Vulnerabilities Dashboard

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

If the dashboard does not contain information and there are not detected vulnerabilities, click **Run Authenticated Vulnerability Scan** to run a scan to detect asset vulnerabilities. See [Running Authenticated Asset Scans](#).
Widgets in the Vulnerabilities Dashboard (Continued)

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities by Severity</td>
<td>Pie chart displaying, in percentages, the severity of vulnerabilities, which can be Low, High, and Medium. See About Vulnerability Severity.</td>
</tr>
<tr>
<td>Top Active Vulnerabilities by Severity</td>
<td>List of the top active vulnerabilities by severity. You can see the CVE Identifier, its severity, and the affected assets. See About Vulnerability Severity.</td>
</tr>
<tr>
<td>Latest Scan Jobs</td>
<td>List of the 5 latest scans run in your environment. It includes the scan date and the number of vulnerabilities found.</td>
</tr>
<tr>
<td>Scan Jobs History</td>
<td>Graph that displays the total number vulnerability scans on each day in the current month.</td>
</tr>
</tbody>
</table>

WatchGuard Dashboard

Depending on the USM Anywhere Sensor you have installed, the widgets might be visible in the WatchGuard dashboard. This dashboard displays data when the WatchGuard XTM data source has been configured.

Access Control Outcomes: MAY 08 2019 - JUN 07 2019
- 65.7% Deny
- 33.3% Allow

Transport Protocol: MAY 08 2019 - JUN 07 2019
- 100.0% tcp

Top Signature Categories
- DEVICE EVENT CATEGORY | COUNT
- Virus/Worm | 1

Top Blocked Categories
- CONTENT CATEGORY | COUNT
- Gambling | 1

Top Blocked Hosts
<table>
<thead>
<tr>
<th>HOST</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>2</td>
</tr>
</tbody>
</table>

Traffic Per Hour
- Deny
- Allow
<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Outcomes</td>
<td>Pie chart displaying, in percentages, the access detected by WatchGuard.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Pie chart displaying, in percentages, the protocols detected by WatchGuard.</td>
</tr>
<tr>
<td>Top Signature Categories</td>
<td>List of the top signature categories detected by WatchGuard.</td>
</tr>
<tr>
<td>Top Signatures</td>
<td>List of the top categories detected by WatchGuard.</td>
</tr>
<tr>
<td>Top Blocked Categories</td>
<td>List of the top categories blocked by WatchGuard.</td>
</tr>
<tr>
<td>Top Blocked Hosts</td>
<td>List of the top hosts blocked by WatchGuard.</td>
</tr>
<tr>
<td>Traffic Per Hour</td>
<td>Graph that displays the traffic detected by WatchGuard per hour during the last 24 hours.</td>
</tr>
</tbody>
</table>

**Windows Authentication Dashboard**

This Windows Authentication dashboard displays data when your environment includes Microsoft Windows security auditing events.

**USM Anywhere™**

**User Guide**
### Logon Session Events

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Logon Correlate by Logon ID</td>
<td>4,441</td>
</tr>
<tr>
<td>An account was logged off</td>
<td>3,671</td>
</tr>
<tr>
<td>Special privileges assigned to new logon</td>
<td>3,431</td>
</tr>
<tr>
<td>A logon was attempted using explicit credentials</td>
<td>5</td>
</tr>
</tbody>
</table>

### Logon Types (JUN 18 - JUN 19 2018)

- 90.5% Network logon (i.e. mapped
- 9.5% Service logon (service startup)

### Domain Controller Authentication Events

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Kerberos service ticket was requested</td>
<td>16</td>
</tr>
<tr>
<td>A Kerberos authentication ticket (TGT) was requested</td>
<td>53</td>
</tr>
<tr>
<td>A Kerberos service ticket was renewed</td>
<td>3</td>
</tr>
</tbody>
</table>

### Logon Failure Reasons

No data available.

### Kerberos Failure Codes

<table>
<thead>
<tr>
<th>Failure Code</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>No error</td>
<td>232</td>
</tr>
</tbody>
</table>

### Ticket Encryption Type

100.0% AES256-CTS-HMAC

### Ticket Pre-Authentication Type

100.0% PA-ENC-TIMESTAMP

### Authentication Package

<table>
<thead>
<tr>
<th>Authentication Package Name</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos</td>
<td>3,583</td>
</tr>
<tr>
<td>Negotiate</td>
<td>770</td>
</tr>
<tr>
<td>NTLM</td>
<td>88</td>
</tr>
</tbody>
</table>

### User Account Changes

No data available.

### Group Changes

No data available.

### Remote Desktop Sessions

- 127.0.0.1
- 10.60.100.1
- 10.60.100.40
- 10.60.100.24
- 10.60.100.4
- 10.60.100.21
### Widgets in the Windows Authentication Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Session Events</td>
<td>Displays the logon session events like successful logon, user initiated logoff, logon failure, remote desktop session reconnected/disconnected, workstation locked/unlocked, and screen saver invoked/dismissed.</td>
</tr>
<tr>
<td>Logon types</td>
<td>Displays the logon types like interactive, network, batch, service, unlock, network cleartext, remote desktop, and logon with cached credentials.</td>
</tr>
<tr>
<td>Domain Controller Authentication Events</td>
<td>Top authentication events received by the Domain Controller. For example: Kerberos tickets of any type (authentication, services).</td>
</tr>
<tr>
<td>Logon Failure Reasons</td>
<td>Top logon failure reasons in the Active Directory. For example: incorrect usernames or bad passwords.</td>
</tr>
<tr>
<td>Kerberos Failure Codes</td>
<td>Top error codes generated by Kerberos service. For example: errors received during authentication and service requests.</td>
</tr>
<tr>
<td>Ticket Encryption Type</td>
<td>Pie chart containing the different encryption types used in Kerberos. For example: DES, RC4, AES, etc.</td>
</tr>
<tr>
<td>Ticket Pre-Authentication Type</td>
<td>Pie chart containing the different Pre-Authentication types used in Kerberos. For example: timestamp, salt, etc.</td>
</tr>
<tr>
<td>Authentication Package</td>
<td>Top Active Directory authentication packet types. For example: Kerberos or NTLM.</td>
</tr>
<tr>
<td>User Account Changes</td>
<td>Displays the user account changes like created, enabled, disabled, deleted, etc.</td>
</tr>
<tr>
<td>Group Changes</td>
<td>Displays the group changes like created, changed, deleted. It also displays if a member has been added or removed.</td>
</tr>
<tr>
<td>Remote Desktop Sessions</td>
<td>Sankey diagram containing remote connections between the different users and destination hosts.</td>
</tr>
</tbody>
</table>

### Windows Dashboard

The Microsoft Windows dashboard will have data when your environment includes NXLog Windows events, Microsoft Azure Windows events, Elastic Winlogbeat Windows events, or AlienVault Agent - Windows EventLog events.
Widgets in the Windows Dashboard

<table>
<thead>
<tr>
<th>Widgets</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events by Channel</td>
<td>Pie chart containing the different channels populating the Windows Event Log. For example: System, Security or Application.</td>
</tr>
<tr>
<td>Top Users</td>
<td>Pie chart containing percentage of Windows Event Logs per user.</td>
</tr>
<tr>
<td>Events by Severity</td>
<td>Pie chart containing percentage of Windows Event Log per severity.</td>
</tr>
<tr>
<td>Top Events</td>
<td>Displays a list of top Windows Events.</td>
</tr>
<tr>
<td>Top Hosts</td>
<td>Top Windows hosts based on Windows Event Logs generated.</td>
</tr>
<tr>
<td>Top Processes</td>
<td>Displays a list of the top Windows processes.</td>
</tr>
<tr>
<td>Top Security Categories</td>
<td>Displays a list of security categories.</td>
</tr>
<tr>
<td>Activity</td>
<td>Timeline graph displaying Windows activity by event category.</td>
</tr>
</tbody>
</table>

USM Anywhere Custom Dashboards

Role Availability

Read-Only ✓ Analyst ✓ Manager ✓

USM Anywhere enables you to create and customize your own dashboards with the widgets and content you need.

Edition: This feature 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.
To create a custom dashboard
1. Go to any dashboard.
2. Click Create Custom Dashboard.

3. Enter a title for your dashboard.
4. Use the Share Dashboard box for sharing your custom dashboard. This option is disabled by default. See Sharing your Custom Dashboard for more information.
5. Add the number of rows you need and select the number of columns you want for each row, between 1 and 4. You can select the row height (small, medium, or large) for each column.
6. Click Save.

Your custom dashboard is created and displayed. The page appears empty because you have not selected any widget yet.
To configure your custom dashboard

USM Anywhere™
User Guide
1. Go to **Dashboards > Custom Dashboards** and open your dashboard.
2. On the widget that you want to configure, click the icon.

3. Choose a widget type between Alarms, Events, Assets, Vulnerabilities, and Configuration Issues. Every widget has its own widget data.

4. You can change the title of the widget.

5. (Optional.) You can select a saved view filter if you have custom views for the selected type of widget.

6. Click Save.
Note: You can move the widgets inside your dashboard. Click the widget that you want to move and drag it to the space you want to move it to. If it is an empty space, the widget will display in it. If it is in a space occupied by another widget, the widgets will replace each other.

To edit your custom dashboard
1. Go to Dashboards > Custom Dashboards and open your dashboard.
2. Select Actions > Edit Dashboard.
3. Modify the information you need to.
4. Click Save.

To edit a widget in your custom dashboard
1. Go to Dashboards > Custom Dashboards and open your dashboard.
2. Click the icon and select Edit.
3. Modify the information of the items that need to be modified.
4. Click Save.
To modify the title of a widget in your custom dashboard:

1. Go to **Dashboards > Custom Dashboards** and open your dashboard.
2. Click the 📇 icon and select **Edit**.
   
   The Edit Widget dialog box opens.
3. Modify the title.
4. Click **Save**.
To clone your custom dashboard

1. Go to Dashboards > Custom Dashboards and open your dashboard.
2. Select Actions > Clone Dashboard.
3. Enter a title for the new dashboard.
4. Click Save.

The new dashboard displays.

**Note:** If you clone a shared custom dashboard, the cloned dashboard will have the shared option disabled by default. See Sharing your Custom Dashboard for more information.

To delete your custom dashboard

1. Go to Dashboards > Custom Dashboards and open your dashboard.
2. Select Actions > Delete Dashboard to open the delete dashboard dialog box.
3. Click Confirm.
Sharing your Custom Dashboard

USM Anywhere enables you to share the custom dashboards you have created. This option is disabled by default.

Keep in mind you cannot edit or delete a shared dashboard. Shared custom dashboards are read-only dashboards. If you want to edit a shared custom dashboard, you have to clone it beforehand. See To clone your custom dashboard for more information.

To share a new custom dashboard

1. Go to any dashboard.
2. Click Create Custom Dashboard.
3. Enter a title for your dashboard.
4. Select the Share Dashboard box for sharing your custom dashboard. This option is disabled by default.
5. Add the number of rows you need and select the number of columns you want for each row, between 1 and 4. You can select the row height (small, medium, or large) for each column.
6. Click Save.

To share an existing custom dashboard

1. Go to Dashboards > Custom Dashboards and open the custom dashboard you want to share.
2. Select Actions > Edit Dashboard.
3. Select the Share Dashboard box for sharing your custom dashboard.
4. Click Save.
To stop sharing a custom dashboard

1. Go to **Dashboards > Custom Dashboards** and open the custom dashboard you want to stop sharing.
2. Select **Actions > Edit Dashboard**.
3. Deselect the Share Dashboard box to remove the option.
4. Click **Save**.

**Example: Creating a Custom Widget on Dashboards**

USM Anywhere enables you to create and customize your own dashboards with the widgets and content you need. In this example, you will create a dashboard with a widget that displays events from a specific sensor.

USM Anywhere provides some widgets for events out of the box (for example, Events by Application, Events by Severity, or Events by Source, to name a few). However, there is no widget for events from a specific sensor. If you want to show events from a specific sensor on your dashboard, you can create a custom widget by using a saved event view.

To create a widget for events from a specific sensor, you first need to filter the events and save them in a view.

**To save a view for events from a specific sensor**

1. Go to **Activity > Events**.
2. Locate the Sensor filter on the left and click the sensor you want to view the events.
   The page reloads showing the events originated from this sensor.
3. (Optional.) Add or adjust filters to limit the view further.
4. When you are satisfied, select **Save View > Save as**.
5. Enter a name for this view.
6. Select **Share View** if you want to share your view with other users.
7. Click **Save**.
   You will use this name in the next procedure.

---

**Edition**: Creating custom dashboard 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.

You can now use the saved view in a widget on a custom dashboard.

**To create a custom dashboard**

1. Go to any dashboard.
2. Click **Create Custom Dashboard**.
3. Enter a title for your dashboard.
4. Use the Share Dashboard box for sharing your custom dashboard. This option is disabled by default. See **Sharing your Custom Dashboard** for more information.
5. Add the number of rows you need and select the number of columns you want for each row, between 1 and 4. You can select the row height (small, medium, or large) for each column.
6. Click **Save**.
7. On the widget that you want to configure, click the icon.

The Edit Widget dialog box opens.

8. From the Widget Type list, select **Events** to display more options.

9. In the Widget Data search field, enter **events over time** and click the **Events over Time** widget.

The title field is automatically populated with the name of the widget. You can change the title if you want.

10. From the Saved View Filter (Optional) list, select the view you have saved in the previous procedure.
11. Click **Save**.

The page reloads displaying the widget you just configured.
To get the most out of USM Anywhere, you need to optimize the management of your environment by understanding USM Anywhere best practices and knowing which ones work best for your setup. The following pages explain USM Anywhere best practices that can help you to achieve this goal:

- **USM Anywhere Scheduler Best Practices** explains essential points and performance issues associated with scheduled jobs that you must keep in mind when scheduling your jobs.
- **USM Anywhere Scans Best Practices** provides information about scans, types of scans, the specific ways of doing a scan, the right order for doing scans and avoid asset duplicity, and so on.
- **Orchestration Rules Best Practices** is where you can find useful recommendations when creating an orchestration rule.
Asset Management

To get the most out of USM Anywhere, you must provide information about all equipment included in your environment, which must be identified by a unique identifier, an IP address.

Once the assets have been identified, there are several tasks that you must carry on. This chapter describes these necessary tasks to manage assets and asset groups. This chapter covers topics such as asset creation and discovery, asset scans, vulnerability scans, scheduling scans, asset monitoring, and analysis.

This topic discusses these subtopics:

- Asset Administration in USM Anywhere ..................................................... 116
- Asset Groups Administration ....................................................................... 186
Asset Administration in USM Anywhere

Through USM Anywhere, you can configure asset management according to your needs. Proper asset management is necessary to make the most of the entire USM Anywhere functionality.

In USM Anywhere, an asset is a piece of equipment on the company's network that bears a unique IP address. An asset can be a server, a router, a firewall, a printer, a PC, or any other network-enabled device.

**Note:** You can watch the How to Use Asset Management in USM to Improve Network Visibility customer training webcast on-demand to learn how to collect an accurate asset inventory.

This topic includes these subtopics:

- Adding Assets
- Importing Assets from a CSV File
- Asset List View
- Selecting Assets in Asset List View
- Searching Assets
- Running Asset Scans
- Running Authenticated Asset Scans
- Scheduling Asset Scans from Assets
- Scheduling Authenticated Asset Scans from Assets
- Adding AlienApps to an Asset
- Viewing Assets Details
- Events Created When an Asset Stops Sending Data
- Managing Asset Fields
- Deleting the Assets
- Editing Assets
- Create an Assets Report
Adding Assets

USM Anywhere provides different ways to add your assets:

- Asset Discovery
- Adding Assets by Using the Setup Wizard
- Adding Assets in the UI
- Adding Assets Through a CSV File

Asset Discovery
USM Anywhere discovers assets automatically if you have a cloud provider (for example, Amazon Web Services [AWS] or Microsoft Azure) or a hypervisor management API (for example, VMware ESX). After deploying the sensor and applying the API credentials, USM Anywhere discovers assets in these environments. See Running an Asset Discovery for more information.

---

**Note:** Asset discovery scans can generate assets for hosts that do not exist when traversing certain network devices. See the Asset Discovery creates assets and is it for each IP address in a network range article for more information.

**Important:** Make sure when you use a virtual private network (VPN) using a Cisco Firewall, that arp-proxy is enabled in the firewall. Otherwise, all the assets will be reported using the same media access control (MAC) address, and USM Anywhere will consider all of them to be different interfaces for the same asset.

---

**Adding Assets by Using the Setup Wizard**
The Setup Wizard is available on USM Anywhere when the sensor is not configured, and is displayed after each login. This wizard includes the initial tasks for getting USM Anywhere ready for deployment. As a result, the wizard collects as much data as possible to analyze and identify threats in your environment.
There are two ways to add assets to scan when using the Setup Wizard: by adding individual assets, or by using network ranges to add multiple assets.

### Adding Individual Assets to Scans

The asset discovery option in the Setup Wizard enables you to add individual assets to scans.

#### To add individual assets using the Setup Wizard

1. Inside the Setup Wizard, click **Asset Discovery**.
2. Enter an asset name and either an IP address, or a fully qualified domain name (FQDN).
3. Click **Save**.

### Adding Multiple Assets to Scans Using a Network Range

The asset discovery option in the Setup Wizard enables you to add multiple assets in a network range to scans.

#### To add multiple assets in a network range using the Setup Wizard

1. Inside the Setup Wizard, click **Asset Discovery**.
2. Click **Scan Networks**.
3. Enter a network name and a Classless Inter-Domain Routing (CIDR) block to specify the subnet's IP address block that you want to scan.
4. If you have more than one sensor configured in your environment, you need to select a sensor. By default, the Scan this network daily to discover new assets and services checkbox is selected. This option configures daily network discovery assets when scanning a network from the wizard.

5. Click Scan.

The length of this process depends on the length of the network range (for example, longer network ranges have longer processes).

After the process finishes and the scan is completed, the number of assets found is displayed. These assets are automatically added to USM Anywhere. In addition, a dynamic asset group is automatically created with these assets.

6. Click Scan Another to start a new scan, or click Next to continue with the following screen.

To add assets by scanning your network

1. Go to Data Sources > Sensors.
2. Click the VMware Sensor with which you want to scan the network.
3. Click Asset Discovery.
4. Click Yes to scan the network.

This step may be different depending on the sensor you have installed.

Note: This option is not available for AWS Sensors because the instances are automatically set.
added to USM Anywhere. In addition, a dynamic asset group is automatically created with these assets.

5. Click **Scan Another** to start a new scan or click **Next** to continue with the following screen.

### Adding Assets in the UI

Adding assets in the user interface (UI) enables you to manually add an asset. To do this, you must know the IP addresses of the assets.

There are two methods of manually adding assets through the UI:

- The quick method, by adding the asset name and either an IP Address or FQDN, and then selecting a USM Anywhere Sensor.
- The advanced method, which requires more data related to the asset that you are adding.

**To add a new asset using the quick method**

1. Go to Environment > Assets.
2. In the upper right side of the page, select **Actions > Quick** to display the following fields above the asset list:

   ![Quick Add Asset](image)

3. Enter the asset name and either the IP address or FQDN in the text boxes displayed above the asset list.

   Use the 🎨 icon to display the rules that must satisfy a valid FQDN.

4. If you have more than one USM Anywhere Sensor connected, select the sensor from the drop-down menu.

   By default, the **Scan the newly added asset for asset details** checkbox is selected. This option scans the newly added asset and displays depending on your sensor. See **Running Asset Scans When Creating a New Asset** for more information.

5. Click **Save**.

---

**USM Anywhere™**

**User Guide**
To add a new asset using the advanced method

USM Anywhere™
User Guide
1. Go to Environment > Assets.
2. In the upper-right side of the page, select Actions > Advanced.
Create Asset

Logo

Asset Type (Optional)

Time Zone

System Default

Asset Scan (NMAP)

- Prevent Remote Scanning

- Scan the newly added asset for asset details

Compliance Scope

- PCI

- HIPAA

Owner (Optional)

No Custom Asset Fields available

Network Interfaces

Remove From Network Interface

IP Address

MAC Address (Optional)

FQDN (Optional)
3. Enter the information in each field.

Add the data of the fields that need to be added, as described in the table below.

### Fields in the Create New Asset window

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that identifies the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the asset.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Select the sensor you want to associate with the asset.</td>
</tr>
<tr>
<td>Logo</td>
<td>Symbol that represents the asset.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>(Optional.) Device type that identifies the asset. Select an option from the list. See <a href="#">USM Accepted Asset Types</a> for more information.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time zone configured for your USM Anywhere instance (default is Coordinated Universal Time [UTC]).</td>
</tr>
<tr>
<td>Prevent Remote Scanning</td>
<td>Select this field to avoid remote scanning. This option displays depending on your deployed sensor.</td>
</tr>
<tr>
<td>Scan the newly added asset for asset details</td>
<td>By default this field is selected. Use it to scan the new added asset. See <a href="#">Running Asset Scans When Creating a New Asset</a> for more information. This option displays depending on your deployed sensor.</td>
</tr>
<tr>
<td>Compliance Scope</td>
<td>To include the asset in the Payment Card Industry Data Security Standards (PCI DSS) asset group, the Health Insurance Portability and Accountability Act (HIPAA) asset group, or both, select the corresponding checkboxes. See <a href="#">Using USM Anywhere for PCI Compliance</a> and <a href="#">USM Anywhere Compliance Templates</a> for more information.</td>
</tr>
<tr>
<td>Owner</td>
<td>(Optional.) Free text field to add an owner of the asset.</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>IP Address. IP address assigned to the asset.</td>
</tr>
<tr>
<td></td>
<td>MAC Address. MAC Address assigned to the asset.</td>
</tr>
<tr>
<td></td>
<td>FQDN. Fully Qualified Domain Name.</td>
</tr>
</tbody>
</table>

**Important:** You must enter at least one of the three fields in Network Interfaces. These fields are highlighted when the values are not valid.

**Note:** Every hour, USM Anywhere refreshes information about the PCI DSS or HIPAA asset groups. If you select the Compliance Scope field, you can see the asset inside the asset group after the following update.

4. Click **Save**.

### Adding Assets Through a CSV File

USM Anywhere enables you to add assets through a comma-separated values (CSV) file. This option adds assets in large quantities to your environment. See [Importing Assets from a CSV File](#) for more information.
To add assets through a CSV file

1. Go to **Environment > Assets**.

2. Select **Actions > Import Assets**.

   The import assets dialog box opens.

3. Drop your CSV file or select the file from your desktop.

4. Select a sensor if you have more than one sensor configured in your environment.

5. Click **Import**.

**Importing Assets from a CSV File**

USM Anywhere™ User Guide

USM Anywhere enables you to import several assets from a comma-separated values (CSV) file. Use this option to add assets in large quantities to your environment from a single file. This file needs to follow a specific format.

**Warning:** If the file does not follow the specific format, the assets will not be imported. See [About the CSV File](#) for more information.
To import assets from a CSV file
1. Go to Environment > Assets.
2. Click Actions > Import Assets to open the Import Assets dialog box.

   **Note:** If there is an asset inside the CSV file that has the same IP address or fully qualified domain name (FQDN) of an asset that already exists in your environment, or if there are any fields that are not valid, the new asset is not added.

3. Drop your file or select the file from your desktop.

   Once you select a file, the name of the file displays and the Import button is active.

   ![Import Assets](image)

   CSV Format
   - Only one asset per row is allowed
   - If an asset with the same IP address of FQDN already exists or if any fields are not valid, that asset will not be added

   Sensor
   Meta-Usma-Vmware

   ![Import button](image)

   If you have more than one sensor configured in your environment, you need to select a sensor.

4. Click Import and the process starts. You can view the status of the process, how many assets have been processed or are pending, or which assets were not imported. In the About the CSV File section, there is a table where you can see the import errors and the reasons for which an asset has not been imported.

   **Note:** When an import process starts and finishes, USM Anywhere generates system events. See Searching for System Events Related to an Asset Import Process for more information.

**About the CSV File**
The CSV file must use this format, no other fields are allowed:

```
Asset Name;Description;Asset Type;PCI;HIPAA;IP Address,FQDN;IP Address,FQDN;...
```

[...] indicates that you can use "IP Address,FQDN" as many times as needed. If you need to skip a field, put two semicolons together leaving no space between them. For example:

```
test1;this is a test asset;;true;true;1.1.1.1
```

```
test2;this is a test asset;;true;false;2.2.2.2
```

```
test3;this is a test asset;;false;false;3.3.3.3,test3.alienvault.com;1.2.3.4
```

![USM Anywhere User Guide](image)
Important: Do not include a header line in the CSV file because it will result in an error of invalid format.

You need to provide an IP address or FQDN value valid for USM Anywhere.

The following table shows some examples of IP addresses and FQDNs.

<table>
<thead>
<tr>
<th>Example</th>
<th>Valid / Invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>Valid</td>
</tr>
<tr>
<td>,my.domain.com</td>
<td>Valid</td>
</tr>
<tr>
<td>1.1.1.1, my.domain.com</td>
<td>Valid</td>
</tr>
<tr>
<td>my.domain.com</td>
<td>Invalid</td>
</tr>
</tbody>
</table>

Please note the following:

- There must be only one asset per row.
- You can import all the files you need, but only one at a time.
- The maximum number of network adapters per asset is limited to 30.
- The maximum number of lines in the CSV file is 200,000.
- The maximum size of the CSV file is 25 MB.

Searching for System Events Related to an Asset Import Process

USM Anywhere generates system events when an import process starts and finishes.

USM Anywhere™
User Guide
To look for system events related to an import process

1. Go to Settings > System Events.
2. Locate the Event Name filter.

3. Select one of these filters:
   - **Asset Import Process Finished**: This option displays the system events generated when the assets import process from a CSV file finishes.
   - **Asset Import Process Started**: This option displays the system events generated when the assets import process from a CSV file starts.

The result of your search displays.

**USM Anywhere™ User Guide**

**Asset List View**

USM Anywhere provides a centralized view of your assets. Go to Environment > Assets to see this centralized view.

The Assets page displays asset inventory and information on those assets. These are the different parts of the Assets page:
On the left side of the page are the search and filters options. Use filters to delimit your search.

At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the assets.

The main part of the page is the list of assets, where each row describes an individual asset. Click an asset to open its details. See Viewing Assets Details for more information. Each asset includes a check box that you can use to select it. You can select all assets in the same page by clicking the check box in the first column of the header row. You can also select all the assets in the system. See Selecting Assets in Asset List View for more information.

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

Refreshing the page

USM Anywhere gives you the option of refreshing the page manually by clicking the icon.

Assets List Columns

For each asset in the assets list, USM Anywhere displays useful information to help you manage that asset. The following table lists the fields you see on the page.

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Name</td>
<td>Name of the asset.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>Platform of the agent. This column displays when you open the Asset List View page from the Agents page.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>Version of the agent. This column displays when you open the Asset List View page from the Agents page.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully qualified domain name.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>IP address for the asset.</td>
</tr>
<tr>
<td>Sensor</td>
<td>USM Anywhere Sensor name associated with the asset. The type of sensor is also displayed below the sensor name.</td>
</tr>
<tr>
<td>Column Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Jobs</td>
<td>Number of scheduled jobs. This column is not displayed when you open the Asset List View page from the Agents page.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Device type that identifies the asset. Select an option from the list (see USM Accepted Asset Types for more information). This column is not displayed when you open the Asset List View page from the Agents page.</td>
</tr>
<tr>
<td>Alarm Counter</td>
<td>Number of alarms detected on the asset.</td>
</tr>
<tr>
<td>Event Counter</td>
<td>Number of events related to the asset.</td>
</tr>
<tr>
<td>Vulnerabilities Counter</td>
<td>Number of vulnerabilities detected on the asset.</td>
</tr>
<tr>
<td>Config Issues</td>
<td>Number of configuration issues related to the asset. This option is only available for Amazon Web Services (AWS) and Microsoft Azure sensors.</td>
</tr>
<tr>
<td>Updated</td>
<td>Date on which the asset was updated. The displayed date depends on your computer's time zone.</td>
</tr>
</tbody>
</table>

**Important:** The alarm and event counts are not updated in real time, but are calculated every hour. If the counts are not updated, it can happen because new events or alarms are in your environment after the last count.

**Important:** The vulnerability and configuration issues counts are updated after every scan.

From the list of assets, you can click any individual asset row to display more information on the selected asset, including how many alarms, events, vulnerabilities, or configuration issues are related to that asset. See Viewing Assets Details for more information.

Each asset includes a check box that you can use to select it. You can select all assets in the same page by clicking the check box in the first column of the header row. You can also select all the assets in the system. See Selecting Assets in Asset List View for more information.

The padlock you can see next to the asset indicates whether the asset has a credential assigned (🔒) or not (🔓). See Managing Credentials in USM Anywhere for more information.
You can choose the number of items to display by selecting **20**, **50**, or **100** below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

Choose the view you want in the Layout page. You can see the assets in a list view or in a grid view.
Click **Generate Report** button to open the Configure Report dialog box. See [Create an Assets Report](#) for more information.

Click the ✅ icon to access these options:

- **Find in events**: Use this option to execute a search of the asset name in the Events page. See [Searching Events](#) for more information.
- **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See [Using OTX in USM Anywhere](#) for more information.
- **Full Details**: See [Viewing Assets Details](#) for more information.
- **Configure Asset**: See [Editing Assets](#) for more information.
- **Delete Asset**: See [Deleting the Asset](#) for more information.
- **Assign Credentials**: See [Managing Credentials in USM Anywhere](#) for more information.
- **Authenticated Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See [Running Authenticated Asset Scans](#) for more information.
- **Scan with AlienApp**: This option enables you to run an asset scan through an AlienApp. See [Running Asset Scans Using an AlienApp](#) for more information.
- **Run Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See [Running Asset Scans](#) for more information.
- **Configuration Issues**: This option opens the Assets Details page. The Configuration Issues tab is selected in the page. See [Viewing Assets Details](#) for more information.
Vulnerabilities: This option opens the Assets Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

Alarms: This option opens the Assets Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

Events: This option opens the Assets Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

In the upper-left corner of the page, there is the **Actions** button.

---

**Important:** You need to select one or more assets if you want to activate the options of the Actions button. Some options can be gray if there isn't any asset selected. See Selecting Assets in Asset List View for more information.

The **Actions** button includes these options:

- **Quick**: Use this option to add the asset name and either an IP address or FQDN, and then select a USM Anywhere Sensor. See Adding Assets in the UI for more information.

- **Advanced**: Use this option to add an asset. This method requires more data related to the asset that you are adding. See Adding Assets in the UI for more information.

- **Import Assets**: Use this option to add several assets through a CSV file. See Importing Assets from a CSV File for more information.

- **Delete selected**: See Deleting the Assets for more information.

- **Edit Fields**: See To assign asset fields to an asset or group of assets for more information.

- **Assign Credentials**: See Managing Credentials in USM Anywhere for more information.
Assign Agent Profile: See Assigning AlienVault Agent Configuration Profiles to Assets for more information. This option is available for users whose role is Manager.

Set Sensor: See To assign a sensor to an asset or a set of assets for more information.

Set Compliance Scope: See Working with Assets and PCI DSS for more information.

Add to Asset Group: See Creating an Asset Group for more information.

Manage Columns: See Configuring Columns on Assets for more information.

Configure Filters: See Managing Filters for more information.

Configuring Columns on Assets

You can configure the columns and fields displayed in the list and save your columns configuration to get back to it whenever you need it.

To configure your columns

1. From the assets list view, select Actions > Manage Columns. The Columns Configuration dialog box opens.

2. Search the columns you want to have in the list view. You can enter your search in the search field.

   Click the icon of an available column to modify the name of the column.
3. Use the and icons to pass the items from one column to the other and select the columns you want to see.

4. You can order the view of your selected columns by clicking one of them and dragging the column to the desired place.

5. Click Apply.

**Note:** If you export a report when you have set custom columns, your report keeps the columns you have configured.

**Important:** If you want to keep your configuration, you need to save it by selecting Save View > Save as. Otherwise, your custom view is not kept when you move to another feature. See Assets Views for more information.

### Assets Views

You can configure the view you want for the list of items in the page.

**To create a view configuration**

1. From the Assets list view, select Actions > Manage Columns.
2. Use the and icons to pass the items from one column to another and select the columns you want to see.
3. Click Apply.
4. If you want to filter the search, select the filters you want to apply.
5. Select Save View > Save as.

The Save Current View dialog box opens.
6. Enter a name for the view.
7. Select Share View if you want to share your view with other users.
8. Click Save.
   The created view is already selected.

To select a configured view
1. From the Assets list view, click View above the filters.
2. Click Saved views and select the view you want to see.

   Note: A shared view includes the icon next to its name.

3. Click Apply.

To delete a configured view
1. From the Assets list view, click View above the filters.
2. Click Saved views and click the icon next to the saved view you want to delete.
   A dialog box displays to confirm the deletion.

   Note: You can delete the views you have created.

3. Click Accept.

   Important: The icon does not display if the view is selected.

Report Templates in Assets

USM Anywhere includes a wide range of report templates classified according to the compliance templates for alarms, vulnerabilities, and events collected in the system. The templates are combined into these two groups:
NIST CSF: The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

ISO 27001: ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).

To apply a report template

1. Go to Environment > Assets.
2. From the Assets list view, click View above the filters and select Report Templates.
3. Select a report.
   You can use the search field or scroll down the list.

4. Click Apply.
   The result displays with the filters applied.

Selecting Assets in Asset List View

USM Anywhere™ User Guide

USM Anywhere enables you to select an asset or multiple assets for export (see Create an Assets Report), and you can use the options you find under the Actions button (see Asset List View).
To select a single asset
- Select the check-box to the left of the asset.

To select multiple assets
- Select the check-box of each asset that you want to include.
- You can go to the next page and select more assets. Keep in mind that USM Anywhere does not preserve the selection on the previous page. If you want to select assets that are displayed in different pages, you can create an asset group. See Creating an Asset Group for more information.

To select all the assets on the same page
- Select the check-box in the first column of the header row.

To select all the assets returned from a search or all the assets in your environment
1. Select all the assets on the page.

Text similar to the following example displays above the asset table:

All 20 assets on this page are selected. Select all 904 related to this filter

where
904 is the number of assets in the system.
2. To select all the assets, click **Select all 904 related to this filter**.

Searching Assets

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure filters** link located in the upper-left corner of the page. See **Managing Filters** for more information.

The following table lists the filters you see on the page.

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Search</td>
<td>Use this filter for searching a specific value of a field. See <strong>Advanced Search Filter</strong> for more information.</td>
</tr>
<tr>
<td>Stats</td>
<td>Filter assets having events, alarms, vulnerabilities, or configuration issues.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Filter assets by the associated USM Anywhere sensor.</td>
</tr>
<tr>
<td>Asset Origin Type</td>
<td>Filter assets by who added the asset to the system.</td>
</tr>
<tr>
<td>Group Membership</td>
<td>Filter assets by the associated group.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>(Only for the Amazon Web Services [AWS] Sensor). Filter assets by AWS instance type.</td>
</tr>
</tbody>
</table>
Filters Displayed by Default in the Main Assets Page (Continued)

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>(Only for the AWS Sensor). Filter assets by AWS region.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter assets by operating system (OS).</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Filter assets by asset type. See USM Accepted Asset Types for more information.</td>
</tr>
</tbody>
</table>

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

**Icons Next to the Filter Title**

Sort the filters alphabetically.

Sort the filters by the number of items that match them.

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the \( \times \) icon next to the filter. Or clear all filters by clicking Reset.

**Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.
Managing Filters

There are many more filters available beyond those that are shown on the Assets page by default. You can configure the filters you want to display by clicking the Configure filters link, which is located in the upper-left corner of the page.

USM Anywhere™
User Guide
To add or delete filters from the Search and Filters area

1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the Configure Filters link.
   The filters configuration dialog box opens.
3. Search the filters you want to have in the list view. You can enter your search in the search field.
4. Use the → and ← icons to pass the items from one column to the other and select the filters you want to see.
5. Click Apply.

To save a filter configuration
1. From the Asset List view, select the filters you want to see.
2. Select **Save View > Save as**.
   The Save Current View dialog box opens.
3. Enter a name for the view.
4. Select **Share View** if you want to share your view with other users.
5. Click **Save**.
The created view is already selected.

**Note:** If you have changed the configuration of the assets columns, this configuration will also be saved together with the filter configuration. See [Assets Views](#) for more information.

## Advanced Search Filter

The Advanced Search filter enables you to enter a search value on a selected field. The following table shows the filter fields that you can find in the first drop-down list.

### Advanced Search Fields (First Drop-Down List)

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filter assets by the name of the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>Filter assets by the asset description.</td>
</tr>
<tr>
<td>UUID</td>
<td>Filter assets by the universally unique identifier (UUID).</td>
</tr>
<tr>
<td>IP/CIDR</td>
<td>Filter assets by IP and Classless Inter-Domain Routing (CIDR). This is a method for allocating IP addresses and routing IP packets. It is the range of IP addresses that define the network.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Filter assets by Fully Qualified Domain Name (FQDN).</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Filter assets by asset type.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Filter assets by instance type.</td>
</tr>
<tr>
<td>Region</td>
<td>Filter assets by region.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter assets by operating system.</td>
</tr>
<tr>
<td>Service</td>
<td>Filter assets by service.</td>
</tr>
<tr>
<td>Software</td>
<td>Filter assets by software.</td>
</tr>
<tr>
<td>Associated Plugin</td>
<td>Filter assets by the plugin associated to the asset.</td>
</tr>
<tr>
<td>Alarm Counter</td>
<td>Filter assets by the number of alarms.</td>
</tr>
<tr>
<td>Event Counter</td>
<td>Filter assets by the number of events.</td>
</tr>
<tr>
<td>Vulnerability Counter</td>
<td>Filter assets by the number of vulnerabilities.</td>
</tr>
<tr>
<td>Configuration Issue Counter</td>
<td>Filter assets by the number of configuration issues.</td>
</tr>
<tr>
<td>PCI Asset</td>
<td>Filter assets by Payment Card Industry (PCI) Asset, if the asset is included or not in the PCI Data Security Standards (DSS) Asset Group. See <a href="#">Asset Group List View</a> and <a href="#">Working with Assets and PCI DSS</a> for more information.</td>
</tr>
<tr>
<td>HIPAA Asset</td>
<td>Filter assets by Health Insurance Portability and Accountability Act (HIPAA) Asset, whether the asset is included in the HIPAA Asset Group. See <a href="#">Asset Group List View</a> for more information.</td>
</tr>
<tr>
<td>Custom User Fields</td>
<td>Filter assets by the fields you have created. If you have not created fields, this filter does not display.</td>
</tr>
</tbody>
</table>
**Note:** The result of a search when you use the Alarm Counter filter or the Event Counter filter depends on if an alarm or an event can identify the source or destination as an asset in the inventory. Your environment can have alarms or events associated with assets both included in the inventory and those not included in the inventory. Assets included in the inventory display their names in blue, and assets not included in the inventory display their names in gray. The alarm and event counter filters only count the identified (blue) assets.

<table>
<thead>
<tr>
<th>EVENT NAME</th>
<th>TIME CREATED</th>
<th>OTX</th>
<th>SOURCE ASSET</th>
<th>DESTINATION ASSET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assume Role</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UpdateInstanceInformation</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UpdateInstanceInformation</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assume Role</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UpdateInstanceInformation</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UpdateInstanceInformation</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Aliases</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Aliases</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Clusters</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View instance status</td>
<td>Tue, Feb 12 2019, 11:49 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important:** The alarm and event counts are not updated in real time but are calculated every hour. If the counts are not updated, it can happen because new events or alarms are in your environment after the last count.

The following table shows the operators that you can find in the second drop-down list.

### Advanced Search Fields (Second Drop-Down List)

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Greater than.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than.</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to.</td>
</tr>
<tr>
<td>Equal</td>
<td>Equal to.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Range of IP addresses.</td>
</tr>
<tr>
<td>Is Empty</td>
<td>Include assets with no IP addresses. This operator is available only for IP/CIDR.</td>
</tr>
<tr>
<td>Is Not Empty</td>
<td>Include assets with IP addresses. This operator is available only for IP/CIDR.</td>
</tr>
<tr>
<td>Like</td>
<td>Search for the specified pattern.</td>
</tr>
<tr>
<td>Operator</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Not Equal</td>
<td>Not equal to.</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>Some filters don't include the NOT operator (for example, Services or Software).</td>
</tr>
<tr>
<td>Not Like</td>
<td>Not true.</td>
</tr>
</tbody>
</table>

**To search assets using the advanced search filter**

1. Go to **Environment > Assets**.
2. Below Advanced Search filter, click **Add Filter**.
3. Select a field from the first drop-down list.
4. Select an operator from the drop-down list.

**Important:** Depending on the field you have chosen in the first drop-down list, the operators vary.
5. Enter the search value.

If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

6. Click the **+** icon.

7. Click **Add Filter** if you want to add a new search.

8. Click the **-** icon.

9. Click **Apply**.

The result of your search displays with the assets identified.

### Standard and Advanced Modes on Assets

USM Anywhere™ User Guide

USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the **+** icon or clicking the **-** icon located in the upper left corner of the page.

#### Standard Mode

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.
To activate the standard mode when the advanced mode is on
1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray.

**Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

**Advanced Mode**
Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

**To activate the advanced mode**
1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green.

**To perform a search in the advanced mode**
1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green.
3. Click the filters that you want to select.
   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click Apply Filters. Or in the upper side of the page, click Apply.

The result of your search displays.

**To search using the NOT operator**
1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.

**Important:** You have to select a filter to see this operator.

**Note:** The selected filter displays the icon and the filter chiclet is labeled in red.
Important: Some filters don’t include the NOT operator (for example, Services or Software).

5. Click Apply.

To search all values of a filter

1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

Running Asset Scans

Use an asset scan to discover hosts and services in the deployed network. To accomplish this goal, the scanner sends crafted packets to the target asset and analyzes the responses. This is not an authenticated scan. You can run scans on individual assets.

Important: This option is available if the sensor associated with the asset allows it.
The asset for which you are scanning must be visible by the sensor through the network. This means that both the sensor and the asset should be able to see each other through at least Layer 3 (network) protocols. If the sensor and the asset are in the same network segment (Layer 2), use Address Resolution Protocol (ARP) requests to discover the asset.

USM Anywhere Sensor sends ARP, Internet Control Message Protocol (ICMP), and TCP requests to discover hosts on the network to which the sensor is connected. A new asset is created if the sensor receives an acknowledgment from any of the previously mentioned protocols.

**Important:** You cannot scan USM Anywhere Sensors.

## Enabling the Asset Scanner App

**To enable the Asset Scanner App**

1. Go to **Data Sources > Sensors** to open the Sensors page.
2. Click the USM Anywhere Sensor for which you want to enable the asset scanner app.
3. Click the **Asset Scanner** tab.

**Note:** This item is not available on AWS sensors.

4. Click **Enable**.

## Running Asset Scans from Assets

**To run an asset scan from Assets**

1. Go to **Environment > Assets**.
2. Complete one of these options to open the Scan Asset dialog box:
   - Next to the asset name that you want to scan, click the **Scan** icon, select **Full Details**, and then select **Actions > Asset Scan**.
   - Next to the asset name that you want to scan, click the **Scan** icon, and then select **Asset Scan**.

The Asset Scan dialog box opens.
3. Select the scan profile that you want to run:

- **Discovery**: This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)
- **Complete**: This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)
- **Vulnerability Discovery**: Performs a general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.
- **Extended Vulnerability Discovery**: Performs a Vulnerability Discovery scan, which actively discovers more about the network.
- **Intensive Vulnerability Discovery**: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

4. Select **Set Debug Mode** if you want to log the results of the scan or if you have a problem with a scan. This option is disabled by default.
5. Click **Scan**.

6. In the Asset details page, click **Scan History** in the table area to display the results of the scan. Note: You can see the status of each scan and the details.

**Important**: Make sure the Asset Scanner app is enabled. See **Enabling the Asset Scanner App** for more information.

**Note**: See **Scheduling Asset Scans from Assets** and **Scheduling Asset Scans from the Job Scheduler Page** for more information about how to schedule an asset scan.

### Running Asset Scans When Creating a New Asset

To run an asset scan when you are creating a new asset:

1. Go to **Environment > Assets**.
2. Select **Actions > Advanced** to open the Create New Asset dialog box. See **Adding Assets in the UI** for more information.
3. The **Scan the newly added asset for asset details** field is selected by default. Use it for scanning the newly added asset.

**Important**: The Asset Scan options are available only for the VMware Sensor and Hyper-V Sensor. USM Anywhere

---

**USM Anywhere™**

**User Guide**
4. Click **Save**.

A message displays at the top of the page to inform you that the scan has been launched and is running. When the scan is complete, the results are visible in the tab **Scan History** of the asset details page. See [Viewing Assets Details](#) for more information.
Running Asset Scans Using an AlienApp

USM Anywhere enables you to select an asset and run an asset scan through an AlienApp.

The asset for which you are scanning must be visible by the sensor through the network. This means that both the sensor and the asset should be able to see each other through at least Layer 3 (network) protocols. If the sensor and the asset are in the same network segment (Layer 2), use Address Resolution Protocol (ARP) requests to discover the asset.

USM Anywhere Sensor sends ARP, Internet Control Message Protocol (ICMP), and TCP requests to discover hosts on the network to which the sensor is connected. A new asset is created if the sensor receives an acknowledgment from any of the previously mentioned protocols.

To run an asset scan through an AlienApp

1. Go to Environment > Assets.
2. Complete one of these options to open the Select Scan Action dialog box:
   - Next to the asset name that you want to scan, click the icon, select Full Details, and then select Actions > Scan with AlienApp.
   - Next to the asset name that you want to scan, click the icon that you want to scan, and then select Scan with AlienApp.

The Select Scan Action dialog box opens.

3. Select one of the options.
   These are the options you can see in the example:

**Important:** The available AlienApps on this dialog box are those that have been configured with the Asset Discovery capability. See Advanced AlienApps for more information.
Running Authenticated Asset Scans

Role Availability

- Read-Only
- Analyst
- Manager

An authenticated asset scan verifies scanned Internet Protocol (IP) addresses and detects vulnerabilities. Log in as administrator or root to perform an authenticated scan. See Managing Credentials in USM Anywhere for more information.

**Warning:** An authenticated scan may fail if the local mail exchanger, which applies to Linux hosts, is enabled in the target asset.

You cannot scan USM Anywhere Sensors.

You can scan an instance or network, but first you need to check these points:

- The sensor reaches the targets
- The sensor is able to scan their ports

If your USM Anywhere Sensor is deployed in Amazon Web Services (AWS) to a virtual private cloud (VPC), see Amazon VPC-to-Amazon VPC connectivity options for more information.

The following table shows the asset scan credentials and escalation options.

### Asset Scan Credentials and Escalation Options

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Method and Credentials</th>
<th>Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux, BSD, Solaris, or macOS</td>
<td>SSH password or public key authentication</td>
<td>sudo or su</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>SSH password</td>
<td>enable password</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows username and password through WinRM</td>
<td>None</td>
</tr>
</tbody>
</table>

To run an authenticated asset scan from Assets

1. Go to Environment > Assets.
2. Complete one of these options:
   - Next to the asset name that you want to scan, click the ✅ icon, select Full Details, and then select Actions > Authenticated Scan.
   
   or

   - Next to the asset name you want to scan, click the ✅ icon and select Authenticated Scan to directly start the asset scan. If the option is not enabled, you will need to add a credential. See Managing Credentials in USM Anywhere for more information.

A message displays at the top of the page to inform you that the authenticated scan is in progress.
Important: Credentials assigned directly to an asset have higher priority than those assigned to an asset group.

3. In the asset details page, click **Scan History** in the table area to display the results of the scan. You can see the status of each scan and its details, which informs you if the scan is unsuccessful due to bad credentials or a connectivity issue between the USM Anywhere Sensor and the asset you are attempting to scan. Each asset will have a **Scan Details** link you can click to download a zip file containing the details of the recent scan. The link will only be present for the most recent scan of each asset, and will be available for one week after the scan has been run.

Below the **Vulnerabilities** tab, you can see the vulnerabilities that the scan has found.

You can also see the vulnerabilities that the scan has found by going to **Environment > Vulnerabilities**. While the scan is running, a **Scanning** button displays. When the scan finishes, the message **Scan finished. Refresh to view scan results** displays. Click **Refresh Scan Results** to update the list.

**Note:** See [Scheduling Authenticated Asset Scans from Assets and Scheduling Asset Scans from the Job Scheduler Page](#) for more information about how to schedule an authenticated asset scan.

### Scheduling Asset Scans from Assets

USM Anywhere provides a simple way to include scans for scheduling using its web user interface (UI). See [USM Anywhere Scheduler](#) for more information.

To schedule an asset scan job from the asset details window

1. Go to **Environment > Assets**.
2. Next to the asset name that you want to include in an asset scan, click the 

   ![Icon](https://example.com/icon.png)

   and select **Full Details**.
3. Select **Actions > Schedule Scan Job**.

   The Schedule New Job dialog box opens.
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Asset Scanner. Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, leave Scan, which is the default option. This option discovers services, operating systems (OSes), hostnames, IP and media access control (MAC) addresses, and vulnerabilities of known hosts.
6. The Asset field displays the name of the asset to scan. You can't modify this field.
7. Select the scan profile that you want to run:
Discovery: This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)
Complete: This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)
Vulnerability Discovery: Performs general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.
Extended Vulnerability Discovery: Performs a Vulnerability Discovery scan, which actively discovers more about the network.
Intensive Vulnerability Discovery: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

8. Select Set Debug Mode if you want to log the results of the scan or if you have a problem with a scan. This option is disabled by default.

Note: The Set Debug Mode option must be used only for debugging purposes because it needs a large amount of disk space for the file or files that it generates. Only AT&T Cybersecurity Technical Support should review these files. You can contact this department for more information.

9. In the Schedule section, specify when USM Anywhere runs the job:
   a. Select the increment as Minute, Hour, Day, Week, Month, or Year.
   Warning: After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See USM Anywhere System Monitor for more information.
   b. Set the interval options for the increment.
   The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.

Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.
Important: USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

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

10. Click Save.
   The job now displays in the job scheduler list.

Note: See USM Anywhere Scheduler for more information.

Scheduling Authenticated Asset Scans from Assets

USM Anywhere provides a simple way to include authenticated scans for scheduling using its web user interface (UI). See USM Anywhere Scheduler for more information.

To schedule an authenticated asset scan job from the asset details window
1. Go to Environment > Assets.
2. Next to the asset name that you want to include in an asset scan, click the icon and select Full Details.
3. Select Actions > Schedule Scan Job.
   The Schedule New Job dialog box opens.

USM Anywhere™
User Guide
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Authenticated Asset Scanner. Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, Scan is the default option. This option discovers services, operating systems, hostnames, IP and MAC addresses, and vulnerabilities of known hosts.
6. The Asset field displays the name of the asset to scan. You can’t modify this field.
7. In the Schedule section, specify when USM Anywhere runs the job:
a. Select the increment as **Minute, Hour, Day, Week, Month, or Year.**

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

b. Set the interval options for the increment.

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

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

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

c. Set the start time.

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

8. Click **Save.**

The job now displays in the job scheduler list.

**Note:** See **USM Anywhere Scheduler** for more information.

**Adding AlienApps to an Asset**
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 AlienApps), 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. See Assign Assets to AlienApps for details.
- By adding one or more AlienApps to the asset (this document).

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 for the logs coming from this asset; therefore, USM Anywhere only uses the assigned AlienApps to parse and normalize those logs.

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

Adding an AlienApp to an asset requires that you know what log data that the USM Anywhere Sensor receives from the asset and which AlienApp(s) are the best match for parsing and normalizing that data to produce meaningful events for your needs.

You can add an AlienApp on the Asset Details page. The Asset Details page provides access to all of the available information and tools for managing an individual asset. See Asset Management for more information about managing discovered assets in USM Anywhere.

**To add an AlienApp from the Asset Details page**

1. Go to Environment > Assets.
2. (Optional.) Use the Search & Filters option to filter the list and help you to locate the asset you want.
3. Click the icon next to the asset name and select Full Details.
This displays the Asset Details.

4. At the bottom of the expanded page, select the AlienApps tab and click Add AlienApp.

5. In the dialog box, select the AlienApp you want to assign to the asset. Enter full or part of the name in the Set a New AlienApp field and select one from the displayed list.

USM Anywhere™ User Guide
The system displays this message at the top of the page:

AlienApp added successfully.

6. (Optional.) Repeat the previous step to add another AlienApp.

7. Click the X icon to close the dialog box.

On the AlienApps tab, you can see the list of AlienApps added.
For logs where a matching AlienApp is not identified, USM Anywhere parses it using a *generic data source*. You can review the generated events in the AlienVault Generic Data Source events view. If the reporting device for the event is defined in the USM Anywhere asset inventory, you can manually assign an AlienApp directly from this view.

See AlienVault Generic Data Source in the *USM Anywhere User Guide* for more information about the information and tools available in this view.

**To assign an AlienApp from a AlienVault Generic Data Source event**

1. Go to Activity > Events.
2. Click View > Saved views > AlienVault Generic Data Source.
3. Click Apply.
4. Review the listed events and locate an event where the reporting device is displayed in blue and you want to manually assign a known AlienApp to the asset.
5. In the Reporting Device column, click the icon next to the asset name and select Assign AlienApp.

The Add AlienApp to an asset dialog box opens.
6. In the dialog box, select the AlienApp to use for log data from the asset.

Enter part of the AlienApp name in the **Set a New AlienApp** field and select the AlienApp from the displayed list.
7. (Optional.) Repeat the previous step to add another AlienApp for the asset.
8. Click the \( \times \) icon to close the dialog box.

Viewing Assets Details

To view the details of an asset
1. Go to Environment > Assets.
2. Next to the asset name whose details you want to review, click the \( \checkmark \) icon.
3. Select Full Details.
Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

In the upper left side of the page, you see the name and IP address, along with other fields that describe the particular asset. One of these fields is the **Create event if asset stops sending data**. Use this field to configure a period of time. USM Anywhere starts generating events when the asset has not received messages within the configured period of time. See [Events Created When an Asset Stops Sending Data](#) for more information.

On the right, you see the status summary for your asset. It displays the total number of alarms, events, vulnerabilities, and configuration issues. The circle can display in orange (for alarms and configuration issues), blue for events, and red for vulnerabilities. The number inside each circle indicates the number of alarms, events, vulnerabilities, and configuration issues for the asset. You can click each circle to view the list of issues of each one.

**Note:** Configuration Issues are only available for AWS and Azure Sensors.

**Important:** The alarms and events counts are not updated in real time, they are calculated every hour. If the counts are not updated, it can be seen because new events or alarms are in your environment after the last count.

**Important:** The vulnerabilities and configuration issues counts are updated after every scan.

Below the status summary, you can see this information:

- **Agent Status.** If there is a deployed agent, it displays the connection status of the AlienVault Agent. You can deploy an agent from here.

- **Credentials.** If the credential has been associated to the asset, it displays its name. You can assign and create the credential from here. See [Managing Credentials in USM Anywhere](#) for more information.
**Last Scanned.** If it exists, the date of the latest scan. You can schedule jobs from here. See [Scheduling Asset Scans from Assets](#), [Scheduling Authenticated Asset Scans from Assets](#), and [Scheduling Asset Scans from the Job Scheduler Page](#) for more information.

In the lower side of the page, there is a table area with tabs, some of them correspond to the circles. Each tab contains a table with records, if present, for your asset.

The following table lists the tabs you see on the page.

### Asset Details View Tabs Description

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>Asset groups on which the asset is included.</td>
</tr>
<tr>
<td>Software</td>
<td>Software that is installed on the asset.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Note: You need to run an authenticated asset scan to have a complete list of installed software." /></td>
</tr>
<tr>
<td>Services</td>
<td>Services that are available on the asset.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Note: You need to run an authenticated asset scan to have a complete list of available services." /></td>
</tr>
<tr>
<td>AlienApps</td>
<td>AlienApps enabled for the asset.</td>
</tr>
<tr>
<td>Alarms</td>
<td>Alarms related to the asset. There is a bubble graph that provides a graphical representation of alarms by intent. Blue circles indicate the number of times that an alarm in an intent showed. A bigger circle indicates a higher number of alarms. You can hover over each of the circles to get the actual number of different types of intent. In addition, if you click any of the blue circles, USM Anywhere displays only the alarms corresponding to that circle. You can change the displayed period of time by clicking the <strong>Last 24 Hours</strong> filter.</td>
</tr>
<tr>
<td>Events</td>
<td>Events related to the asset. Click an event to see its details.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Vulnerabilities related to the asset. You can filter the active or inactive vulnerabilities by clicking the specific radio button. Click a vulnerability to see its details.</td>
</tr>
<tr>
<td>Configuration Issues</td>
<td>Information about operational processes. You can filter the active or inactive configuration issues by clicking the specific radio button. Click a configuration issue to see its details.</td>
</tr>
<tr>
<td>Scan History</td>
<td>List of the asset scans already run. It includes a time-stamp of the scan, the scan type, the status, and the details of each scan. You can also click the <strong>Scan Details</strong> link here to download a file containing the details of the most recent authenticated asset scan here for up to a week after the scan was run.</td>
</tr>
<tr>
<td>File Integrity</td>
<td>This tab is available if the AlienVault Agent has been deployed in the asset. It displays stats about File Integrity Monitoring Events. You can configure a time slot on which the events were received. These slots can be last hour, 24 hours, 7 days, 30 days, or 90 days.</td>
</tr>
<tr>
<td>Agent</td>
<td>This tab is available if the AlienVault Agent has been deployed in the asset. It displays information about the agent. You can see the status of the agent (connected or not) and the current version. You can configure a time slot on which the events were received. These slots can be last hour, 24 hours, 7 days, 30 days, or 90 days. You can also see the asset configuration profile. Users whose role is Manager, can also change the configuration profile. See <a href="#">Assigning AlienVault Agent Configuration Profiles</a> for more information.</td>
</tr>
</tbody>
</table>

In the upper right side of the page is the **Actions** button. Use this button to perform actions on the asset. These are the actions:

- **Configure Asset:** See [Editing Assets](#) for more information.
- **Delete Asset:** See [Deleting the Assets](#) for more information.
- **Add to Asset Group:** See [Creating an Asset Group](#) for more information.
- **Agent Query:** See [The AlienVault Agent Events and Queries](#) for more information. This option is available for users whose role is Analyst or Manager.
**Asset Scan:** This option displays or not depending on the sensor associated with the asset. See [Running Asset Scans](#) for more information.

**Assign credentials:** See [Managing Credentials in USM Anywhere](#) for more information.

**Authenticated Scan:** See [Running Authenticated Asset Scans](#) for more information.

**Scan with AlienApp:** See [Running Asset Scans Using an AlienApp](#) for more information.

**Schedule Scan Job:** See [Scheduling Asset Scans from Assets, Scheduling Authenticated Asset Scans from Assets, and Scheduling Asset Scans from the Job Scheduler Page](#) for more information.

---

### Events Created When an Asset Stops Sending Data

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

USM Anywhere gives you the option of configuring a threshold after which asset inactivity is a concern. When your environment is not receiving events from an asset within the configured period of time, USM Anywhere generates monitoring events that display in the **Events List View** page. Since these events are not tied to any USM Anywhere Sensor that you have deployed, you will see a new sensor, with the name of your USM Anywhere subdomain, listed for these events. USM Anywhere will generate new monitoring events until the asset starts reporting again. You can see two types of monitoring events:

- **Event from asset not received:** Event details include the asset name. It includes the total disconnected time and when the last message was received.

**Warning:** Currently, the **Event from asset not received** event is generated at the same time as the regular event and system event. Soon, this event will be generated only as a system event. See [Regular Events and System Events](#) and [Orchestration Rule for the "Event from Asset Not Received" System Event](#) for more information.

- **Event from asset received:** Event details include the asset name.

**Warning:** Monitoring events are generated when your environment is not receiving events from an asset either because the asset is not sending events or because of a filtering rule. If you have a rule that filters events coming from an asset, from the perspective of USM Anywhere that asset is not sending events.

**To configure the period of time**

1. Go to **Environment > Assets**.
2. Next to the asset name whose details you want to review, click the ![icon](#) icon.
3. Select **Full Details**
4. In the upper left side of the page, set a period of time in the **Create event if asset stops sending data** field by clicking the ![icon](#) icon. You can select a predefined value between None, 1 hour, 6, 12, 24, 72 hours, 1 week, or 2 weeks.

**Note:** By default this field is configured to None.

**Important:** The **Create event if asset stops sending data** field is based on the Reporting Device Address field, not the Source field. When a device reports information about its state, the Reporting Device Address field will display the same data as the Source or Destination fields. If the device reports information that is different from its state, for example issues in its network, the Reporting Device Address field will display different information from the Source or Destination fields.
5. Click the icon to set the value.

The events are displayed in the Events List View page.
To see events created when an asset stops sending data

1. Go to Activity > Events.
2. Locate the Event Name filter and select the filter Event from asset not received.
The result displays with the filtered events.

3. Click the event to see its details.

Managing Asset Fields

All assets include several fields for identifying and classifying each asset. You can add all fields you need, modify them or delete them when you do not need them.

Note: It is not possible to modify or delete the fields that are system defaults.

Creating Asset Fields

To create an asset field

1. Go to Settings > System.
2. In the left navigation panel, click Asset Fields to open the page.
3. Click New Asset Field.
   The Create Asset Field dialog box opens.
4. Enter a display name.

5. (Optional.) Enter a description.

6. Select a display priority. You can choose Summary, Detail, or Hidden. Choose Hidden if you do not want to see this field in the details of the assets.

7. Select a type.

See the options in the table:

Options in the Type field (Create an asset field)

<table>
<thead>
<tr>
<th>Denomination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Text in the default field.</td>
</tr>
<tr>
<td>Select</td>
<td>Enter the choices. You can add more than one by clicking the + icon.</td>
</tr>
<tr>
<td>Numeric</td>
<td>Enter a numerical data to identify the field. You can use the icon to increase or decrease the number (↑).</td>
</tr>
<tr>
<td>IP</td>
<td>Enter an IP address.</td>
</tr>
<tr>
<td>Boolean</td>
<td>Select one of the options: No Default, True, or False.</td>
</tr>
</tbody>
</table>

8. Click Save.
Modifying Asset Fields

To modify an asset field
1. Go to Settings > System.
2. In the left navigation panel, click Asset Fields to open the page.
3. Locate the asset field you want to modify. You can filter the search by name, user, priorities, and type of field.
4. In the line of the asset field you want to modify, click the icon. This icon displays in the line of the editable fields that are not in the system by default.
5. Modify the information of the items that need to be modified.
6. Click Save.

Deleting Asset Fields

To delete an asset field
1. Go to Settings > System.
2. In the left navigation panel, click Asset Fields to open the page.
3. Locate the asset field that you want to delete. You can filter the search by name, user, priorities, and type of field.
4. Click the icon.
5. Click Accept to confirm.

Assign Asset Fields to an Asset or Group of Assets

To assign asset fields to an asset or group of assets
1. Go to Environment > Assets.
2. Select the asset or the group of assets. See Selecting Assets in Asset List View for more information.
3. Select Actions > Edit Fields.
4. Select the asset fields you want to assign the selected assets.
5. Click Save.

### Displaying Asset Fields from Assets

To display asset fields:

1. Go to Environment > Assets.
2. Next to the asset name whose asset fields you want to review, click the icon and select **Full Details**.
3. Below the main data of the asset, click More.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addresses</td>
<td>[redacted]</td>
</tr>
<tr>
<td>MAC Addresses</td>
<td>[redacted]</td>
</tr>
<tr>
<td>FQDN</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Services</td>
<td>0</td>
</tr>
<tr>
<td>Software Installed</td>
<td>18</td>
</tr>
<tr>
<td>Sensor</td>
<td>AWS-Sensor, AWS</td>
</tr>
<tr>
<td>Create Event IF Asset Stops Sending Data</td>
<td>None</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows (x64) architecture</td>
</tr>
<tr>
<td>Asset State</td>
<td>Running</td>
</tr>
<tr>
<td>Asset ID (External)</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Found</td>
<td>Fri, Oct 02 2020, 12:20 AM CEST</td>
</tr>
<tr>
<td>Created</td>
<td>Wed, Nov 27 2019, 04:57 PM CET</td>
</tr>
<tr>
<td>Updated</td>
<td>Mon, Nov 15 2021, 11:12 PM CET</td>
</tr>
<tr>
<td>Operating System Source</td>
<td>Authenticated Asset Scan</td>
</tr>
<tr>
<td>Alarms</td>
<td>128</td>
</tr>
<tr>
<td>AWS Account ID</td>
<td>[redacted]</td>
</tr>
<tr>
<td>AWS Region</td>
<td>eu-west-1</td>
</tr>
<tr>
<td>AWS Architecture</td>
<td>[redacted]</td>
</tr>
<tr>
<td>AWS Image ID</td>
<td>[redacted]</td>
</tr>
<tr>
<td>AWS Instance Is Windows</td>
<td>true</td>
</tr>
<tr>
<td>AWS Subnet ID</td>
<td>[redacted]</td>
</tr>
<tr>
<td>AWS VPC ID</td>
<td>[redacted]</td>
</tr>
<tr>
<td>AWS Instance Profile ID</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Launch Time</td>
<td>Wed, Nov 27 2019, 04:57 PM CET</td>
</tr>
<tr>
<td>AWS Monitoring State</td>
<td>disabled</td>
</tr>
<tr>
<td>Asset Field 1</td>
<td>This is the text, type Summary</td>
</tr>
<tr>
<td>Asset Field 2</td>
<td>This is the text, type Detail</td>
</tr>
</tbody>
</table>
Deleting the Assets

Keep in mind these points when you are deleting assets and your environment has an Amazon Web Services (AWS) Sensor, Microsoft Azure Sensor, Google Cloud Platform (GCP) Sensor, or a VMware Sensor installed:

- If you delete an asset, but it is still active/visible in your network environment, the asset is automatically added to your asset inventory for any asset discovery jobs that run after the deletion action.
- If you delete an asset that has alarms or vulnerabilities associated to it, the asset state will be marked as "terminated". All saved data associated to the asset is maintained in its current state.
- If you delete a sensor, all assets on the sensor will be removed from USM Anywhere. However, if you redeploy the sensor, asset configurations that point to the replaced sensor will have the universally unique identifier (UUID) information in that configuration updated to the new sensor UUID.

To delete an asset from the list view

1. Go to Environment > Assets.
2. Next to the asset name that you want to delete, click the icon and select Delete Asset.
   
The Delete Asset dialog box opens.

3. Click Delete to delete the asset.

To delete an asset from the asset details page

1. Go to Environment > Assets.
2. Next to the asset name that you want to delete, click the icon and select Full Details.
3. Click Actions > Delete Asset.
4. Click Delete to delete the asset.

To bulk delete assets

1. Go to Environment > Assets.
2. Select the assets you want to delete. See Selecting Assets in Asset List View for more information.
1. Go to Environment > Assets.
2. Next to the asset name that you want to edit, click the \( \text{\textdownarrow} \) icon and select Configure Asset.

The configure asset dialog box opens.

Editing Assets

Role Availability

Read-Only

Analyst

Manager

If you want to change, delete, or add information regarding assets that have been identified by your USM Anywhere Sensor, follow the guidelines on this page to edit your assets.

3. Click Actions > Delete Selected.
4. Click Delete.

Delete Assets

You are about to delete assets from the database. This is an action that cannot be undone. Are you sure you would like to delete 20 assets?

Delete

Cancel
Configure Asset

Name
JMAAWS

Description (Optional)

Sensor
Meta-Usma-Dev-Sensor

Logo

Asset Type (Optional)
BroadbandRouter

Time Zone
System Default

Compliance Scope

☑ PCI
☐ HIPAA

Owner (Optional)

Custom Fields

MyAssetField (Optional)
true

Custom Field Detail Test 1 (Optional)
3. Modify the data of the items that need to be modified, as described in the Field Descriptions table below.

### Field Descriptions for the Edit Asset Details page

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name identifying the asset. This field is required.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional.) A short description for the asset.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Sensor to associate with the asset.</td>
</tr>
<tr>
<td>Logo</td>
<td>Symbol that represents the asset.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>(Optional.) Device type that identifies the asset. Select an option from the list. See USM Accepted Asset Types for more information.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time zone assigned to the asset. The default value is System Default, which causes the asset to inherit the sensor's time zone. Changing the asset's time zone automatically applies the new time zone to all new logs collected from the asset.</td>
</tr>
<tr>
<td>Compliance Scope</td>
<td>Add the asset to Payment Card Industry (PCI) and/or Health Insurance Portability and Accountability Act (HIPAA). See Working with Assets and PCI DSS and USM Anywhere Compliance Templates for more information.</td>
</tr>
<tr>
<td>Owner</td>
<td>(Optional.) Free text field to add an owner of the asset.</td>
</tr>
<tr>
<td>Custom Fields</td>
<td>Asset fields created by the user. The fields that are system defaults will not be displayed. See Managing Asset Fields for more information.</td>
</tr>
</tbody>
</table>
| Network Interfaces | IP Address. IP address assigned to the asset.  
MAC Address. MAC Address assigned to the asset.  
FQDN. Fully Qualified Domain Name. |

**Important:** You must enter at least one of the three fields in Network Interfaces. These fields are highlighted when the values are not valid.

4. Click **Save**.
<table>
<thead>
<tr>
<th>Asset Type Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Device that provides network-based data storage services.</td>
</tr>
<tr>
<td>Firewall</td>
<td>A firewall controls what traffic is allowed into or out of a network. Some also have additional capabilities. This category does not include general-purpose operating systems (OSes) that happen to come with a firewall, but it does include OS distributions purpose-built to work only as a firewall.</td>
</tr>
<tr>
<td>Game console</td>
<td>A video game console like the Microsoft Xbox or Sony PlayStation.</td>
</tr>
<tr>
<td>General purpose</td>
<td>General-purpose operating systems like Linux and Microsoft Windows.</td>
</tr>
<tr>
<td>Hub</td>
<td>A hub joins network segments by re-broadcasting all traffic. Hubs are distinct from switches, which selectively transmit packets only to relevant destinations.</td>
</tr>
<tr>
<td>Laptop</td>
<td>Small and portable personal computer.</td>
</tr>
<tr>
<td>Load balancer</td>
<td>A device that distributes inbound traffic to multiple devices to ease the load on those devices.</td>
</tr>
<tr>
<td>Media device</td>
<td>This category includes all kinds of audiovisual equipment, including portable music players, home audio systems, TVs, and projectors.</td>
</tr>
<tr>
<td>PBX</td>
<td>A private branch exchange (PBX) routes telephone calls within a private organization and connects them to the public telephone network or Voice over Internet Protocol (VoIP).</td>
</tr>
<tr>
<td>PDA</td>
<td>A personal digital assistant (PDA) is a handheld computer. Devices that are also telephones go in the &quot;phone&quot; category.</td>
</tr>
<tr>
<td>Phone</td>
<td>A network-capable telephone that is not a VoIP phone. Devices in this category are typically mobile phones.</td>
</tr>
<tr>
<td>Power-device</td>
<td>Miscellaneous power devices like uninterruptible power supplies (UPSes) and surge protectors.</td>
</tr>
<tr>
<td>Printer</td>
<td>Network-enabled printers, including printers with an embedded print server.</td>
</tr>
<tr>
<td>Print server</td>
<td>A print server connects a printer to a network. Printers that contain their own print server go in the &quot;printer&quot; category instead.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>Any kind of proxy, including web proxies and other servers that cache data for users and forward packets between different networks as opposed to extending one network.</td>
</tr>
<tr>
<td>Remote management</td>
<td>Devices that allow servers or other equipment to be monitored or managed remotely.</td>
</tr>
<tr>
<td>Router</td>
<td>Routers connect multiple networks. They are distinct from hubs and switches, because they route packets between different networks as opposed to extending one network.</td>
</tr>
<tr>
<td>Security-misc</td>
<td>Any security device that doesn't fall into the “firewall” category belongs in this category. This includes intrusion detection and prevention systems.</td>
</tr>
<tr>
<td>Server</td>
<td>Device that provides functionality for other programs or devices.</td>
</tr>
<tr>
<td>Specialized</td>
<td>The catch-all category. If a device doesn't fall into one of the other categories, it is specialized. Examples in this category are diverse and include such things as clocks, oscilloscopes, climate sensors, and more.</td>
</tr>
<tr>
<td>Storage-misc</td>
<td>Data storage devices like tape decks and network-attached storage appliances.</td>
</tr>
<tr>
<td>Asset Type Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Switch</td>
<td>A device that extends a network by selectively re-broadcasting packets. Switches are distinct from hubs, which broadcast all packets.</td>
</tr>
<tr>
<td>Telecom-misc</td>
<td>Devices used by telephone systems that are not PBXs, like voicemail and Integrated Services Digital Network (ISDN) systems.</td>
</tr>
<tr>
<td>Terminal</td>
<td>A device with a keyboard and monitor with the primary purpose of communicating directly with a terminal server or mainframe.</td>
</tr>
<tr>
<td>Terminal server</td>
<td>A device providing terminal facilities to clients over a network.</td>
</tr>
<tr>
<td>VoIP adapter</td>
<td>A device that converts between VoIP protocols and normal telephone traffic. Also may convert different VoIP protocols.</td>
</tr>
<tr>
<td>VoIP phone</td>
<td>A phone capable of a VoIP protocol.</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless access points (WAPs) offer a wireless connection to a network. Most work with radio technology like 802.11b. but some use infra-red or something else. Devices that could also be put in another category, like wireless broadband routers, are put in the WAP category because WAPs require special network considerations.</td>
</tr>
<tr>
<td>Web server</td>
<td>Device that provides contents to the World Wide Web. A web server processes incoming network requests over HTTP and several other related protocols.</td>
</tr>
<tr>
<td>Webcam</td>
<td>Any kind of camera that stores or transmits pictures or video. This includes everything from consumer webcams to security system cameras.</td>
</tr>
</tbody>
</table>

**Important:** AT&T Cybersecurity recommends Google Chrome as the preferred browser for generating reports.

To create an assets report:

1. Go to **Environment > Assets**.
2. You can use filters to define the assets content you want to display in your report. Or select the assets you want to include in your report.
3. Click the **Generate Report** button to open the Configure Report dialog box.
   - The filters selected and displayed for the page view are the ones that are populated in the report.
4. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, or Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report. For CSV the options are 20, 50, 100, 500, 1000, or 50 K. For PDF the options are 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.
Asset groups are administratively created objects that group similar assets for specific purposes. Assets are grouped based on IP addresses, and USM Anywhere monitors these groups. Grouping based on IP addresses facilitates an easier search and management of assets.

This topic discusses these subtopics:

- Creating an Asset Group
  - How to Create a PCI Dynamic Asset Group
- Asset Group List View
- Searching Asset Groups
- Running Asset Groups Scans
- Running Authenticated Asset Groups Scans
- Scheduling Asset Group Scans from Asset Groups
- Scheduling Authenticated Asset Group Scans from Asset Groups
- Configuring an Asset Group
- Viewing Asset Group Details
- Deleting an Asset Group
USM Anywhere supports static and dynamic asset groups. A static group consists of assets that you manually assign to the group. A dynamic group is defined using rules that automatically add or remove assets from the group, based on the criteria you have defined.

By default, AT&T Cybersecurity creates these dynamic asset groups:

- **Assets with Agents**: Asset group containing assets with agents.
- **Assets with Alarms**: Asset group containing assets with alarms.
- **Assets with Vulnerabilities**: Asset group containing assets with vulnerabilities.
- **Database Servers**: Asset group containing database servers.
- **HIPAA**: Asset group containing Health Insurance Portability and Accountability Act (HIPAA) assets. HIPAA is a standard for protecting sensitive patient data.
- **Linux Assets**: Asset group containing Linux systems.
- **PCI DSS**: Asset group containing Payment Card Industry (PCI) assets.
- **Web Servers**: Asset group containing web servers.
- **Windows Assets**: Asset group containing Microsoft Windows systems.

USM Anywhere also creates a default asset group for each Amazon Web Services (AWS) Elastic Load Balancing (ELB) instance in your environment. The AWS Sensor ELB group includes the ELB instance and any AWS Sensor instance connected to the load balancer and registered with the ELB service. USM Anywhere automatically discovers and enables you to collect ELB access logs if you have ELB access logging enabled.

**Important**: AT&T Cybersecurity recommends that you limit your asset groups to 1024 or fewer assets. While asset groups can be larger, selecting an asset group for any searching or filtering will only return data for the most recent 1024 assets. To see more data, create multiple asset groups each with 1024 or fewer assets.

Creating a Static Asset Group

USM Anywhere enables you to create a static asset group.
To create a static asset group from the asset groups main window

1. Go to Environment > Asset Groups.
2. Select Actions > Static.

3. Enter the name of the asset group. This field is required.
[Note: The valid characters for the asset group name are uppercase letters (A-Z), lowercase letters (a-z), numerical digits (0-9), hyphens (-), underscore (_), and blank space. You can enter up to 64 characters.]

4. (Optional.) Enter a description for identifying this group.

5. Locate the assets that you want to add to the group, and click Add Asset or Scan Network.
   
   If you click Scan Network, enter the name for a network and the Classless Inter-Domain Routing (CIDR) block to specify the subnet's IP address block that you want to scan.

6. (Optional.) Delete assets from the group by clicking the icon. You can view a specific asset by clicking the icon, and use Cancel to discard the changes.

7. Click Save.

Creating a Dynamic Asset Group

USM Anywhere enables you to create a dynamic asset group.
To create a dynamic asset group from the asset groups main window

1. Go to **Environment > Asset Groups**.
2. Select **Actions > Dynamic**.

### Configure Dynamic Asset Group

**Name**

Asset group name

**Description**

Optional

### ADD SEARCH CRITERIA

**All Fields**

**Contains**

Enter search value

**MATCHES AGAINST ADDED CRITERIA: 757 ASSETS**

<table>
<thead>
<tr>
<th>SELECTED ASSETS</th>
<th>IP ADDRESSES</th>
<th>SENSOR</th>
<th>CREDENTIALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>develop-usm-saas-control-aws-c...</td>
<td>10.0.0.1...</td>
<td>USMA-Sensor</td>
<td>-</td>
</tr>
<tr>
<td>mmoral8</td>
<td>10.0.0.1...</td>
<td>USMA-Sensor</td>
<td>-</td>
</tr>
<tr>
<td>develop-usm-saas-es-aws-swiftk...</td>
<td>10.0.0.1...</td>
<td>USMA-Sensor</td>
<td>-</td>
</tr>
<tr>
<td>pg-move-testing-002-dev-senso...</td>
<td>10.0.0.1...</td>
<td>USMA-Sensor</td>
<td>-</td>
</tr>
<tr>
<td>develop-usmc-gatling-aws-sures...</td>
<td>10.0.0.1...</td>
<td>USMA-Sensor</td>
<td>-</td>
</tr>
</tbody>
</table>

3. Enter the name of the asset group.

   This field is required.

**Note:** The valid characters for the asset group name are uppercase letters (A-Z), lowercase letters (a-z), numerical digits (0-9), hyphens (-), underscore (_), and blank space. You can enter up to 64 characters.

**Important:** You cannot use special characters like forward slash (/), backslash (\) or ampersand (&). When a special character is entered, the system will automatically replace it with its equivalent (\) or (\) using the characters (\) or (\), respectively.
4. (Optional.) Enter a description for identifying this group.
5. Add the search criteria for the assets you want to be part of this group:
Select a field: You can choose between fields, custom user fields, tags, and sensor apps fields. You can use the same field multiple times in a group. The table below includes the available fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Counter</td>
<td>Search asset groups by the number of alarms.</td>
</tr>
</tbody>
</table>
| Asset State        | Search asset groups by asset state. Depending on your installed sensor, this state can vary:  
                        - AWS:  
                          - Running: Asset (AWS instance) is running.  
                          - Available: RDS instance is running.  
                          - Stopped: Asset is not running.  
                        - VmWare /Hyper-V:  
                          - PoweredOn: Asset is running.  
                          - PoweredOff: Asset is not running. This state can be used for correlation.  
                          - Suspended: Asset is not running. This state can be used for correlation.  
                        - GCP / Azure:  
                          - Running: Asset is running.  
                          - Stopped: Asset is not running.  
| Asset Type         | Search asset groups by asset type.                                      |
| Associated Plugin  | Search asset groups by the plugin associated to the asset.             |
| Configuration Issue Counter | Search asset groups by the number of configuration issues.       |
| Description        | Search asset groups by the asset description.                          |
| Event Counter      | Search asset groups by the number of events.                           |
| FQDN               | Search asset groups by Fully Qualified Domain Name (FQDN).             |
| HIPAA Asset        | Search asset groups by Health Insurance Portability and Accountability Act (HIPAA) Asset, if the asset is included or not in the HIPAA Asset Group. See Asset Group List View for more information. |
| Instance Type      | Search asset groups by instance type.                                   |
| IP/CIDR            | Search asset groups by IP/Classless Inter-Domain Routing (CIDR). This is a method for allocating IP addresses and routing IP packets. It is the range of IP addresses that define the network. |
| Name               | Search asset groups by the name of the asset.                          |
| Operating Service  | Search asset groups by operating system.                               |
| PCI Asset          | Search asset groups by Payment Card Industry (PCI) Asset, if the asset is included or not in the PCI Data Security Standards (DSS) Asset Group. See Asset Group List View and Working with Assets and PCI DSS for more information. |
| Region             | Search asset groups by region.                                         |
| Sensor             | Search asset groups by sensor.                                         |
| Service            | Search asset groups by service.                                        |
| Software           | Search asset groups by software.                                       |
Field Name | Meaning
--- | ---
UUID | Search asset groups by the universally unique identifier (UUID).
Vulnerability Counter | Search asset groups by the number of vulnerabilities.
Custom User Fields | Search asset groups by the fields you have created. If you have not created fields, this filter does not display.
Tags | (Only for Amazon Web Services [AWS] Sensors). Identify asset groups by the tag assigned to an AWS resource.
Sensor Apps Fields | (Only for AWS Sensors). Identify asset groups by parameters of the AWS instance.

**Note:** The result of a search when you use the Alarm Counter filter or the Event Counter filter depends on if an alarm or an event can identify the source or destination as an asset in the inventory. Your environment can have alarms or events associated with assets both included in the inventory and those not included in the inventory. Assets included in the inventory display their names in blue, and assets not included in the inventory display their names in gray. The alarm and event counter filters only count the identified (blue) assets.

**Important:** The alarm and event counts are not updated in real time, but are calculated every hour. If the counts are not updated, it can happen because new events or alarms are in your environment after the last count.

**Select an operator:** Depending on the selected field, you can choose different operators. The table below shows the available operators:

### Operators to Create a Dynamic Asset Group

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Greater than</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
</tr>
<tr>
<td>Equal</td>
<td>Equal to</td>
</tr>
<tr>
<td>IP Range</td>
<td>Range of IP addresses</td>
</tr>
<tr>
<td>Like</td>
<td>Search for the specified pattern</td>
</tr>
<tr>
<td>Not Equal</td>
<td>Not equal to</td>
</tr>
<tr>
<td>Not Like</td>
<td>Not true</td>
</tr>
</tbody>
</table>

**Enter a search criteria:** Enter the value you want to search.

**Note:** You can use the same field multiple times in a group.

6. Click the + icon to add your search criteria.

You click this icon to add several fields. You can use the same field multiple times in a group.
How to Create a PCI Dynamic Asset Group

In this example we are going to create a PCI Dynamic Asset Group for tagging instances in AWS as PCI compliant. This asset group helps you to tag all instances automatically. You do not have to mark them manually; the compliance scanners work with auto-scaling.

To create a PCI Dynamic Asset Group for tagging instances in AWS

1. Go to Environment > Asset Groups.
2. Select Actions > Dynamic.
3. Enter the name of the asset group, for example PCI Dynamic Asset Group.
4. (Optional.) Enter a description for identifying this group.
5. Add the search criteria for the assets you want to be part of this group. Select AWS Tag aws:autoscaling:groupName.
6. Select Equal and enter PCI.
7. Click the + icon.
8. Click Apply Criteria.
9. Click Save.

How to Create a Dynamic Asset Group Based on a Sensor

In this example we are going to create a dynamic asset group based on a sensor. This is helpful when you have more than one USM Anywhere Sensor deployed in your environment. The asset group tags all assets monitored by the same sensor automatically. You do not have to mark them manually.

To create a dynamic asset group based on a sensor

1. Go to Environment > Asset.
2. From the Sensor filter on the left, select the USM Anywhere Sensor you want to create the asset group for.
   - The page reloads showing only the assets monitored by the selected sensor.
3. (Optional.) If desired, add filters to limit the assets to more specific criteria.

4. Select **Actions > Add to Asset Group**.

The Add Assets to Group dialog box displays.

5. Enter a name and description for the asset group.

6. Click **Save**.

The asset group is created. You can find it under Environment > Asset Groups.

**Asset Group List View**
USM Anywhere provides a centralized view of managing your asset groups. Go to Environment > Asset Groups to see this centralized view. It has the same look and feel as the asset list view and the functionalities are the same as well. The difference is that in this view, you are managing asset groups instead of assets.

By default, AT&T Cybersecurity creates these dynamic asset groups:

- **Assets with Agents**: Asset group containing assets with agents.
- **Assets with Alarms**: Asset group containing assets with alarms.
- **Assets with Vulnerabilities**: Asset group containing assets with vulnerabilities.
- **Database Servers**: Asset group containing database servers.
- **HIPAA**: Asset group containing Health Insurance Portability and Accountability Act (HIPAA) assets. HIPAA is a standard for protecting sensitive patient data.
- **Linux Assets**: Asset group containing Linux systems.
- **PCI DSS**: Asset group containing Payment Card Industry (PCI) assets.
- **Web Servers**: Asset group containing web servers.
- **Windows Assets**: Asset group containing Microsoft Windows systems.

USM Anywhere also creates a default asset group for each Amazon Web Services (AWS) Elastic Load Balancing (ELB) instance in your environment. The AWS Sensor ELB group includes the ELB instance and any AWS Sensor instance connected to the load balancer and registered with the ELB service. USM Anywhere automatically discovers and enables you to collect ELB access logs if you have ELB access logging enabled.

**Note:** It is not possible to edit or delete a dynamic asset group created by default.

The asset groups page displays asset groups inventory and information on those asset groups. On the left you can find the search and filter options. In the upper side of the page, you can see any filters you have applied, and you have the option to create and select different views of the asset groups. The main part of the page is the actual list of asset groups. Each row describes an individual asset group.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the \(\times\) icon to hide the filter pane. Click the \(\uparrow\) icon to expand the filter pane.

USM Anywhere creates by default static and dynamic asset groups. See [Creating an Asset Group](#).

### Asset Group List Details Options

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Group Description</td>
<td>Identifier for this group.</td>
</tr>
<tr>
<td>Assets</td>
<td>Number of assets in the group.</td>
</tr>
<tr>
<td>Asset Grouping</td>
<td>Type of asset grouping: static or dynamic.</td>
</tr>
<tr>
<td>Created</td>
<td>Exact date of creation of the asset group. The displayed date depends on your computer's time zone.</td>
</tr>
</tbody>
</table>

Next to the asset group name, click the \(\downarrow\) icon to access these options:

- **Full Details**: See [Viewing Assets Details](#) for more information.
- **Asset Group Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See [Running Asset Groups Scans](#) for more information.
Assign Credentials: See Managing Credentials in USM Anywhere for more information.

Authenticated Scan: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Authenticated Asset Scans for more information.

Configuration Issues: This option opens the Asset Group Details page. The Configuration Issues tab is selected in the page. See Viewing Assets Details for more information.

Vulnerabilities: This option opens the Asset Group Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

Alarms: This option opens the Asset Group Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

Events: This option opens the Asset Group Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Click Generate Report button to open the Configure Report dialog box. The management of this feature is similar to the one for assets, see Create an Assets Report for more details.

Select Actions > Static or Actions > Dynamic to create an asset group. See Creating a Static Asset Group and Creating a Dynamic Asset Group for more details.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

Views
You can configure the view you want for the list of items in the page.

To create a view configuration:
1. From the Asset Groups list view, select the filters you want to apply.
2. Select Save View > Save as...

The Save Current View dialog box opens.

Save Current View

Save a view of the current filter and table columns. Saved views can be exported as reports.

View Name

MyNewView

Share View

Save

3. Enter a name for the view.
4. Select Share View if you want to share your view with other users.
5. Click Save.
   The created view is already selected.

To select a configured view
1. From the Asset Groups list view, click View above the filters.
2. Click Saved views and select the view you want to see.

   Note: A shared view includes the icon next to its name.

3. Click Apply.

To delete a configured view
1. From the Asset Groups list view, click View above the filters.
2. Click Saved views and click the icon next to the saved view you want to delete.

   A dialog box displays to confirm the deletion.

   Note: You can delete the views you have created.

3. Click Accept.

   Important: The icon does not display if the view is selected.

Searching Asset Groups

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the Configure filters link located in the upper-left corner of the page. The management of filters is similar to that for assets. See Managing Filters for more information.

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Grouping</td>
<td>Filter asset groups by &quot;Static&quot; and &quot;Dynamic&quot;.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Use this filter to search for a specific value of a field. The advanced search is similar to that for assets. See Advanced Search Filter for more information.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Filter asset groups by the associated sensor.</td>
</tr>
<tr>
<td>Asset Origin Type</td>
<td>Filter asset groups by who added the asset group to the system.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>(Only for the AWS Sensor). Filter asset groups by AWS instance type.</td>
</tr>
<tr>
<td>Region</td>
<td>(Only for the AWS Sensor). Filter asset groups by AWS region.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter asset groups by Operating System.</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Filter asset groups by asset type. See USM Accepted Asset Types for more information.</td>
</tr>
</tbody>
</table>
Filters Displayed by Default in the Main Asset Groups Page (Continued)

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated Plugin</td>
<td>Filter asset groups by assets that have plugins manually enabled.</td>
</tr>
<tr>
<td>Service</td>
<td>Filter asset groups by service.</td>
</tr>
<tr>
<td>Software</td>
<td>Filter asset groups by software.</td>
</tr>
</tbody>
</table>

**Note:** Keep in mind that the "Enter search phrase" box and the "Asset Grouping" filter make the search in the asset groups. The rest of the filters make the search in the members of the asset group. So long as a member of the asset group matches the selected filter, USM Anywhere will display the asset group, even if there is only a member matching that filter.

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

**Icons Next to the Filter Title**

- Sort the filters alphabetically.
- Sort the filters by the number of items that match them.

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the X icon next to the filter. Or clear all filters by clicking Reset.

**Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.
USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

**Standard Mode**
This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

To activate the standard mode when the advanced mode is on
1. Go to Environment > Asset Groups.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray, .

**Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

**Advanced Mode**
Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

To activate the advanced mode
1. Go to Environment > Asset Groups.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.

   This turns the icon green, .
To perform a search in the advanced mode

1. Go to Environment > Asset Groups.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green, ☑️.
3. Click the filters that you want to select.
   The selected filters display inside a dashed rectangle.
4. In the lower-left corner of the page, click Apply Filters. Or in the upper side of the page, click Apply.
   The result of your search displays.

To search using the NOT operator

1. Go to Environment > Asset Groups.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.

Important: You have to select a filter to see this operator.

Note: The selected filter displays the icon and the filter chiclet is labeled in red.
Important: Some filters don't include the NOT operator (for example, Services or Software).

5. Click **Apply**.

To search all values of a filter:

1. Go to **Environment > Asset Groups**.
2. In the upper-left corner of the page, click the **Advanced** icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

**Searching Asset Groups by Using the Search Field**

Use the search field to enter queries and refine your search. You can enter free text, use wildcards, and use advanced search syntax. When searching, keep in mind the accepted query string syntax list in this table:
## Accepted Query String Syntax

<table>
<thead>
<tr>
<th>Type of Query</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard query with a blank space between terms</td>
<td>By default, a space between query terms is considered an implicit “OR”.</td>
<td>blacklist malicious</td>
</tr>
<tr>
<td>Literal, using double quotes</td>
<td>Matches entries that contain the same exact terms.</td>
<td>&quot;blacklist malicious&quot;</td>
</tr>
<tr>
<td>Boolean operators, using parentheses</td>
<td>They are AND, OR, and NOT. Parentheses can be used to group terms for precedence. Parentheses are also used to designate subsearches.</td>
<td>(http OR tcp) AND ftp</td>
</tr>
<tr>
<td>Wildcards, asterisk (*)</td>
<td>Matches any number of characters. Cannot be used at the beginning of a search query.</td>
<td>instance*</td>
</tr>
<tr>
<td>Wildcards, question mark (?)</td>
<td>Matches a single letter in a specific position. Cannot be used at the beginning of a search query.</td>
<td>qu?ck</td>
</tr>
<tr>
<td>Regexp, using /expression/</td>
<td>Regular expression inside forward slash characters. A dialog box opens to confirm the search.</td>
<td>/Describe.*Instances/</td>
</tr>
<tr>
<td>pulse:ID</td>
<td>Pulses are collections of IOCs. You need to insert the word pulse followed by a colon and the pulse</td>
<td>pulse:59432536c1970e343ce61bf0</td>
</tr>
</tbody>
</table>

Any characters may be used in a query, but certain characters are reserved and must be escaped. The reserved characters are these:

```
+ - = & | > < ! { } [ ] ^ " ~ \ /
```

Use a backslash (for example, "\>") to escape any reserved character (including a backslash).

### To search Asset Groups using the search field

1. Enter your query in the search field.
   
   If you want to search for a phrase containing two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   **Note:** Keep in mind that wildcard characters are considered as literals.

2. Click the icon.
The result of your search displays with the items identified.

**Advanced Search Filter on Asset Groups**

The Advanced Search filter enables you to enter a search value on a selected field. The following table shows the filter fields that you can find in the first drop-down list.

**Advanced Search Fields (First Drop-Down List)**

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filter asset groups by the name of the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>Filter asset groups by the asset description.</td>
</tr>
<tr>
<td>UUID</td>
<td>Filter asset groups by the universally unique identifier (UUID).</td>
</tr>
<tr>
<td>IP/CIDR</td>
<td>Filter asset groups by IP and Classless Inter-Domain Routing (CIDR).</td>
</tr>
<tr>
<td></td>
<td>This is a method for allocating IP addresses and routing IP packets. It is the range of IP addresses that define the network.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Filter asset groups by Fully Qualified Domain Name (FQDN).</td>
</tr>
<tr>
<td>Asset Type</td>
<td>Filter asset groups by asset type.</td>
</tr>
<tr>
<td>Instance Type</td>
<td>Filter asset groups by instance type.</td>
</tr>
<tr>
<td>Region</td>
<td>Filter asset groups by region.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter asset groups by operating system.</td>
</tr>
<tr>
<td>Service</td>
<td>Filter asset groups by service.</td>
</tr>
<tr>
<td>Software</td>
<td>Filter asset groups by software.</td>
</tr>
<tr>
<td>Associated Plugin</td>
<td>Filter asset groups by the plugin associated to the asset.</td>
</tr>
<tr>
<td>Alarm Counter</td>
<td>Filter asset groups by the number of alarms.</td>
</tr>
<tr>
<td>Event Counter</td>
<td>Filter asset groups by the number of events.</td>
</tr>
<tr>
<td>Vulnerability Counter</td>
<td>Filter asset groups by the number of vulnerabilities.</td>
</tr>
<tr>
<td>Configuration Issue Counter</td>
<td>Filter asset groups by the number of configuration issues.</td>
</tr>
<tr>
<td>PCI Asset</td>
<td>Filter asset groups by Payment Card Industry (PCI) Asset, if the asset is included or not in the PCI Data Security Standards (DSS) Asset Group. See <a href="#">Asset Group List View</a> and <a href="#">Working with Assets and PCI DSS</a> for more information.</td>
</tr>
</tbody>
</table>
**Advanced Search Fields (First Drop-Down List) (Continued)**

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Asset</td>
<td>Filter asset groups by Health Insurance Portability and Accountability Act (HIPAA) Asset, whether the asset is included in the HIPAA Asset Group. See Asset Group List View for more information.</td>
</tr>
<tr>
<td>Custom User Fields</td>
<td>Filter asset groups by the fields you have created. If you have not created fields, this filter does not display.</td>
</tr>
</tbody>
</table>

**Note:** The result of a search when you use the Alarm Counter filter or the Event Counter filter depends on if an alarm or an event can identify the source or destination as an asset in the inventory. Your environment can have alarms or events associated with assets both included in the inventory and those not included in the inventory.

The following table shows the operators that you can find in the second drop-down list.

**Advanced Search Fields (Second Drop-Down List)**

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>Greater than.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than.</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to.</td>
</tr>
<tr>
<td>Equal</td>
<td>Equal to.</td>
</tr>
<tr>
<td>IP Range</td>
<td>Range of IP addresses.</td>
</tr>
<tr>
<td>Is Empty</td>
<td>Include assets with no IP addresses. This operator is available only for IP/CIDR.</td>
</tr>
<tr>
<td>Is Not Empty</td>
<td>Include assets with IP addresses. This operator is available only for IP/CIDR.</td>
</tr>
<tr>
<td>Like</td>
<td>Search for the specified pattern.</td>
</tr>
<tr>
<td>Not Equal</td>
<td>Not equal to.</td>
</tr>
<tr>
<td>Not Like</td>
<td>Not true.</td>
</tr>
</tbody>
</table>

**Important:** Some filters don't include the NOT operator (for example, Services or Software).
To search asset groups using the advanced search filter

1. Go to **Environment > Asset Groups**.
2. Below Advanced Search filter, click **Add Filter**.
3. Select a field from the first drop-down list.
4. Select an operator from the drop-down list.

**Important:** Depending on the field you have chosen in the first drop-down list, the operators vary.
5. Enter the search value.
   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

6. Click the icon.

7. Click Add Filter if you want to add a new search.

8. Click the icon.

9. Click Apply.

The result of your search displays with the assets identified.
USM Anywhere enables you to run a scan against assets included in an asset group. To accomplish this, the scanner sends crafted packets to the target asset group and analyzes the responses. This is not an authenticated scan.

**Note:** If you want to discover new assets, you can run an asset discovery scan. See **Running an Asset Discovery** for more information.

### To run an asset group scan from Asset Groups

1. Go to **Environment > Asset Groups**.
   - Next to the asset group name that you want to scan, click the **icon**, select **Full Details**, and then select **Actions > Asset Group Scan**.
   - or
   - Next to the asset group name that you want to scan, click the **icon** and select **Asset Group Scan** to directly start the asset group scan.

2. Select the scan profile that you want to run:
   - **Discovery**: This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)
   - **Complete**: This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)
   - **Vulnerability Discovery**: Performs general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.
   - **Extended Vulnerability Discovery**: Performs a Vulnerability Discovery scan, which actively discovers more about the network.
   - **Intensive Vulnerability Discovery**: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

3. Select **Set Debug Mode** if you want to log the results of the scan or if you have a problem with a scan.
   - This option is disabled by default.

   **Note:** The Set Debug Mode option must be used only for debugging purposes because it needs a large amount of disk space for the file or files it generates. Only AT&T Cybersecurity Technical Support should review these files. You can contact this department for more information.

4. Click **Scan**.
5. In the Asset Groups details page, click **Scan History** in the table area to display the results of the scan. You can see the scan if it has completed or not.

**Note:** See **Scheduling Asset Group Scans from Asset Groups** and **Scheduling Asset Groups Scans from the Job Scheduler Page** for more information about how to schedule an asset group scan.

### Running an Asset Discovery

Asset Discovery finds and provides you visibility into the assets in your environments. You can discover all the IP-enabled devices on your network, determining what software and services are installed on them, how they are configured, and which active threats are being executed against them.
To run an asset discovery from Settings
1. Go to Data Sources > Sensors to open the Sensors page.
2. Click the sensor you want to run an asset discovery.
3. Click the Asset Discovery tab to open the Asset Discovery window.

Important: Make sure when you use a virtual private network (VPN) using a Cisco Firewall, that arp-proxy is enabled in the firewall. Otherwise, all the assets will be reported using the same media access control (MAC) address, and USM Anywhere will consider all of them to be different interfaces for the same asset.

4. Click Yes to scan the network.

This step may be different depending on the sensor you have installed.

Note: In Amazon Web Services (AWS) Sensors, this option is not available because the instances are automatically set.

5. Click Scan Another to start a new scan or click Next to continue with the following step.

6. In the Asset Groups details page, click Scan History in the table area to display the results of the scan. You can see the status of each scan and the details.

Important: If you run Asset Discovery in an environment that discovers assets using a native application (AWS, Google Cloud Platform [GCP], Microsoft Azure, VMware, etc.), or in a Dynamic Host Configuration Protocol (DHCP) network environment, then you could potentially duplicate assets in USM Anywhere. You can configure local DNS Nameservers to avoid duplicate assets from being created and update existing assets with the new and correct IP Address. See Defining the DNS Nameservers for more information.

Running Authenticated Asset Groups Scans

An authenticated asset scan verifies scanned IPs within an Asset Group and detects vulnerabilities. Log in as administrator or root to perform an authenticated scan. See Managing Credentials in USM Anywhere for more information.

Warning: Keep in mind that an authenticated scan may fail if the local mail exchanger, which applies to Linux hosts, is enabled in the target asset.

USM Anywhere™ User Guide

Asset Scan Credentials and Escalation Options

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Method and Credentials</th>
<th>Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux, BSD, Solaris, or macOS</td>
<td>SSH password or public key authentication</td>
<td>sudo or su</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>SSH password</td>
<td>enable password</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows username and password through Windows Remote Management</td>
<td>None</td>
</tr>
</tbody>
</table>

To run an authenticated asset scan from Asset Groups
1. Go to Environment > Asset Groups.
   - Next to the asset group name that you want to scan, click the ✔ icon, select Full Details, and then click Actions > Authenticated Scan.
Next to the asset group name that you want to scan, click the ✔ icon and select **Authenticated Scan** to directly start the asset group scan. If the option is not enabled, you will need to add a credential. See [Managing Credentials in USM Anywhere](#).

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

2. In the asset group details page, click **Scan History** in the table area to display the results of the scan. You can see the status of each scan and its details, which informs you if the scan has been successful or not. You can also click a line to expand the asset group row to check the individual asset results. Each asset group will have a **Scan Details** link you can click to download a zip file containing the details of the recent scan. The link will only be present for the most recent scan of each asset, and will be available for one week after the scan has been run.

Click **Scan Details** to download the zip file:

- If you click **Scan Details** located in the asset group job row, the downloaded file will include one file per scanned asset.
- If you click **Scan Details** located in the individual asset results, the downloaded file will include the information for just that asset.

**Note:** You can see the vulnerabilities that the scan has found below the Vulnerabilities Events tab.

### Scheduling Asset Group Scans from Asset Groups

USM Anywhere provides a simple way to include scans for scheduling using its web user interface (UI). See [USM Anywhere Scheduler](#) for more information.

#### Scheduling Asset Group Scans

To schedule an asset group scan job from the asset group details window:

1. Go to **Environment > Asset Groups**.
2. Click the ✔ icon you want to include in an asset group scan and select **Full Details**.
3. Click **Actions > Schedule Scan Job**.

The Schedule New Job dialog box opens.

---

**USM Anywhere™ User Guide**
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Asset Scanner.
   Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a USM Anywhere sensor in case you have more than one installed.
5. Select the **App Action:**
   - **Asset Discovery**
     Discovers assets in your environment, detects changes in assets, and discovers malicious assets in the network.
Select Existing Asset Group: In the *Enter asset group name* field, search for the asset groups to scan. These asset groups are already existing, and you can search for them by entering the name of the asset group or by browsing for them.

Create New Asset Group to Scan Using CIDR Block: You can create a new asset group from a Classless Inter-Domain Routing (CIDR) block. You need to indicate the CIDR block and the network name you want to scan. This option discovers new assets and scans the discovered assets.

**Important:** Use the Create New Asset Group to Scan Using CIDR Block option for creating new CIDR-based asset groups without leaving the scheduler form. After clicking Save, a new asset group based on the selected CIDR is created.

Your scan job will have the Select Existing Asset Group option selected and the CIDR-based asset group assigned automatically.

**Important:** Make sure when you use a virtual private network (VPN) using a Cisco Firewall, that arp-proxy is enabled in the firewall. Otherwise, all the assets will be reported using the same media access control (MAC) address, and USM Anywhere will consider all of them to be different interfaces for the same asset.

Asset Group Scan

Discovers services, operating systems, hostnames, IP and MAC addresses, and vulnerabilities of known hosts. This option scans the assets that are already in the group.

The Asset Group field displays the name of the asset group to scan. You can't modify this field.

6. In the App Action field, the Asset Group Scan is the default option.
7. Select the scan profile that you want to run:
   - **Discovery:** This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)
   - **Complete:** This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)
   - **Vulnerability Discovery:** Performs general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.
   - **Extended Vulnerability Discovery:** Performs a Vulnerability Discovery scan, which actively discovers more about the network.
Intensive Vulnerability Discovery: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

8. (Optional.) Select the assets you want to exclude from the scan.

9. Select Set Debug Mode if you want to log the results of the scan or if you have a problem with a scan. This option is disabled by default.

Note: The Set Debug Mode option must be used only for debugging purposes because it needs a large amount of disk space for the file or files that it generates. Only AT&T Cybersecurity Technical Support should review these files. You can contact this department for more information.

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

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

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

b. Set the interval options for the increment.

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

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

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

11. Click Save.
The job now displays in the job scheduler list.

**Note:** See [USM Anywhere Scheduler](https://www.usmauth.com/scheduler) for more information.

---

### Scheduling Authenticated Asset Group Scans from Asset Groups

USM Anywhere provides a simple way to include authenticated scans for scheduling using its web user interface (UI). See [USM Anywhere Scheduler](https://www.usmauth.com/scheduler) for more information.

To schedule an authenticated asset group scan job from the asset group details window:

1. Go to **Environment > Asset Groups**.
2. Click the ✅ icon you want to include in an asset scan and select **Full Details**.
3. Select **Actions > Schedule Scan Job**.
4. The Schedule New Job dialog box opens.

---

**USM Anywhere™**

**User Guide**
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Authenticated Asset Scanner.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, Asset Group Scan is the default option.
6. In the Asset Group field, you can either enter the asset group name or browse asset groups.
7. In the Schedule section, specify when USM Anywhere runs the job:
a. Select the increment as **Minute, Hour, Day, Week, Month, or Year**.

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

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

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

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

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

8. Click **Save**.
The job now displays in the job scheduler list.

*Note:* See **USM Anywhere Scheduler** for more information.
Configuring an Asset Group

### Configuring a Static Asset Group

To configure a static asset group

1. Go to **Environment > Asset Groups**.
2. Click the icon you want to configure and select **Configure Asset Group**.
3. Modify the name of the asset group if you need to. This field is required.
4. (Optional.) Modify the description if you need to.
5. You can add search criteria to the group. Click **Apply Criteria** if you want to add the searched criteria.
6. You also can modify or delete assets from the group by clicking the or icons.
7. Use **Delete** to delete the group or **Cancel** to discard changes.
8. Click **Save**.

### Configuring a Dynamic Asset Group

To configure a dynamic asset group

1. Go to **Environment > Asset Groups**.
2. Click the icon you want to configure and select **Configure Asset Group**.
3. Modify the name of the asset group if you need to. This field is required.
4. (Optional.) Modify the description.
5. Search the assets you want to add to the group and click **Add Asset** or **Scan Network**.
   - If you click **Scan Network**, type the name of a network and the CIDR block to specify the subnet’s IP Address block that you want to scan.
6. You can also delete assets from the group by clicking the icon. You can view a specific asset by clicking the icon.
7. Use **Cancel** to discard the changes and **Delete** to delete the group.
8. Click **Save**.

### Viewing Asset Group Details

From the **Asset Group List** view, you can display the details of an asset group.

To view the details of an asset group

1. Go to **Environment > Asset Groups**.
2. Click the icon whose details you want to view.
3. Select **Full Details**.
In the asset groups details, on the upper left side of the page, you see the name, the description, the type of grouping, the number of assets that are part of that group, and the criteria of grouping.

On the right, you see the status summary for your asset group. It displays the total number of configuration issues, vulnerabilities, alarms, and events. The circle can display in orange (for alarms and configuration issues), blue for events, and red for vulnerabilities. There is a number inside each circle to indicate the number of alarms, events, vulnerabilities and configuration issues associated with the members of the asset group. You can click each circle to explore the information of each one.

**Note:** Configuration Issues are only available for AWS and Azure Sensors.

At the bottom, there is a table area with tabs, some of which correspond to the circles. Each tab contains a table with records, if present, for your asset group.

### Asset Groups Details view tab description

<table>
<thead>
<tr>
<th>Tab</th>
<th>Information Shown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>Assets that are part of the group. Click <strong>View</strong> to go to the details of the asset.</td>
</tr>
<tr>
<td>Software</td>
<td>Software installed on the assets of the group.</td>
</tr>
<tr>
<td>Services</td>
<td>Services available on the assets of the group.</td>
</tr>
<tr>
<td>Alarms</td>
<td>Alarms related to the assets of the group. There is a bubble graph that provides a graphical representation of alarms by intent. Blue circles indicate the number of times that an alarm in an intent showed. A bigger circle indicates a higher number of alarms. You can hover over each of the circles to get the actual number of different types of intent. In addition, if you click any of the blue circles, USM Anywhere displays only the alarms corresponding to that circle. You can change the displayed period of time by clicking the <strong>Last 24 Hours</strong> filter.</td>
</tr>
<tr>
<td>Events</td>
<td>Events related to the assets of the group. Click an event to see its details.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Vulnerabilities related to the assets of the group. You can filter the active or inactive vulnerabilities by clicking the specific radio button. Click a vulnerability to see its details.</td>
</tr>
<tr>
<td>Configuration Issues</td>
<td>Information about operational processes. You can filter the active or inactive configuration issues by clicking the specific radio button. Click a configuration issue to see its details.</td>
</tr>
<tr>
<td>History</td>
<td>Additions and removals to the group.</td>
</tr>
<tr>
<td>Scan History</td>
<td>List of the asset scans already run. It includes a time-stamp of the scan, the scan type, its status, and the details of each scan. You can also click the <strong>Scan Details</strong> link here to download a file containing the details of the most recent authenticated asset group scan here for up to a week after the scan was run.</td>
</tr>
</tbody>
</table>

The button **Actions**, located in the upper right side of the page, enables you to access these options:

- **Configure Asset Group**, see [Configuring an Asset Group](#) for more details.
- **Delete Asset Group**, see [Deleting an Asset Group](#) for more details.
- **Edit Fields**. This option is similar to the one for Assets, see [To assign asset fields to an asset or group of assets](#) for more details.
Note: Keep in mind if you assign an asset field to an asset group, you assign the asset field to its members, not to the asset group.

- Assign Credentials to Group Members. This option assigns credentials to the members of the asset group. This option is similar to the one for Assets, see Managing Credentials in USM Anywhere for more details.
- Assign Agent Profile. This option assigns a specific agent profile to the members of the asset group. See Assigning AlienVault Agent Configuration Profiles to Asset Groups for more information.
- Set Sensor, see To assign a sensor to an asset group for more details.
- Asset Group Scan, see Running Asset Groups Scans.
- Assign Credentials. This option assigns credentials to current members of the Asset Group and Assets added to the group later. See Managing Credentials in USM Anywhere for more details.
- Authenticated Scan, see Running Authenticated Asset Groups Scans.
- Schedule Scan Job, see Scheduling Asset Group Scans from Asset Groups, Scheduling Authenticated Asset Group Scans from Asset Groups, and Scheduling Asset Groups Scans from the Job Scheduler Page for more details.

Deleting an Asset Group

There are two ways to delete an asset group:
- From the asset groups list view
- From the edit asset group details page

Note: It is not possible to edit or delete a dynamic asset group created by default.

To delete an asset group from the list view
1. Go to Environment > Asset Groups.
2. Next to the asset group you want to delete, click the icon.
3. Select Delete Asset Group to display a new window and confirm the deletion.
4. Click Delete.
To delete an asset group from the edit asset group details page

1. Go to **Environment > Asset Groups**.
2. Click the icon you want to delete and select **Full Details**.
3. Select **Actions > Delete Asset Group** to open a new window and confirm the deletion.
4. Click **Delete**.

**User Behavior Analytics**

User behavior analytics (UBA) extends your USM Anywhere Sensor's awareness by enabling it to track actors as well as assets within your environment. With UBA, USM Anywhere can help you identify malicious or compromised users, and enable you to better prioritize alarms with the addition of user data.

In addition to analyzing users, UBA also analyzes each of a user's separate accounts, and enables you to manually combine detected users to ensure that your user analytics are accurate. Events and alarms can thus be enhanced with user data, including user entities and their individual accounts, as either the source user or the destination user.

To incorporate UBA into your USM Anywhere instance, you must provide information about all users acting in your environment. Each user must be identified by a unique username and account type.

Once users have been identified, there are several tasks that you must complete to ensure that complete and actionable data is being captured and acted upon. This chapter describes these necessary tasks, and covers topics such as user discovery and merging, user scans, user monitoring, and configuration.

This topic discusses these subtopics:

- **User List View**
- **User Discovery**
- **Understanding User Status in User Data Sources**
- **Viewing Full User Details**
- **Events, Alarms, and Notifications Created When a User's Status Changes**
- **Merging Users**
- **Deleting Users**
- **Importing Users from a CSV File**
USM Anywhere provides a centralized view of users in your environment. To view the user list, go to Environment > Users.

The Users main page displays user inventory and information on those users. On the left side of the page, you can find the search and filter options. At the top of the page, you can see any filters you have applied. The main part of the page is the list of users, where each row describes an individual user.

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

**Note:** User entities with no name or service account in their name field appear as "Unspecified".

The following table lists the default columns that appear in the user list view, and their descriptions.
<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>An actor (person or service account) active in your environment (sometimes referred to as the <em>user entity</em>).</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time on which that user was last active in your environment.</td>
</tr>
<tr>
<td>Email</td>
<td>A list of the email addresses associated with that user entity.</td>
</tr>
<tr>
<td>Origins</td>
<td>The name of each sensor in which one of this user's accounts was discovered.</td>
</tr>
</tbody>
</table>

Click the ▼ icon to access these options:

- **Full Details**: Navigate to this user's Full Details page.
- **Configure User**: Open the Configure User dialog box.
- **Merge User**: Open the Merge User dialog box.
- **Delete User**: Delete this user.

**Important**: Deleting a user is a permanent action and cannot be undone.
User Discovery

USM Anywhere automatically discovers users in your environment with the user discovery jobs you have configured. See Scheduling User Discovery Jobs from the Job Scheduler Page to learn about these jobs and how to configure them.

Users Discovered in Your Environment

USM Anywhere uses the user discovery jobs you have configured to extract and maintain an updated list of the users who are active in your environment. User accounts are discovered and matched by comparing specific fields from your environment, that differ between user authentication mechanisms. This means that the fields USM Anywhere uses to detect and resolve discovered users in Amazon Web Services (AWS) will differ from the fields used in Google Cloud Platform (GCP) or Okta. The following table outlines which fields are used in each user source.

### Possible User Entity and Account States

<table>
<thead>
<tr>
<th>User Source</th>
<th>User Account Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>SOURCE_USERNAME and SOURCE_ACCOUNT</td>
</tr>
<tr>
<td>AD</td>
<td>SOURCE_USERNAME</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USERNAME</td>
</tr>
<tr>
<td></td>
<td>SOURCE_USERNAME and SOURCE_NTDOMAIN</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USERNAME and DESTINATION_NTDOMAIN</td>
</tr>
<tr>
<td>Azure AD and Office 365</td>
<td>SOURCE_USERNAME</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USERNAME</td>
</tr>
<tr>
<td>Okta</td>
<td>SOURCE_USERNAME</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USERNAME</td>
</tr>
<tr>
<td>G Suite and GCP</td>
<td>SOURCE_USERNAME</td>
</tr>
<tr>
<td></td>
<td>SOURCE_USER_EMAIL</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USERNAME</td>
</tr>
<tr>
<td></td>
<td>DESTINATION_USER_EMAIL</td>
</tr>
</tbody>
</table>

To see a list of the users active in your environment and their accounts:

1. Go to Environment > Users.
   - All of your discovered users are listed here.

   **Note:** By default, inactive users are not shown. You can use this list's filters to view them.

2. Click the name (or the chevron next to the name) of a user whose accounts you want to view, and then click Full User Details.
This user's accounts are listed under the Accounts tab.

**Active and Inactive Users**

In addition to detecting which users are active in each environment, USM Anywhere carefully tracks users and user accounts that have become inactive. This enables USM Anywhere advanced threat detection capabilities, which take a user's activity and account status into consideration in generating and prioritizing alarms.

While different user authentication mechanisms each approach users' active status differently, USM Anywhere normalizes all of those disparate approaches to present one unified and unambiguous reporting of the status of each user entity and all of its accounts.

**Note:** See [Understanding User Status in the User Data Source](#) to read more about how each user authentication mechanism handles users' statuses.

To view a user entity's or account's status, check the dot next to the username or account name. When the dot is green, the user or account it represents is active. If it is gray, the user or account it represents is in a status other than active.

These are the possible user entity and account states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>If any of the user's accounts are active, the user is active.</td>
</tr>
<tr>
<td>Inactive</td>
<td>If all of the user's accounts are in a status other than active, the user is inactive.</td>
</tr>
</tbody>
</table>
### Possible User Entity and Account States (Continued)

<table>
<thead>
<tr>
<th>Data Source</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Active</td>
<td>A user account is active when it's validated and reported by the provider API.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>When a user account is disabled by the provider but still reported by the provider API, that user account is considered disabled.</td>
</tr>
<tr>
<td></td>
<td>Retired</td>
<td>When a user account no longer exists in the provider system, that account is considered retired.</td>
</tr>
</tbody>
</table>

**Note:** Due to the information provided by AWS, AWS user accounts are marked "retired" when they have not appeared in any scans for 30 days.

### Understanding User Status in User Data Sources

USM Anywhere detects the status of user entities and their accounts, and normalizes those statuses for you under Environment > Users. To understand how USM Anywhere normalizes these statuses, review the following table. This table lists the normalized states for each data source next to the unique states that map to them in the data source.

**Note:** See Managing Users to read more about how USM Anywhere uses and displays the normalized states for users and their accounts.

#### User Account States by User Data Source

<table>
<thead>
<tr>
<th>Data Source</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Retired</td>
<td>The user is no longer listed in Identity and Access Management (IAM).</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Unsupported.</td>
</tr>
<tr>
<td>Azure</td>
<td>Retired</td>
<td>The user is deleted from Microsoft Azure Active Directory (AD).</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>The &quot;Block sign in&quot; value is &quot;Yes&quot;.</td>
</tr>
<tr>
<td>Active directory and Office 365</td>
<td>Retired</td>
<td>The user is sent to the Microsoft Windows Recycle Bin using the delete action.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>&quot;disabled&quot; is flagged in the properties dialog box.</td>
</tr>
<tr>
<td>GCP</td>
<td>Retired</td>
<td>The &quot;deletionTime&quot; field has any value.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>The account is flagged as &quot;suspended&quot;.</td>
</tr>
<tr>
<td>Okta</td>
<td>Retired</td>
<td>The user is deleted from the directory screen.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>&quot;userStatus&quot; is set to any value other than &quot;Active&quot;.</td>
</tr>
</tbody>
</table>

### Viewing Full User Details
To view a user's full details

1. Go to **Environment > Users**.
2. Next to the user name whose details you want to review, click the ✔ icon.
3. Select **Full Details**.

In the upper left side of the page, you see the details for the user entity, including their description, last seen datestamp, location, manager, phone number, and emails. On any user that has been merged, you will see a list of emails.

Across the bottom of the page, you see the accounts, alarms, and events for your asset.

**User Accounts**

You will find all of this user's accounts listed under the Accounts tab.

- **Application**: The application in which this user account is active.
- **Status**: The status of the user account. A green circle indicates that the account is active, while a gray circle indicates that the account is inactive. See [Understanding User Status in User Data Sources](#) for more information about these statuses.
- **Origin**: The name of the sensor in which this user account was discovered.
- **User Name**: The username or service account name associated with this user account.
- **Account Name**: The organizational account in which this user account exists.
- **Description**: This description comes from the user account source and is not editable in USM Anywhere.

**User Alarms**

You will find all of the alarms related to this user account under the Alarms tab. An alarm may be related to a user if that user was the source of the action (the source user) or was acted upon (the destination user).

**Note**: You can filter the alarms list by limiting the Created Date using the dropdown on the right.

To view a user's alarms

1. Go to **Environment > Users**.
2. Next to the name of the user whose events or alarms you want to view, click the ✔ icon.
3. Select **Full User Details**.
4. Click the Alarms tab to view this user's alarms.

The columns in the Alarms table are automatically populated from the alarms. See Alarm Management for more information about these alarm details.

User Events

You will find all of the events related to this user account under the Eventstab. An event may be related to a user if that user was the source of the action (the source user) or was acted upon (the destination user).

**Note:** You can filter the events list by limiting the Created Date using the drop-down on the right.

To view a user's events

1. Go to Environment > Users.
2. Next to the name of the user whose events or alarms you want to view, click the icon.
3. Select Full User Details.
4. Click the Events tab to view this user's events.
The columns in the Events table are automatically populated from the events. See Event Management for more information about these event details.

Events, Alarms, and Notifications Created When a User's Status Changes

USM Anywhere enables you to configure alarms to alert you when a user's entity or account status changes. USM Anywhere generates monitoring events that display in the Events List View page. See Events List View for more information. You can see two types of monitoring events related to User Behavior Analytics (UBA) user status: user status changed and account status changed. From these events, you may configure alarm rules to alert you when these status changes trigger events.

USM Anywhere™
User Guide
To see events created when a user entity or account status changes

1. Go to Settings > System Events.
2. Locate the Event Name filter and select either User Status Changed or Account Status Changed.
3. Click the event to see its details.
To create alarm rules when a user entity or account status changes:

1. Go to **Settings > Rules** and either:
   - Click **Create Orchestration Rule > Create Alarm Rule**.
   - Or click **Alarm Rules**, and then click **Create Alarm Rule**.
2. Populate the new alarm rule as described in **Alarm Rules**.
3. Under Rule Condition, use the Match drop-down list to select **system_events**.
4. Click **Add Condition**.
5. Select **Event Name**, then **Equals**, and then either **User Status Changed** or **Account Status Changed**.

![Rule Condition](image)

**CURRENT RULE**

\[(packet_type == \text{system_event}) \land (event\_name == \text{Account Status Changed}) \lor (event\_name == \text{User Status Changed})\]

6. Click **Save Rule**.

The alarm rule has been created. You can see it from **Settings > Rules**. See Alarm Rules from the Orchestration Rules Page for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### Merging Users

If there are user entities in your user list who all represent the same user in your environment, you have the option of manually merging the entities together. The resulting single user entity retains associations with all user accounts connected to any of the former user entities, and after the merge will behave in every way as one single user entity.

When two users are merged, all of the user accounts, activity, and associated alarms and events from each user entity are unified under a single merged user entity. User details (like "Description", "Location", and "Phone") are merged using the...
Primary User principle. During the merge process, User Behavior Analytics (UBA) will look for user details in your primary user entity first, and populate the newly merged user entity with those details. If the primary user has a blank detail field, UBA will use data from the secondary user to populate that field in the merged user.

**Important:** Any data from the secondary user that is not included in the resulting merged user entity will be deleted after the merge process is complete.

The one exception to this rule is a user’s email address. If both of your user entities have email addresses, instead of keeping the primary and discarding the secondary, the resulting merged user will retain both emails in a comma-separated list. Similarly, every email associated with a user entity is preserved through the merge process.

**Note:** While secondary user entities are deleted as part of the merge process, if you search for a user who has been merged and deleted, your search will automatically return the user entity into which your searched user was merged.

To merge two users

1. Go to **Environment > Users**.
2. Next to the user-name of one of the two users you wish to merge, click the icon.
3. Select **Full Details**.
4. Click **Actions**, and then click **Merge User**.
   
   The merge users dialog box opens.

**Note:** You can also access this dialog by click the icon on the User List view.
5. Use the search bar on the right to search for the other user you wish to merge, and select it from the list.

6. Use the radio buttons to identify one of the users as the primary.

7. Click **Review**.

   The review window opens. This is where you can preview all of the user accounts that will be united under your new merged user entity.

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Seen</strong></td>
<td><strong>Last Seen</strong></td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td><strong>Location</strong></td>
</tr>
<tr>
<td>Austin</td>
<td>San Mateo</td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td><strong>Manager</strong></td>
</tr>
<tr>
<td>Gregory Shelton</td>
<td>Gregory Shelton</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td><strong>Phone</strong></td>
</tr>
<tr>
<td>(512)555-0293</td>
<td>(512)555-0652</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td><strong>Email</strong></td>
</tr>
<tr>
<td><a href="mailto:ballen@fakedomain.com">ballen@fakedomain.com</a></td>
<td><a href="mailto:agibson@fakedomain.com">agibson@fakedomain.com</a></td>
</tr>
</tbody>
</table>
8. If all of the accounts are correct, click Merge.

When the merge process completes, you will see a new Full User Details page displaying the details of your newly merged user.

Deleting Users

USM Anywhere™ User Guide

USM Anywhere provides different ways to delete users from your user behavior monitoring:

- Deleting users from the List view
- Deleting users from the User Details page
- Deleting user accounts from the User Details page

**Important:** Deleting a user is an action that cannot be undone.
To delete a user from the list view

1. Go to **Environment > Users**.
2. Next to the username you want to delete, click the **v** icon and select **Delete User**.

The delete user dialog box opens.

To delete a user from the User Details Page

1. Go to **Environment > Users**.
2. Next to the username you want to delete, click the **v** icon and select **Full Details**.
3. Click **Actions > Delete User**.
   
   The delete user dialog box opens.
4. Click **Delete**.
To delete a user account

1. Go to **Environment > Users**.
2. Next to the name of the user whose account you want to delete, click the [ ] icon and select **Full Details**.
3. Under the Accounts tab, click the **[ ]** icon.

   ![Accounts Table]

   The delete user dialog box opens.

4. Click **Delete**.

Importing Users from a CSV File

USM Anywhere enables you to import users from a CSV or text file. Use this option to add users in large quantities to your environment from a single file. User information added this way supersedes user information from other sources but will not remove any preexisting information about any users in your environment.

**Warning:** If the file does not follow the specific format, the users will not be successfully imported. See About the CSV File for more information.

To import users from a CSV file

1. Go to **Environment > Users**.
2. Click **Actions > Import Users** to open the Import Users dialog box.

   ![Import Users Dialog]

   **Note:** If a user in your CSV or text file shares an email address with an existing user behavior analytics (UBA) user, then all fields from your file will be added to that existing user's entry. Where both the existing user and your file's entry have information in a field, the fields will be combined, with the file's information becoming the new primary.

3. Drop your file or select the file from your desktop.
   Once you select a file, the name of the file displays and the Import button is active.

4. Click Import to start the process.
   You can see the status of the process from how many users have been processed or are pending, or which users were not imported. In the About the CSV File section, there is a table where you can see the import errors and the reasons for which a user has not been imported.

   **Note:** When an import process starts and finishes, USM Anywhere generates system events. See Searching for System Events Related to a User Import Process for more information.

**About the CSV File**

The CSV file must use this format; no other fields are allowed:

*User Name; User Email; Manager Name; Office Location; Phone Number; Description*
Important: Do not include a header line in the CSV file because it will result in an error of invalid format.

You need to provide at minimum a username and user email valid for USM Anywhere. All other fields are optional.

Please note the following:

- There must be only one user per row.
- You can import all the files you need, but only one at a time.
- The maximum number of lines in the CSV file is 100,000.
- The maximum size of the CSV file is 25 MB.

Searching for System Events related to a User Import Process

USM Anywhere generates system events when an import process starts and finishes.

To look for system events related to an import process

1. Go to Settings > System Events.
2. Locate the Event Name filter.
3. Select one of these filters:
   - **User Import Process Finished**: This option displays the system events generated when the user import process from a CSV file finishes.
   - **User Import Process Started**: This option displays the system events generated when the user import process from a CSV file starts.

   The result of your search is displayed.

USM Anywhere™ User Guide
Alarms Management

An alarm in USM Anywhere consists of one or more events, based on one of the following:

- One or more rules performed by the correlation engine of USM Anywhere, which analyzes these events for behavioral patterns. These rules look at and connect events to assess their priority and reliability. When the engine identifies a pattern, it generates an alarm, which requires attention and investigation. See Correlation Rules for more information.

  **Important:** The "Suspicious Behavior - OTX Indicators of Compromise" correlation rule generates alarms if the pulse comes from the AlienVault OTX account.

- One orchestration rule, which is designed to raise an alarm when a particular type of event is found. See Orchestration Rules for more information.

  **Note:** USM Anywhere stores 10 of the events which have generated the alarm, for 365 days. If the alarm was generated by more than 10 events, USM Anywhere stores the first and the last 9 events.

USM Anywhere enables you to drive actions in response to incoming alarms. Perhaps the most common action is sending an email to administrators to provide real-time notification of a critical security incident. Each user can decide if wants to receive alarm notifications. See Managing Your Profile Settings for more information.

  **Note:** You can watch the Conducting Security Analysis with AT&T Cybersecurity USM Anywhere customer training webcast on-demand to learn how to leverage USM Anywhere to perform security analyst duties.

This topic discusses these subtopics:

- Alarms List View
- Selecting Alarms in Alarm List View
- Searching Alarms
- Viewing Alarm Details
- Labeling the Alarms
- Alarm Status
- Create Alarms Report
USM Anywhere provides a centralized view of your alarms. Go to Activity > Alarms to see this centralized view.

**Note:** You can watch the Conducting Security Analysis with AT&T Cybersecurity USM Anywhere customer training webcast on-demand to learn how to leverage USM Anywhere to perform security analyst duties.

The Alarms page displays information on alarms. These are the different parts of the Alarms page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the alarms.
- The main part of the page is the list of alarms, where each row describes an individual alarm. Click an alarm to open a summary view. See Viewing Alarm Details for more information. Each alarm includes a check box that you can use to select it. You can select all alarms in the same page by clicking the check box in the first column of the header row. You can also select all the alarms in the system. See Selecting Alarms in Alarm List View for more information.

**Important:** An alarm is created when USM Anywhere receives the event, which may appear later than the time when the event was created. You can verify by comparing the Time Created and Time Received field of an event.

### Refreshing the page

USM Anywhere gives you the option of refreshing the page automatically in a period of time that you can configure.

You can configure a period of time for refreshing the data on the Alarm page. See Managing Your Profile Settings for more information.

Following the name of the view, you can click the icon to stop the auto-refresh countdown and refresh the page manually.

There is an auto-refresh countdown that refreshes the page at a regular interval. The number inside the blue circle indicates the remaining time until the next refresh. See Managing Your Profile Settings to configure this interval.
Alarm Summary Graph

The section above the page includes a bubble graph that provides a graphical representation of alarms by intent. Blue circles indicate the number of times that an alarm in an intent showed. A bigger circle indicates a higher number of alarms. You can hover over each of the circles to get the actual number of different types of intent. In addition, if you click any of the blue circles, USM Anywhere displays only the alarms corresponding to that circle. You can change the displayed period of time by clicking the Last 24 Hours filter.

Alarms graphed by intent are sorted into five different categories, which are represented by the graphic icons in the display:

- Delivery & Attack (💧)
- Environmental Awareness (🌐)
- Exploitation & Installation (.navigateByUrl)
- Reconnaissance & Probing (🔎)
- System Compromise (🪤)

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

Use the icon to change the alarms view, which is by default Alarms by Intent.

### Alarm Strategies By Intent

<table>
<thead>
<tr>
<th>Environmental Awareness</th>
<th>Reconnaissance &amp; Probing</th>
<th>Delivery &amp; Attack</th>
<th>Exploitation &amp; Installation</th>
<th>System Compromise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Access Control Modification (30)</td>
<td>Brute Force Permission Initialization (5)</td>
<td>Exploit Kit (34)</td>
<td>C&amp; C Communication (52)</td>
<td></td>
</tr>
<tr>
<td>Security Critical Infrastructure Update (64)</td>
<td></td>
<td></td>
<td></td>
<td>Malware Infection (7)</td>
</tr>
<tr>
<td>New User Creation (160)</td>
<td></td>
<td></td>
<td></td>
<td>Botnet Infection (6)</td>
</tr>
<tr>
<td>Access Control Modification (94)</td>
<td></td>
<td></td>
<td></td>
<td>C&amp; C Communication - Sinkhole (4)</td>
</tr>
<tr>
<td>Anomalous Access Failure (76)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Permission Modification (64)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomalous Infrastructure Update (25)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomalous User Behavior (14)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Alarms By Intent

- System Compromise
- Exploitation & Installation
- Delivery & Attack
- Reconnaissance & Probing
- Environmental Awareness
The icon accesses these options:

- **Alarms by Intent**: This view is a bubble graph that provides a graphical representation of alarms by intent.
- **Count / Time**: The Count/Time view is a graph that provides a graphical representation of the number of alarms in a period of time.

**Important**: The period of time is mapped with the `timestamp_occurred` field. This field can be overwritten by the current sensor UTC timestamp if, when processing events, a delay is detected up to 15 minutes or the `timestamp_occurred` field is not provided.

- **MITRE ATT&CK**: The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a framework for understanding attackers’ behaviors and actions.
- **Alarm Strategies by Intent**: This view is a table that provides a representation of alarms strategies by intent.

### The MITRE ATT&CK View

USM Anywhere and AT&T Alien Labs™ Open Threat Exchange® (OTX™) include MITRE ATT&CK information. The alarms view incorporates a table with tactics and techniques to describe adversarial actions and behaviors. Techniques are specific actions an attacker might take and tactics are phases of attacker behavior. This view includes the alarms mapping to their corresponding ATT&CK techniques and helps you to understand the context and the scope of an attack. See [MITRE ATT&CK](https://mitre-attack.github.io/attck/) for more information.

#### The MITRE ATT&CK Table

![MITRE ATT&CK Table](https://example.com/mitre-attck-table.png)

The(headers of the table are the 11 ATT&CK tactics, and each tactic has numerous techniques, which are the rows. The tooltips match the identification (ID) technique provided by MITRE ATT&CK. Some techniques display in several tactics. If you click in one of the techniques, the specific filters are added and the list shows the result.

#### USM Anywhere includes MITRE ATT&CK Dashboard to display MITRE ATT&CK information.
The Alarm Strategies by Intent view displays a table that lists the purposes of the alarm. The table headers represent the intent of the alarms. The table rows display the strategies.

### Environmental Awareness
- Network Access Control Modification (10)
- Security Critical Infrastructure Update (10)
- New User Creation (7)
- Access Control Modification (9)
- User Permission Modification (7)
- Anomalous Access Failure (6)
- Anomalous User Behavior (6)
- Anomalous Infrastructure Update (2)
- Suspicious Behavior (6)
- Publicly Accessible Resource (7)
- Anomalous User Activity (5)
- Anonymous Channel (3)
- Desktop Software - Bitcoin (2)
- Desktop Software - File Sharing (2)
- Network Anomaly - Protocol on Unexpected Port (2)
- Bulk Data Replication (1)
- Network Anomaly (1)
- Suspicious Security Critical Event (1)

### Environmental Awareness
- Brute Force Permission Enumeration (4)
- Web Server Attack - SQL Injection (3)
- Portscan (2)

### Reconnaissance & Probing
- Exploit Kit (49)
- Vulnerable Software Exploitation (7)
- Brute Force Authentication (35)
- Suspicious Download (15)
- Web Server Attack (7)
- Credential Abuse (17)
- Malware Infection (1)

### Delivery & Attack
- Exploit Kit (49)
- Vulnerable Software Exploitation (7)
- Brute Force Authentication (35)
- Suspicious Download (15)
- Web Server Attack (7)
- Credential Abuse (17)
- Malware Infection (1)

### Exploitation & Installation
- Malware Infection (44)
- C&C Communication (82)
- C&C Communication - Sinkhole (7)
- Botnet Infection (6)

### System Compromise

#### Alarms List Columns

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Summary</td>
<td>Displays several fields which are the type of attack, the method of attack, and how long the alarm happened in the past.</td>
</tr>
<tr>
<td>Priority</td>
<td>Impact of the detected attack. It can be Low, Medium, or High. See <a href="#">Priority Field for Alarms</a> for more information.</td>
</tr>
<tr>
<td>Alarm Status</td>
<td>Status applied to the alarm. By default, it can be Open, In Review, and Closed. See <a href="#">Alarm Status</a> for more information. The alarms that have the status &quot;Closed&quot; are not displayed in the list.</td>
</tr>
<tr>
<td>Sources</td>
<td>Hostname or IP address of the source, (including a national flag icon if the country is known) for an event creating the alarm.</td>
</tr>
</tbody>
</table>
List of the Default Columns in Alarms (Continued)

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destinations</td>
<td>Hostname or IP address of the destination, (including a national flag icon if the country is known) that received the events generating the alarm.</td>
</tr>
<tr>
<td>Source Users</td>
<td>Name of the user entity that was the source for an event creating the alarm.</td>
</tr>
<tr>
<td>Destination Users</td>
<td>Name of the user entity that was the destination of an event creating the alarm.</td>
</tr>
<tr>
<td>Investigations</td>
<td>Identification (ID) of the investigation associated to the alarm. See Adding an Alarm to an Investigation and USM Anywhere Investigations for more information.</td>
</tr>
<tr>
<td>Sensors</td>
<td>Sensor name associated with the alarm. The type of sensor is also displayed below the sensor name.</td>
</tr>
<tr>
<td>Labels</td>
<td>Labels applied to the alarm. By default, it can be In Progress, False Positive, Open, and Closed. You can create and manage labels. See Labeling the Alarms for more information.</td>
</tr>
</tbody>
</table>

From the list of alarms, you can click any individual alarm row to display more information on the selected alarm, including individual events that actually triggered the alarm. See Viewing Alarm Details for more information.

To select an alarm, select the checkbox to the left of the alarm. You can select all alarms at the same time by selecting the first checkbox in the column. These buttons display when you select an alarm:

- **Remove Alarm Labels**: This button displays if there are labels associated to any alarm. Use this button to remove a label or labels from an alarm. See Labeling the Alarms for more information.
- **Apply Labels**: You can add a label to an alarm, which enables you to have classified alarms. See Labeling the Alarms for more information.
- **Add To Investigation**: You can create an investigation for an alarm or associate an investigation to an alarm. See Adding an Alarm to an Investigation and USM Anywhere Investigations for more information.
- **Alarm Status**: You can add a status to an alarm. See Alarm Status for more information.

To distinguish between label and status, see Differences between Statuses and Labels.

The asset name includes a chevron icon that can be gray (_GRAY) if the asset is not in the system, or blue (_BLUE) if the asset has been added to the system.

Click the gray chevron icon (_GRAY) to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.
- **Find in event**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.
- **Look up in OTX**: This option searches the IP address of the source asset in the AT&T Cybersecurity Alien Labs Open Threat Exchange® (OTX™) page. See Using OTX in USM Anywhere for more information.
- **Add asset to system**: Use this option to create the asset in the system. See Adding Assets for more information.

Click the blue chevron icon (_BLUE) to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.
- **Find in events**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.
- **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.
- **Configure Asset**: See Editing Assets for more information.
Delete Asset: See Deleting the Assets for more information.

Assign Credentials: See Managing Credentials in USM Anywhere for more information.

Authenticated Scan: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Authenticated Asset Scans for more information.

Scan with AlienApp: This option enables you to run an asset scan through an AlienApp. See Running Asset Scans Using an AlienApp for more information.

Run Scan: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Asset Scans for more information.

Configuration Issues: This option opens the Asset Details page. The Configuration Issues tab is selected in the page. See Viewing Assets Details for more information.

Vulnerabilities: This option opens the Asset Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

Alarms: This option opens the Asset Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

Events: This option opens the Asset Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

You can configure the view you want for the list of alarms. See Alarms Views for more information.

Click Generate Report button to open the Configure Report dialog box. See Create Alarms Report for more information.

Click the ⏰ icon to change the graph to a Count/Time, MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) or Alarms Strategies by Intent view. See Alarms List View for more information.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

Click the ⤩ icon to filter your search by row fields. See Filtering Alarms by Row Fields for more information.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Configuring Columns on Alarms

You can configure the columns that are displayed in the list and save your columns configuration to get back to it whenever you need it.
To configure your columns

1. From the alarms list view, click the icon. The Manage Columns dialog box opens.

2. Search the columns you want to have in the list view. You can enter your search in the search field.

3. Use the and icons to pass the items from one column to the other and select the columns you want to see.

4. You can order the view of your selected columns by clicking one of them and dragging the column to the desired place.

5. Click Apply.

Note: If you export a report when you have set custom columns, your report keeps the columns you have configured.

Important: If you want to keep your configuration, you need to save it by selecting Save View > Save as. Otherwise, your custom view is not kept when you move to another feature. See Alarms Views for more information.

Priority Field for Alarms

In USM Anywhere, all alarms have a priority field, which indicates the importance of the alarm. This is a measurement to determine the impact of the alarm in our network.

The priority field can display the text Low, Medium, or High. This text comes from correlation and orchestration rules. When you create an orchestration rule, you have to enter a priority value between 0 and 100. AT&T Alien Labs™ creates the correlation rules and they already include a value. The Alien Labs team sets the value for the correlation rules depending on how critical the alarm is.

The displayed text on the column of alarms depends on the value that the rule has according to this table:
Priority Field for Alarms

<table>
<thead>
<tr>
<th>Displayed text</th>
<th>Value in the rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Between 0 and 33</td>
</tr>
<tr>
<td>Medium</td>
<td>Between 34 and 66</td>
</tr>
<tr>
<td>High</td>
<td>Between 67 and 100</td>
</tr>
</tbody>
</table>

Open the details of an alarm to learn the exact value of the priority level. See Viewing Alarm Details for more information. After you are in the alarm details page, hover over the priority text and a dialog box will show you the exact value.

See Correlation Rules and Orchestration Rules for more information.

Alarms Views

You can configure the view you want for the list of items in the page.

To create a view configuration:
1. From the Alarms list view, click the icon.
2. Use the and icons to pass the items from one column to another and select the columns you want to see.
3. Click Apply.
4. If you want to delimit the search, select the filters you want to apply.
5. Select Save View > Save as.
   The Save Current View dialog box opens.
6. Enter a name for the view.
7. Select **Share View** if you want to share your view with other users.
8. Click **Save**. The created view is already selected.

**To select a configured view**
1. From the Alarms list view, click **View** above the filters.
2. Click **Saved views** and select the view you want to see.

**Note:** A shared view includes the 🗝 icon next to its name.

3. Click **Apply**.

**To delete a configured view**
1. From the Alarms list view, click **View** above the filters.
2. Click **Saved views** and click the 🗝️ icon next to the saved view you want to delete.

A dialog box displays to confirm the deletion.

**Note:** You can delete the views you have created.

3. Click **Accept**.

**Important:** The 🗝️ icon does not display if the view is selected.

**Report Templates in Alarms**

USM Anywhere includes a wide range of report templates classified according to the compliance templates for alarms, vulnerabilities, and events collected in the system. The templates are combined into these two groups:
NIST CSF: The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

ISO 27001: ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).

To apply a report template
1. Go to Activity > Alarms.
2. From the Alarms list view, click View above the filters and select Report Templates.
3. Select a report.
   You can use the search field or scroll down the list.

4. Click Apply.
   The result displays with the filter applied.

USM Anywhere™ User Guide

USM Anywhere™ enables you to select an alarm or multiple alarms to add a label, an investigation, or a status to the selected alarms.
To select a single alarm

- Select the check-box to the left of the alarm.

<table>
<thead>
<tr>
<th>ALARM SUMMARY</th>
<th>PRIORITY</th>
<th>ALARM STATUS</th>
<th>SOURCES</th>
<th>DESTINATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>📣 Security Critical Infrastructure Update</td>
<td>Medium</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53 Bucket Access Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>📣 Suspicious Behavior</td>
<td>Medium</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3 block public access was disabled for an S3 bucket</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>📣 Vulnerability Scanning</td>
<td>Low</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulns</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To select multiple alarms

- Select the check-box of each alarm that you want to include.

<table>
<thead>
<tr>
<th>ALARM SUMMARY</th>
<th>PRIORITY</th>
<th>ALARM STATUS</th>
<th>SOURCES</th>
<th>DESTINATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>📣 Security Critical Infrastructure Update</td>
<td>Medium</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53 Bucket Access Changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>📣 Suspicious Behavior</td>
<td>Medium</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3 block public access was disabled for an S3 bucket</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>📣 Vulnerability Scanning</td>
<td>Low</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulns</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>📣 Vulnerability Scanning</td>
<td>Low</td>
<td>Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulns</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 hours ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To select all the alarms on the same page

- Select the check-box in the first column of the header row.
  
  You can apply labels to all the alarms on the page, or add them to an investigation, or change their alarm status.

To select all the alarms returned from a search or all the alarms in your environment

1. Select all the alarms on the page.

Text similar to the following example displays above the alarm table:

All 20 alarms on this page are selected. Select all 3572 related to this filter

Where
3572 is the number of alarms related to the selected filter in your environment.

2. To select all the alarms, click **Select all 3572 related to this filter**.

**Important**: Keep in mind that when you select all the alarms in your environment, the Alarms Status button is the only active button. This means that you cannot apply the same labels to all the alarms related to the filter, nor can you add all of them to an investigation.

**Searching Alarms**

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure filters** link located in the upper-left corner of the page. The management of filters is similar to that for assets. See **Managing Filters** for more information.

The following table lists the filters you see on the page.
## Filters Displayed by Default in the Main Alarms Page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Identify alarms triggered in the last hour, 24 hours, 7 days, 30 days, or 90 days. You can also configure your own period of time by clicking the <strong>Custom Range</strong> option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select <strong>AM</strong> or <strong>PM</strong>.</td>
</tr>
<tr>
<td>Open/In Review/Closed</td>
<td>Filter alarm by Alarm Status. See <a href="#">Alarm Status</a> for more information.</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Filter suppressed alarms. See <a href="#">Creating Suppression Rules from the Alarms Page</a> for more information.</td>
</tr>
<tr>
<td>Not Suppressed</td>
<td>Filter hiding suppressed alarms. The suppressed alarms are hidden by default.</td>
</tr>
<tr>
<td>Labels</td>
<td>Filter alarms by the applied labels. See <a href="#">Labeling the Alarms</a> for more information.</td>
</tr>
<tr>
<td>Intent</td>
<td>Filter alarms by the purpose of the alarm. It can be Delivery &amp; Attack, Environmental Awareness, Exploitation &amp; Installation, Reconnaissance &amp; Probing, and System Compromise. See <a href="#">Intent</a> for more information.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Filter alarms by the type of attack. See <a href="#">Strategy</a> for more information.</td>
</tr>
<tr>
<td>Method</td>
<td>If known, filter alarms by the method of attack or infiltration associated with the indicator that generated the alarm. See <a href="#">Method</a> for more information.</td>
</tr>
<tr>
<td>Sensors</td>
<td>Filter alarms by the associated USM Anywhere Sensor. See <a href="#">USM Anywhere Sensor Management</a> for more information.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>Filter alarms by asset group.</td>
</tr>
<tr>
<td>Priority</td>
<td>Filter alarms by low, medium, or high priority. See <a href="#">Priority Field for Alarms</a> for more information.</td>
</tr>
</tbody>
</table>

**Note:** Filtering large asset groups will only return data from the most recent 1024 assets. See [Creating An Asset Group](#) for more information about this limitation.

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

### Icons Next to the Filter Title

- **Sort the filters alphabetically.**
- **Sort the filters by the number of items that match them.**

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the **X** icon next to the filter. Or clear all filters by clicking **Reset**.
Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

Filtering Alarms by Row Fields

USM Anywhere includes a column with the icon in the Alarms List View page. Use this icon to add filters to your search. When you click this icon, a dialog box displays with the specific fields of that row.

To filter alarms by row fields:

1. Go to Activity > Alarms to open the Alarms List View page.
2. Click the icon of the row you want to add the filters to.

The Add Filters dialog box appears.
3. Select the fields that you want to filter during your search. Click **Equals** or **Not** to limit your search.

4. Click **Apply**.

   The result of your search displays with the filters applied.

**Searching Alarms by Using the Search Field**

Use the search field to enter queries and refine your search. You can enter free text, use wildcards, and use advanced search syntax. When searching, keep in mind the accepted query string syntax list in this table:
### Type of Query

<table>
<thead>
<tr>
<th>Type of Query</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard query with a blank space between terms</td>
<td>By default, a space between query terms is considered an implicit “OR”.</td>
<td>blacklist malicious</td>
</tr>
<tr>
<td>Literal, using double quotes</td>
<td>Matches entries that contain the same exact terms.</td>
<td>&quot;blacklist malicious&quot;</td>
</tr>
<tr>
<td><strong>Note:</strong> IP addresses and FQDNs are considered literal searches, so they don’t require quotation marks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boolean operators, using parentheses</td>
<td>They are AND, OR, and NOT. Parentheses can be used to group terms for precedence. Parentheses are also used to designate subsearches.</td>
<td>(http OR tcp) AND ftp</td>
</tr>
<tr>
<td>Wildcards, asterisk (*)</td>
<td>Matches any number of characters. Cannot be used at the beginning of a search query.</td>
<td>instance*</td>
</tr>
<tr>
<td>Wildcards, question mark (?)</td>
<td>Matches a single letter in a specific position. Cannot be used at the beginning of a search query.</td>
<td>qu?ck</td>
</tr>
<tr>
<td>Regexp, using /expression/</td>
<td>Regular expression inside forward slash characters. A dialog box opens to confirm the search.</td>
<td>/Describe.*Instances/</td>
</tr>
<tr>
<td><strong>Note:</strong> The characters &quot;, *, ?, (, and ) are special characters included in expressions. If you want to search by these characters, you need to manually escape them by preceding them with a backslash.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pulse:ID</td>
<td>Pulses are collections of IOCs. You need to insert the word pulse followed by a colon and the pulse</td>
<td>pulse:59432536c1970e343ce61bf0</td>
</tr>
</tbody>
</table>

Any characters may be used in a query, but certain characters are reserved and must be escaped. The reserved characters are these:

+ - = & > < ! { } \ ^ ~ : /

Use a backslash (for example, "\") to escape any reserved character (including a backslash).

### To search Alarms using the search field

1. Enter your query in the search field.
   
   If you want to search for a phrase containing two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").
   
   **Note:** Keep in mind that wildcard characters are considered as literals.

2. Click the icon.
The result of your search displays with the items identified.

**Searching Alarms by Using the Pulse ID**

You can use the search field to search alarms by pulse identification (ID). Pulses are collections of IOCs, reported by the AT&T Alien Labs™ Open Threat Exchange® OTX™ community, on which other community members review and comment. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IOCs, reported by the OTX community worldwide. See Open Threat Exchange® and USM Anywhere for more information.

To search alarms by using the pulse ID

1. Go to Activity > Alarms.
2. Enter your query in the Enter search field. Either paste the full URL or insert the word pulse followed by a colon and the pulse. For example, enter: `https://otx.alienvault.com/pulse/59432536c1970e343ce61bf0` or `pulse:59432536c1970e343ce61bf0`.
3. Click the icon.
4. The query submission dialog box opens.
USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

**Standard Mode**

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

**To activate the standard mode when the advanced mode is on**

1. Go to Activity > Alarms.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray.

**Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

**Advanced Mode**

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

**To activate the advanced mode**

1. Go to Activity > Alarms.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.

   This turns the icon green.

**To perform a search in the advanced mode**

1. Go to Activity > Alarms.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.

   This turns the icon green.

3. Click the filters that you want to select.

   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click **Apply Filters**. Or in the upper side of the page, click **Apply**.

   The result of your search displays.
To search using the NOT operator

1. Go to **Activity > Alarms**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not:

   **Important:** You have to select a filter to see this operator.

   **Note:** The selected filter displays the icon and the filter chiclet is labeled in red.

5. Click **Apply**.

To search all values of a filter

1. Go to **Activity > Alarms**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

   **Note:** This option searches all filters that are not empty. If the filter includes the [No Value], this value will not be checked not displayed. See Searching Alarms for more information.

About the No Value Option
The [No Value] option is a special value available for some filters. Use this value when you want to filter items that do not have the filter property defined or do not match the other defined property values in the filter. You can use the No Value option with other filter criteria and apply this value to an individual filter. (For example, you can use this filter for filtering alarms without labels.)

Viewing Alarm Details

The alarm details page provides in-depth information on an alarm, what caused it, and how to resolve the situation.
To view the details of an alarm

1. Go to **Activity > Alarms**.
2. Click the alarm to display a summary view, then click the alarm name to open the full details of the alarm.

Click the ⭐ icon to bookmark an item for quick access. Clicking the ⭐ icon on the secondary menu shows the bookmarked items and provides links to them.

Not all alarms found during monitoring are necessary in managing your environment because they do not pose a security threat. Frequently, these are alarms that create a noisy environment, making it difficult to monitor other alarms that require more attention. You can identify these alarms and suppress them by using a rule.

The alarms details page includes alarm management functions that are supported for your assigned user role:

- **Select Action**: See [Applying Actions to Alarms](#) for more information.
- **Create Rule**: See [Creating Rules from Alarms](#) for more information.

The alarm details include the main fields that identify an alarm. Keep in mind that you can edit or add values into these fields:
- **Status**: This field indicates the status for the alarm: open, in review, or closed. You can click the icon to edit the field and apply a status. See [Alarm Status](#) for more information.

- **Labels**: This field indicates if the alarm has been classified by using a label. You can click the icon to manage the labels of the alarm. See [Labeling the Alarms](#) for more information.

- **Investigation**: This field indicates if the alarm has been associated to an investigation. You can click the icon to edit the field and enter the title or the number that identifies each investigation. See [Adding an Alarm to an Investigation](#) for more information.

- **HTTP Hostname**: If the alarm includes this field, you can search for events by using it. See [Searching Events from the Details of an Alarm](#) for more information.

- **DNS RR Name**: If the alarm includes this field, you can search for events by using it. See [Searching Events from the Details of an Alarm](#) for more information.

Below the alarm details, you can see the source, the destination, the associated alarm if it exists, the associated events, a description, and, in the case of an alarm with a high priority, a recommendation to fix the problem.

The icon located next to the asset enables you to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See [Searching Alarms](#) for more information.

- **Find in events**: Use this option to execute a search of the asset name in the Events page. See [Events List View](#) for more information.

- **Look up in OTX**: This option searches the IP address of the source asset in the Open Threat Exchange page. See [Using OTX in USM Anywhere](#) for more information.

- **Add asset to system**: Use this option to create the asset in the system, see [Adding Assets](#) for more information.

**Note**: The value in the FQDN field comes from the event itself (raw log). This field can have a real FQDN, an IP address, or be empty.

3. In the upper right corner, click the previous and next buttons to navigate between items.
4. Click the icon to close the dialog box.

**Note**: See the [Searching Events from the Details of an Alarm](#) page for more information about the options in the HTTP Hostname, DNS RR Name, Source, and Destination fields.

### Applying Actions to Alarms

#### USM Anywhere™ User Guide

USM Anywhere enables you to respond to an alarm. Use this button to associate the item with an action. Depending on the USM Anywhere sensor you have installed, you will see different actions:

- **Get Forensics Information**: This option enables you to run pre-defined Linux and Windows scripts to get more info from the system. These scripts are already defined in USM Anywhere. The Basic, Moderate, and Full Forensic Info options get elemental, limited, and complete forensic information from assets. Keep in mind that the Full Forensic Info option will take more time for including all options. See [Scheduling a Forensics and Response Job](#) in the USM Anywhere AlienApps Guide for more information.

- **Scan (unauthenticated)**: You can launch an unauthenticated scan of an asset. See [Running Asset Scans](#) for more information.

- **Scan (authenticated)**: You can launch an authenticated scan of an asset. See [Performing Vulnerability Scans](#) for more information.
Creating Rules from Alarms

Role Availability

USM Anywhere enables you to create and manage your own orchestration rules from the alarms details page, which is the easiest way to configure an orchestration rule.

Warning: Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the Contains, Match and Match, case insensitive operators apply to future events and alarms, not to events and alarms received in the current day.

You can create these rules:

- **Suppression rule**: You can create a rule to suppress alarms that match a particular set of criteria. See Creating Suppression Rules from the Alarms Page and Suppression Rules from the Orchestration Rules Page for more information.
- **Notification rule**: You can create a notification rule according to a method. See Creating Notification Rules from the Alarms Page and Notification Rules from the Orchestration Rules Page.

Creating Suppression Rules from the Alarms Page

Role Availability

There are cases where the alarms in USM Anywhere are false positives, and you may want to suppress this kind of alarm to prevent those false positives from flooding your system. To suppress an alarm, you need to create a suppression rule. USM Anywhere applies the suppression rule to similar alarms from the current day (up to 10K alarms) and to future alarms. Therefore, existing alarms are suppressed but kept open, while future alarms are suppressed and closed.

Warning: Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the Contains, Match and Match, case insensitive operators apply to future events and alarms, not to events and alarms received in the current day.

To create a suppression rule from the Alarms page

1. Go to Activity > Alarms.
2. Locate the alarm that you want to include in the suppression rule.
   See Searching Alarms for more information.
3. Click the alarm that you want to suppress.
4. Click Create Rule > Create Event Suppression Rule or Create Rule > Create Alarm Suppression Rule.
5. You have already suggested property values to create a matching condition, but if you want to add new property values, click Add Condition.

Note: If the field is related to the name of a country, you should use the country code defined by the ISO 3166.
Note: The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

Important: Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.

Note: If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

6. (Optional.) Click Add Group to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click Next.

Important: A dialog box opens if there are warning messages. Click Cancel to review the warning messages, or click Accept to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.

10. Modify these two options:
   - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number
In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

1. Click **Save**.

   The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See Orchestration Rules for more information.

   **Important:** It takes a few minutes for an orchestration rule to become active.

   Suppressed alarms remain in the system but are hidden in the web user interface (UI) by default. If you want to see these alarms, click **Suppressed** in the Search & Filters area. The table displays suppressed alarms along with the other alarms. Use the following instructions if you want to display just the suppressed alarms.

   **To only display the suppressed alarms**
   
   1. Go to **Activity > Alarms**.
   2. In the Search & Filters area, click **Not Suppressed** to remove the **Suppressed: False** filter, and then click **Suppressed** to add the **Suppressed: True** filter.
   3. Click **Closed** to include the closed alarms.
   4. In the upper-left corner of the page, click the **Configure Filters** link to see alarms suppressed by a certain rule.
   5. In the Search filters field, enter **Suppress**.
   6. Select the **Suppress Rule Name** filter.
   7. Click the icon to pass the selected filter from the available filters to the selected ones.
   8. Click **Apply**.

     The page reloads, and the Suppress Rule Name filter is added at the lower-left corner.

     9. Search the Suppress Rule Name filter and click the rule.

     If no rule name displays, it is because the rules are not suppressing the alarms or the Suppressed filter is not enabled

     See **Search** for more information. You can click the icons below the filters.

     **Note:** You can save the view for later use. See **Alarms Views** for more information about how to create a configuration view.

**To show triggered Alerter Rules**

1. Go to **Settings > Rules > Orchestration Rules** to open the All Orchestration Rules page.
2. In the Create an Alarm row, click the icon.

   The **Alarms List View** page opens. The page includes Rules Name as a filter so that you can see how many alarms match the selected rule.

**Creating Notification Rules from the Alarms Page**
You can create your own notification rules from the Orchestration Rules page or the Alarms details page, which is the easiest way to configure the matching conditions.

To create a notification rule from the Alarms page

1. Go to Activity > Alarms.
2. Search the alarms that you want to include in the notification rule and click one of them.

   See Searching Alarms for more information.
4. You have already suggested property values to create a matching condition, but if you want to add new property values, click Add Condition.

   **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

   **Important:** Instead of using the `equals` and `equals`, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

   **Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

5. (Optional.) Click Add Group to group your conditions.

   **Note:** See Operators in the Orchestration Rules for more information.

   **Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

6. Click Next.
Important: A dialog box opens if there are warning messages. Click Cancel to review the warning messages, or click Accept to continue creating the rule.

7. Enter a name for the rule.
8. (Optional.) Enter a description for identifying this rule.
9. Select a notification method:

- **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the USM Anywhere Deployment Guide for more information.

- **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the USM Anywhere Deployment Guide for more information.

- **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

Note: The rolling 24-hour, 200-email limit refers to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

- **PagerDuty:** This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the USM Anywhere Deployment Guide for more information.

- **Slack:** This method makes use of a user-created Slack Webhook integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the USM Anywhere Deployment Guide for more information.

10. Modify these two options:

- **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences does not match within this timeframe, there is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule will trigger if five configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

11. Click Save.

The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.

Important: It takes a few minutes for an orchestration rule to become active.
Adding an Alarm to an Investigation

USM Anywhere enables you to associate alarms with an investigation.

**Important:** You can link up to 100 alarms to each investigation.

**To add an alarm to an investigation from the alarms main page**

1. Go to **Activity > Alarms**.
2. Search the alarm you want to associate the investigation. See **Searching Alarms** for more information.
3. Select the checkbox to the left of the alarm.
4. Click **Add To Investigation** and enter the title or the number that identifies the investigation.
5. Click **Save**.

**To add an alarm to an investigation from the alarms details page**

1. Go to **Activity > Alarms**.
2. Locate the alarm you want to add to the investigation. See **Searching Alarms** for more information.
3. In the **Investigation** field, click the **Collision** icon and enter the title or the number that identifies the investigation.
Note: Click Create New Investigation if you want to start a new investigation. See Creating a New Investigation for more information.

4. Click Save.

The connection has been done and you can see it from Investigations. See Evidence on Investigations for more information.

Searching Events from the Details of an Alarm

USM Anywhere enables you to search for events from the details of an alarm using the selected value as a filter in the search.

The HTTP Hostname or the DNS RR Name fields

All alarms that include the fields HTTP Hostname or the DNS RR Name give you the option of searching for events by using these fields. The alarm needs to include these fields.
To configure the HTTP Hostname or the DNS RR Name filters
1. Go to Activity > Alarms.
2. In the upper-left corner of the page, click the Configure Filters link.
3. In the search filters box, enter HTTP or DNS and select the desired filter.
4. Use the → and ← icons to pass the items from one column to the other.
5. Click Apply.
   The selected filters display.

To use the search pivot in the HTTP Hostname or the DNS RR Name fields
1. Go to Activity > Alarms.
2. Click an alarm that includes the fields HTTP Hostname or the DNS RR Name to see its details.
3. Click the ▼ icon located next to the asset name in one of these fields.
4. Choose a date range:
   - **Last 24 hours**: Run the search in the last 24 hours.
   - **Custom Range**: Customize a range and narrow it to delimit your search per minutes and seconds.

5. Click **Find in events** to display the events list page with the specific events.

**Searching for Events by Using the Source or Destination Fields**

USM Anywhere gives you the option of searching for events by using the Source or the Destination fields.

To search for events using the Source field:

1. Go to **Activity > Alarms**.
2. Click an alarm to see its details.
3. Click the icon next to the Source field.
4. Choose a date range:
   - **Last 24 hours**: Run the search in the last 24 hours.
   - **Custom Range**: Customize a range and narrow it to delimit your search per minutes and seconds.

5. Click one of these links:
   - **Find Source in Events**: Use this link to search events having the same source as the alarm.
   - **Find Source & Destination in Events**: Use this link to search events having the same source and destination as the alarm.

The result of your search displays with the filters applied.

**Labeling the Alarms**

USM Anywhere includes a set of labels to further classify your alarms. See [Searching Alarms](#) for more information.

You can't edit or delete the set of default labels:

- Closed
- False Positive
- In Progress
- Open

USM Anywhere enables you to create, edit, and delete your own labels. You can apply a label to one or more alarms. You can also apply multiple labels to the same alarm. To distinguish between labels and statuses, see [Differences between Statuses and Labels](#).

To label an alarm from the alarms main page

1. Go to **Activity > Alarms**.
2. Search for the alarm or alarms to which you want to apply a label. See [Searching Alarms](#), for more information.
3. Complete one of these options:
To label an alarm from the alarms page, follow these steps:

1. Go to Activity > Alarms.
2. Search for the alarm to which you want to apply a label. See Searching Alarms for more information.
3. Click the alarm.
4. Click Apply Labels and select a label.
5. Click Save.
To create a new label
1. Go to Activity > Alarms.
2. Select the checkbox to the left of an alarm. You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.
3. Click Apply Labels.
4. Click Manage Custom Labels.
5. Click Create New Label.
6. Enter a name for the label.
7. Click Save.

To edit a label
1. Go to Activity > Alarms.
2. Select the checkbox to the left of an alarm. You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.
3. Click Apply Labels.
4. Click Manage Custom Labels.
5. Click the icon next to the label you want to edit.
6. Modify the name of the label.
7. Click the icon to apply the changes.

To delete a label
1. Go to Activity > Alarms.
2. Select the checkbox to the left of an alarm. You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.
3. Click Apply Labels.
4. Click Manage Custom Labels.
5. Click the icon next to the label you want to delete.

6. Click **Delete** to confirm the deletion.

**To remove a label from an alarm**

1. Go to **Activity > Alarms**.
2. Do one of these options:
   - Select the checkbox to the left of an alarm. You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column. Then click **Remove Alarm Labels**, click the label, and click **Remove**.
   - Locate the alarm from which you want to remove the label, and click the icon next to the label.

**Alarm Status**

USM Anywhere includes a set of statuses, which you can use to classify your alarms, track alarm status, and search alarms using statuses as a filter. See **Searching Alarms** for more information on how to search alarms.

You can't edit or delete the set of default statuses:

- Open
- In Review
- Closed

USM Anywhere enables you to apply just one status to an alarm. You can't apply multiple statuses to the same alarm. See **Differences between Statuses and Labels** to distinguish between label and status.

**Note:** The alarms that have the "closed" status will not display in the Alarm list view.
To apply a status to an alarm from the alarms main page
1. Go to Activity > Alarms.
2. Search the alarm you want to apply a status. See Searching Alarms for more information.
3. Select the checkbox to the left of the alarm.
4. Click Alarm Status and select a status.
5. Click Apply.

To apply a status to an alarm from the alarms details page
1. Go to Activity > Alarms.
2. Search the alarm you want to apply a status. See Searching Alarms for more information.
3. Click the alarm.
4. In the Status field, click the icon to edit it.
5. Select a status and click the icon.

To bulk set the alarm status
1. Go to Activity > Alarms
2. Select all of the alarms to which you want to apply a status by selecting the checkbox to the left of an alarm. See Searching Alarms for more information. You can also select several of them or select all alarms at the same time by selecting the first checkbox in the column. You can also select all the alarms in the system. See Selecting Alarms in Alarm List View for more information.
3. Click Alarm Status and select a status.
4. Click Apply.

To search alarms having a status
1. Go to Activity > Alarms.
2. Click the filter to select the name of the status on the left pane.
   The alarm list displays the alarms that have the selected status.

Differences between Statuses and Labels
USM Anywhere includes several statuses and labels you can use to classify your alarms. A status is a property of the alarm and a label is a tag you can assign to an alarm.
These are the main differences:
• You can add all the labels you need to, but you are not allowed to create a new alarm status.
• You can apply a label to more than one alarm, but you are not able to apply more than one status to an alarm.
• Alarms that have the "Closed" status will not display in the Alarm list view.

Create Alarms Report
You can create a PDF or CSV report of the alarms directly from the alarms page.

⚠️ Important: AT&T Cybersecurity recommends Google Chrome as the preferred browser for generating reports.

To create an alarm report
1. Go to Activity > Alarms.
2. You can use filters to define the alarms content you want to display in your report. Or select the alarms you want to include in your report.
3. Click the Generate Report button to open the Configure Report dialog box.
   The filters selected and displayed for the page view are the ones that are populated in the report.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.

6. Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

7. Under the Format section, select either CSV or PDF for the format of the report.

8. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, or Monthly.

9. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

10. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

12. (Optional.) Add a description that will be included.

13. Under the Number of records section, choose the maximum number of records to include on the report. For CSV the options are 20, 50, 100, 500, 1000, or 50 K. For PDF the options are 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the + and the - icons.

15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.
Events Management

An event is a record of activity, which contains information and that resides in a log file. USM Anywhere collects, normalizes, and enriches logs with additional metadata, which are called events.

After USM Anywhere is installed in your environment, events start flowing through your system, so you can start gaining visibility into the type of events that are occurring, what natural or non-threatening activity is taking place, and what activity can be a possible attack.

This topic discusses these subtopics:

- Events List View
- Searching Events
- Viewing Event Details
- Create an Events Report
- Protecting Your Sensor's Performance with EPS Adaptive Response
- Raw Logs in Events
Events List View

USM Anywhere provides a centralized view of your events. Go to Activity > Events to see this centralized view.

The Events page displays information on events. These are the different parts of the Events page:

- On the left side of the page are the search and filters options. Use filters to delimit your search. See Searching Events for more information.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the events.
- The main part of the page is the list of events, where each row describes an individual event. Click an event to open a summary view. See Viewing Event Details for more information.

Your environment can display events when an asset has not received messages within a configured period of time. To see this kind of events, you previously need to configure a period of time that indicates when the asset has to start generating events. See Events Created When an Asset Stops Sending Data for more information.

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

The following table lists the fields you see on the page.

<table>
<thead>
<tr>
<th>Column / Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Time Created</td>
<td>The date and time of the creation of the event. The displayed date depends on your computer's time zone.</td>
</tr>
<tr>
<td>OTX</td>
<td>Indicate if it is an OTX event or not. If the icon displays active, click it to go to OTX.</td>
</tr>
<tr>
<td>Source Asset</td>
<td>Hostname or IP address of the host (with the national flag if the country is known) that initiates the event.</td>
</tr>
</tbody>
</table>

**Important:** If you want to create a rule, instead of using this field, use the Source Name or Source Asset ID fields.
List of the Default Columns in Events (Continued)

<table>
<thead>
<tr>
<th>Column / Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Asset</td>
<td>Hostname or IP address of the host (with the national flag if the country is known) that receives the event.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Name of the USM Anywhere Sensor detecting the event. The type of sensor is also displayed below the sensor name.</td>
</tr>
<tr>
<td>Username</td>
<td>Username associated with the event.</td>
</tr>
</tbody>
</table>

Important: If you want to create a rule, instead of using this field, use the Destination Name or Destination Asset ID fields.

The asset name includes the ▶ icon if the asset is not in the system, or the ▶ icon if the asset has been added to the system.

Click the ▶ icon to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events.
- **Look up in OTX**: This option searches the IP address of the source asset in the Open Threat Exchange page. See Using OTX in USM Anywhere
- **Add asset to system**: Use this option to create the asset in the system. See Adding Assets.

Click the ✔ icon to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.
- **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.
- **Configure Asset**: See Editing Assets for more information.
- **Delete Asset**: See Deleting the Assets for more information.
- **Assign Credentials**: See Managing Credentials in USM Anywhere for more information.
- **Authenticated Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Authenticated Asset Scans for more information.
- **Scan with AlienApp**: This option enables you to run an asset scan through an AlienApp. See Running Asset Scans Using an AlienApp for more information.
- **Run Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Asset Scans for more information.
• **Configuration Issues**: This option opens the Assets Details page. The Configuration Issues tab is selected in the page. See Viewing Assets Details for more information.

• **Vulnerabilities**: This option opens the Assets Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

• **Alarms**: This option opens the Assets Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

• **Events**: This option opens the Assets Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

You can configure the view you want for the list of events. See Event Views for more information.

Click **Generate Report** button to open the Configure Report dialog box. See Create an Events Report for more details.

The graph above the events list displays the amount of events in a period of time. You can change this period by clicking Last 24 Hours filter.

Click the 🔍 icon to access these options:

- **Actions / User**: Reports USM Anywhere account activity based on specific account users and summarized by Create, Read, Update, and Delete categories.

- **Count / Time**: The Count/Time view is a graph that provides a graphical representation of the number of events in a period of time.

  **Important**: The period of time is mapped with the timestamp_occurred field. This field can be overwritten by the current sensor UTC timestamp if, when processing events, a delay is detected up to 15 minutes or the timestamp_occurred field is not provided.

- **Auth / User**: Reports authorization actions.

- **Source Map**: Provides the number of events associated with each country on a global map.

Click the ⭐ icon to bookmark an item for quick access. Clicking the ⭐ icon on the secondary menu shows the bookmarked items and provides links to them.

Click the ♦️ icon to filter your search by row fields. See Filtering Events by Row Fields for more information.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

**Configuring Columns**

You can configure the columns and fields displayed in the list and save your columns configuration to get back to it whenever you need it.
To configure your columns

1. From the events list view, click the icon.

   The Manage Columns dialog box opens.

   ![Manage Columns dialog box](image)

   - **Available Columns**
     - Access Control Outcome
     - Access key id
     - Account Name
     - Account id
     - Account vendor
   - **Selected Columns**
     - Event Name
     - Time Created
     - Source Asset
     - OTX
     - Destination Asset
     - Source User

   ![Manage Columns dialog box](image)

2. Search the columns you want to have in the list view. You can enter your search in the search field.

3. Use the ➔ and ◀ icons to pass the items from one column to the other and select the columns you want to see.

4. You can order the view of your selected columns by clicking one of them and dragging the column to the desired place.

5. Click **Apply**.

   **Note:** If you export a report when you have set custom columns, your report keeps the columns you have configured.

   **Important:** If you want to keep your configuration, you need to save it by selecting **Save View > Save as**. Otherwise, your custom view is not kept when you move to another feature. See **Event Views** for more information.

Event Views
You can configure the view you want for the list of items in the page.

**To create a view configuration**

1. From the Events list view, click the icon.
2. Use the and icons to pass the items from one column to another and select the columns you want to see.
3. Click **Apply**.
4. If you want to delimit the search, select the filters you want to apply.
5. Select **Save View > Save as**.
   - The Save Current View dialog box opens.

   ![Save Current View](image)

   - Enter a name for the view.
   - Select **Share View** if you want to share your view with other users.
   - Click **Save**.
     - The created view is already selected.
To select a configured view

1. From the Events list view, click View above the filters.
2. Click Saved views and select the view you want to see.
   
   **Note:** A shared view includes the icon next to its name.

3. Click Apply.

To delete a configured view

1. From the Events list view, click View above the filters.
2. Click Saved views and click the icon next to the saved view you want to delete.
   
   A dialog box displays to confirm the deletion.

   **Note:** You can delete the views you have created.

3. Click Accept.

   **Important:** The icon does not display if the view is selected.

Predefined Views

USM Anywhere includes several predefined views of events based on usual environments and technologies. These views have pre-defined column headers that show the most relevant event fields. You can see a summarized event view without having to spend the time creating a custom view.

These predefined views operate the same way as the views you can create yourself. Some of these views have also predefined filters.
To open the predefined views

1. Go to Activity > Events.
2. Open the View option and select Saved Views.
3. Select a view and click Apply.

## Predefined Views for Events

<table>
<thead>
<tr>
<th>View</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlienVault Generic Plugin</td>
<td>Displays log data when the USM Anywhere Sensor is unable to match them with AlienApps based on hints and manual associations.</td>
</tr>
<tr>
<td>AWS Cloud Activity</td>
<td>Displays the most relevant event fields for AWS CloudTrail, AWS S3 Access, and ELB Access.</td>
</tr>
</tbody>
</table>
Predefined Views for Events (Continued)

<table>
<thead>
<tr>
<th>View</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Cloud Activity</td>
<td>Displays the most relevant event fields for Azure environmental logs.</td>
</tr>
<tr>
<td>Firewall Events</td>
<td>Displays the most relevant fields for firewall events. For instance request URL, source username, destination username, etc. depending on the set of fields that is most common to the list of supported firewall AlienApps.</td>
</tr>
<tr>
<td>Linux Events</td>
<td>Displays the most relevant fields for Linux Events generated by the Linux CRON, SSH, and SUDO AlienApps.</td>
</tr>
<tr>
<td>Network IDS</td>
<td>Displays the most relevant event fields for NIDS.</td>
</tr>
<tr>
<td>Open Threat Exchange</td>
<td>Displays the most relevant feeds that the pulse has matched.</td>
</tr>
<tr>
<td>Web Server Events</td>
<td>Displays the most relevant fields for Web Server Events, which include Apache, NGinx, and Windows IIS.</td>
</tr>
<tr>
<td>Windows Events</td>
<td>Displays the most relevant fields for Windows Events forwarded by NXLog.</td>
</tr>
</tbody>
</table>

Report Templates in Events

USM Anywhere includes a wide range of report templates classified according to the compliance templates for alarms, vulnerabilities, and events collected in the system. The templates are grouped into:

- **PCI**. Payment Card Industry Data Security Standards (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These reports are identified and based on specific PCI DSS requirements to provide the auditor with the specific information requested. For example, PCI DSS requirement 10.7.a: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.

- **NIST CSF**. The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

- **HIPAA**. The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. This includes covered entities, anyone who provides treatment, pay-
ment and operations in healthcare, and business associates, anyone with access to patient information and provides support in treatment, payment, or operations. Subcontractors, or business associates of business associates, must also be in compliance.

- **ISO 27001.** ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).


- **Data Sources.** You can find templates based on the most commonly used data sources including NIDS, AWS, Amazon DynamoDB, Amazon S3, AWS VPC Flow Logs, AWS Load Balancers, Azure, Cisco Umbrella, Cylance, FireEye, Fortigate, G Suite, McAfee ePO, Office 365, Okta, Palo Alto, SonicWall, Sophos UTM, Watchguard, VMware, Windows, AlienVault Agent. There is also a template for the AlienVault Generic Data Source.

**To apply a report template**

1. Go to **Activity > Events.**
2. From the Events list view, click **View** above the filters and select **Report templates.**
3. Select a report.
   
   You can use the search field or scroll down the list.
4. Click **Apply**.

The result displays with the filters applied.

**AlienVault Generic Data Source**
The AlienVault Generic Data Source is a predefined view of events which displays log data when the USM Anywhere Sensor is unable to match them with any AlienApps based on hints and manual associations.

This view works the same as the events list view. On the left you can find the search and filter options. In the upper side of the page, you can see any filters you have applied, and you have the option to create and select different views of the events. The main part of the page is the actual list of events. Each row describes an individual event.
If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

The following table lists the fields you see on the page.

### List of the Default Columns in the AlienVault Generic Data Source

<table>
<thead>
<tr>
<th>Column / Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Time Created</td>
<td>The date and time of the creation of the event. The displayed date depends on your computer’s time zone.</td>
</tr>
<tr>
<td>OTX</td>
<td>Indicate if it is an OTX event or not. If the icon displays as active, click it to go to OTX.</td>
</tr>
<tr>
<td>Reporting Device</td>
<td>The asset that sent the syslog.</td>
</tr>
<tr>
<td>Source Asset</td>
<td>Hostname or IP address of the host (with the national flag if the country is known) that initiates the event.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> If you want to create a rule, instead of using this field, use the Source Name or Source Asset ID fields.</td>
</tr>
<tr>
<td>Destination Asset</td>
<td>Hostname or IP address of the host (with the national flag if the country is known) that receives the event.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> If you want to create a rule, instead of using this field, use the Destination Name or Destination Asset ID fields.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Name of the USM Anywhere Sensor detecting the event. The type of sensor is also displayed below the sensor name.</td>
</tr>
<tr>
<td>Username</td>
<td>Username associated with the event.</td>
</tr>
</tbody>
</table>

The Reporting Device column includes the assets that sent the syslog. Next to the asset name of this column, click the icon to access these options:

- **Assign plugin:** See Adding AlienApps to an Asset for more information.
- **Full Details:** See Viewing Assets Details for more information.
- **Configure Asset:** See Editing Assets for more information.
- **Delete Asset:** See Deleting the Assets for more information.
- **Assign Credentials:** See Managing Credentials in USM Anywhere for more information.
- **Authenticated Scan:** This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Authenticated Asset Scans for more information.
• Scan with AlienApp: This option enables you to run an asset scan through an AlienApp. See Running Asset Scans Using an AlienApp for more information.

• Run Scan: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Asset Scans for more information.

• Configuration Issues: This option opens the Assets Details page. The Configuration Issues tab is selected in the page. See Viewing Assets Details for more information.

• Vulnerabilities: This option opens the Assets Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

• Alarms: This option opens the Assets Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

• Events: This option opens the Assets Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

Next to the source and destination asset name, click the ▼ icon to access these options:

• Add to current filter: Use this option to add the asset name as a search filter. See Searching Events.

• Look up in OTX: This option searches the IP address of the source asset in the Open Threat Exchange page. See Using OTX in USM Anywhere

• Add asset to system: Use this option to create the asset in the system. See Adding Assets.

You can configure the view you want for the list of events; see Views for more information.

Click Generate Report button to open the Configure Report dialog box. See Create an Events Report for more details.

The graph above the events list displays the amount of events in a period of time. You can change this period by clicking Last 24 Hours filter.

Click the  icon to access these options:

• Actions / User: Reports USM Anywhere account activity based on specific account users and summarized by Create, Read, Update, and Delete categories.

• Count / Time: Provides Reports USM Anywhere account activity based on specific account users and summarized by Create, Read, Update, and Delete categories.

• Auth / User: Reports authorization actions.

• Source Map: Provides the number of events associated with each country on a global map.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

Click the ⬇️ icon to filter your search by row fields. See Filtering Events by Row Fields for more information.
You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

**Configuring Columns**

You can configure the columns and fields displayed in the list and save your columns configuration to get back to it whenever you need it.

**To configure your columns**

1. From the AlienVault Generic Data Source list view, click the icon.

   The Manage Columns dialog box opens.

2. Search the columns you want to have in the list view. You can enter your search in the search field.

3. Use the and icons to pass the items from one column to the other and select the columns you want to see.

4. You can order the view of your selected columns by clicking one of them and dragging the column to the desired place.

5. Click **Apply**.

   **Note:** If you export a report when you have set custom columns, your report keeps the columns you have configured.
Important: If you want to keep your configuration, you need to save it by selecting Save View > Save as. Otherwise, your custom view is not kept when you move to another feature. See AlienVault Generic Data Source for more information.

Views

You can configure the view you want for the list of items in the page.

To create a view configuration

1. From the AlienVault Generic Plugin list view, click the icon.
2. Use the ➡️ and ◀️ icons to pass the items from one column to another and select the columns you want to see.
3. Click Apply.
4. If you want to delimit the search, select the filters you want to apply.
5. Select Save View > Save as.

   The Save Current View dialog box opens.

   ![Save Current View dialog box](image)

6. Enter a name for the view.
7. Select Share View if you want to share your view with other users.
8. Click Save.

   The created view is already selected.
To select a configured view

1. From the AlienVault Generic Plugin list view, click View above the filters.
2. Click Saved views and select the view you want to see.

   ![Note: A shared view includes the icon next to its name.]

3. Click Apply.

To delete a configured view

1. From the AlienVault Generic Plugin list view, click View above the filters.
2. Click Saved views and click the icon next to the saved view you want to delete.

   A dialog box displays to confirm the deletion.

   ![Note: You can delete the views you have created.]

3. Click Accept.

   ![Important: The icon does not display if the view is selected.]

Searching Events

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the Configure filters link located in the upper-left corner of the page. The management of filters is similar to that for assets. See Managing Filters for more information.
Filters displayed by default in the main Events page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Filter events triggered in the last hour, last 24 hours, last 7 days, last 30 days, or last 90 days. You can also configure your own period of time by clicking the <strong>Custom Range</strong> option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select <strong>AM</strong> or <strong>PM</strong>.</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Filter suppressed events. The suppressed events are hidden by default. See <a href="#">Creating Suppression Rules from the Events Page</a> for more information.</td>
</tr>
<tr>
<td>Account Name</td>
<td>Filter events by the account that has generated the event.</td>
</tr>
<tr>
<td>Data Source</td>
<td>Filter events by the data source used to normalize the event.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Filter events by the short, user-readable description of the event.</td>
</tr>
<tr>
<td>Source Asset</td>
<td>Filter events by the name of the asset that produced the event.</td>
</tr>
<tr>
<td>Source User</td>
<td>Filter events by the name of the user that produced the event.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Filter events by the name of the USM Anywhere Sensor that received the event.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>When the host for the event source or destination is an asset belonging to one or more of your asset groups, this field filters the asset group name or names.</td>
</tr>
<tr>
<td>Username</td>
<td>Filter events by the username associated with the asset that generated the event.</td>
</tr>
</tbody>
</table>

**Note:** Filtering large asset groups will only return data from the most recent 1024 assets. See [Creating An Asset Group](#) for more information about this limitation.

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

**Icons Next to the Filter Title**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="alpha" /></td>
<td>Sort the filters alphabetically.</td>
</tr>
<tr>
<td><img src="image" alt="alpha" /></td>
<td>Sort the filters by the number of items that match them.</td>
</tr>
</tbody>
</table>

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the **X** icon next to the filter. Or clear all filters by clicking **Reset**.
**Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.
About the Was Fuzzied Filter

When USM Anywhere receives raw log data on the USM Anywhere Sensor, it tries to match them with integrations based on hints and manual associations. Sometimes that process fails and events are processed by the AlienVault Generic Data Source, which attempts to find some common information using "fuzzy" matching. These events can be found by filtering by the data source integration or the "Was Fuzzied" fields.

**Important:** An event having the "Was Fuzzied" field with the value "true" has its data source property as "[empty]".

See The AlienVault Generic Data Source in the *USM Anywhere Deployment Guide* for more information about how this it attempts to normalize an unmatched log message.
To search events that are not matched with a specific data source

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the Configure Filters link.
3. Search the filter Was Fuzzied.
4. Click the ➔ icon to select the filter.
5. Click Apply.
6. In the left panel, search the Was Fuzzied integration.
7. Click true. The number between parentheses indicates the number of events that were created with the AlienVault Generic Data Source.

**Note:** The false value displays the events that have an assigned data source. The number between parentheses indicates the number of events.

Filtering Events by Row Fields

USM Anywhere includes a column with the 🔄 icon in the Events List View page. Use this icon to add filters to your search. When you click this icon, a dialog box displays with the specific fields of that row.

**To filter events by row fields**

1. Go to Activity > Events to open the Events List View page.
2. Click the 🔄 icon of the row you want to add the filters to.

   The Add Filters dialog box appears.
3. Select the fields that you want to filter during your search. Click **Equals** or **Not** to limit your search.

4. Click **Apply**.

   The result of your search displays with the filters applied.

**Searching Events by Using the Search Field**

Use the search field to enter queries and refine your search. You can enter free text, use wildcards, and use advanced search syntax. When searching, keep in mind the accepted query string syntax list in this table:
## Accepted Query String Syntax

<table>
<thead>
<tr>
<th>Type of Query</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard query with a blank space between terms</td>
<td>By default, a space between query terms is considered an implicit “OR”.</td>
<td>blacklist malicious</td>
</tr>
<tr>
<td>Literal, using double quotes</td>
<td>Matches entries that contain the same exact terms.</td>
<td>&quot;blacklist malicious&quot;</td>
</tr>
<tr>
<td><strong>Note</strong>: IP addresses and FQDNs are considered literal searches, so they don’t require quotation marks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boolean operators, using parentheses</td>
<td>They are AND, OR, and NOT. Parentheses can be used to group terms for precedence. Parentheses are also used to designate subsearches.</td>
<td>(http OR tcp) AND ftp</td>
</tr>
<tr>
<td>Wildcards, asterisk (*)</td>
<td>Matches any number of characters. Cannot be used at the beginning of a search query.</td>
<td>instance*</td>
</tr>
<tr>
<td>Wildcards, question mark (?)</td>
<td>Matches a single letter in a specific position. Cannot be used at the beginning of a search query.</td>
<td>qu?ck</td>
</tr>
<tr>
<td>Regexp, using /expression/</td>
<td>Regular expression inside forward slash characters. A dialog box opens to confirm the search.</td>
<td>/Describe.*Instances/</td>
</tr>
<tr>
<td><strong>Note</strong>: The characters &quot;, *, ?, (, and ) are special characters included in expressions. If you want to search by these characters, you need to manually escape them by preceding them with a backslash.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pulse:ID</td>
<td>Pulses are collections of IOCs. You need to insert the word pulse followed by a colon and the pulse</td>
<td>pulse:59432536c1970e343ce61bf0</td>
</tr>
</tbody>
</table>

Any characters may be used in a query, but certain characters are reserved and must be escaped. The reserved characters are these:

+ - = & | > < ! { } [] ^ " ~ : \ /

Use a backslash (for example, "\>") to escape any reserved character (including a backslash).
To search Events using the search field

1. Go to Activity > Events.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

**Important:** The indexed fields are Event Name, Raw Log, Rep Device Asset ID, Source Asset ID, and Destination Asset ID.

**Note:** Keep in mind that wildcard characters are considered as literals.

3. Click the icon.

The result of your search displays with the items identified.

**Example: Search for IP Addresses in a Network with Regex**

You can use regular expressions (regex) to broaden your search in a number of ways. See Using Regular Expressions in USM Anywhere for more information. One of the most common applications for regex in a search is to search for an IP address range in a network.

As an example, to search for hosts in the 25. network range, enter the following regex into the search field:

```
/25.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}/
```

Here is a more detailed anatomy of this example:

- `/ ... /`: The regex search is indicated by the expression contents being contained between forward slashes.
- `25.:` Indicates the network range being searched.
- `[0-9]`: This set of brackets in the expression is a variable number range.
• \{1,3\} The numbers in this set of braces indicates that the search will look for any pattern using the preceding number range a minimum 1 time, to a maximum 3 times.

• \[0-9\] \{1,3\} Because an IPv4 address consists of 4 sets of numbers, from 0-255, separated by periods, the \[0-9\] \{1,3\} part of this regular expression is used to include any possible number from that range.

**Note:** Because the search field does not search all fields in an event, the results will be limited to IP addresses in the Event Name, Raw Log, Rep Device Asset ID, Source Asset ID, and Destination Asset ID fields.

**Searching Events by Using the Pulse ID**

You can use the search field to search events by pulse identification (ID). Pulses are collections of IOCs, reported by the AT&T Alien Labs™ Open Threat Exchange® OTX™ community, on which other community members review and comment. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IOCs, reported by the OTX community worldwide. See Open Threat Exchange® and USM Anywhere for more information.

**To search events by using the pulse ID**

1. Go to Activity > Events.
2. Enter your query in the Enter search field. Either paste the full URL or insert the word **pulse** followed by a colon and the pulse. For example, enter: `https://otx.alienvault.com/pulse/59432536c1970e343ce61bf0` or `pulse:59432536c1970e343ce61bf0`.
3. Click the **Q** icon.
4. The query submission dialog box opens.

5. Click **Accept** to continue.

   The result of your search displays with the items identified. This result matches entries containing IOCs in your environment.

**Standard and Advanced Modes on Events**

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

USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

**Standard Mode**

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.
To activate the standard mode when the advanced mode is on

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the ✗ icon.
3. This turns the icon gray, ✗.

**Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

**Advanced Mode**

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

**To activate the advanced mode**

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the ✗ icon to activate the advanced mode.
   
   This turns the icon green, ✔.

**To perform a search in the advanced mode**

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the ✗ icon to activate the advanced mode.
   
   This turns the icon green, ✔.
3. Click the filters that you want to select.
   
   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click **Apply Filters**. Or in the upper side of the page, click **Apply**.

   ![Apply Filters](image)

   The result of your search displays.
To search using the NOT operator

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the \(\boxed{\times}\) icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.

**Important:** You have to select a filter to see this operator.

**Note:** The selected filter displays the \(\boxed{\times}\) icon and the filter chiclet is labeled in red.

5. Click Apply.

To search all values of a filter

1. Go to Activity > Events.
2. In the upper-left corner of the page, click the \(\boxed{\times}\) icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.
About the No Value Option

The [No Value] option is a special value available for some filters. Use this value when you want to filter items that do not have the filter property defined or do not match the other defined property values in the filter. You can use the No Value option with other filter criteria and apply this value to an individual filter. (For example, you can use this filter for filtering events without an associated account name.)
In the Data Source filter, the equivalent of No Value is [AlienVault Generic Data Source]. If you select this option, it means you are searching for events that do not have a specific data source. See The AlienVault Generic Data Source for more information.

In the Packet Payload filter, the equivalent of No Value is [No Parsable Value]. The Packet Payload field stores the Base64 encoded payload associated with the network-based intrusion detection system (NIDS) events. Due to the size limit of the underlying technology, the maximum length USM Anywhere can parse is 32766 B. When the payload exceeds this limit, USM Anywhere stores the data in this field unparsed. The No Parsable Value option includes two types of events: events with no data and events with data exceeding 32766 B. Both events are not parsable. Therefore, sometimes you may see events with payload data when you select the No Parsable Value option in the Packet Payload filter, similar to the following screenshot.
Viewing Event Details

The event details page provides in-depth information on events.
To view the details of an event

1. Go to Activity > Events.
2. Click the event to display a summary view, then click the event name to open the full details of the event.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

The Event Details page includes event management functions that are supported for your assigned user role:
- **Select Action**: See *Applying Actions to Events* for more information.
- **Create Rule**: See *Creating Rules from Events* for more information.
- **Generate Report**: This option displays if you have opened the full details of the event. See *Create an Events Report* for more information.

The event details include the main fields that identify an event. Keep in mind that you can edit or add values into this field:

- **Investigation**: This field indicates if the event has been associated to an investigation. You can click the pencil icon to edit the field and enter the title or the number that identifies each investigation. See *Adding an Event to an Investigation* for more information.

You can see the event details, then the source, the destination, the source and destination users, the payload, and the log. The checkmark icon located next to the Source, Destination, and two User fields enables you to access to several options. See *Events List View* for more information about those options.

In addition, you have these three options:

- **Add to current filter**: This option enables you to add the asset to the selected filters.
- **Look up in OTX**: This option searches the IP address of the source asset in the AT&T Cybersecurity Open Threat Exchange (OTX™) page. See *Using OTX in USM Anywhere* for more information.
- **Add asset to system**: Use this option to create the asset, see *Adding Assets* for more information.

**Note**: The value in the FQDN field comes from the event itself (raw log). This field can have a real FQDN, an IP address, or be empty.

3. In the upper right corner, click the **previous** and **next** buttons to navigate between items.
4. Click the **×** icon to close the dialog box.

### Applying Actions to Events

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

USM Anywhere enables you to respond to the event. Use this button to associate the item with an action. Depending on the USM Anywhere Sensor you have installed, you will see different actions:

- **Get Forensics Information**: This option enables you to run pre-defined Linux and Windows scripts to get more info from the system. These scripts are already defined in USM Anywhere. The Basic, Moderate, and Full Forensic Info options get elemental, limited, and complete
forensic information from assets. Keep in mind that the Full Forensic Info option will take more time for including all options. See Scheduling a Forensics and Response Job in the USM Anywhere AlienApps Guide for more information.

- **Scan (unauthenticated):** You can launch an unauthenticated scan of an asset. See Running Asset Scans for more information.

- **Report Domain:** See AlienApp for Cisco Umbrella Actions in the USM Anywhere AlienApps Guide for more information.

- **Agent Query:** You can run an agent query in response to any event. See for more information.

### Creating Rules from Events

USM Anywhere enables you to create and manage your own orchestration rules from the Events details pages, which is the easiest way to configure an orchestration rule.

**Warning:** Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the **Contains, Match and Match, case insensitive** operators apply to future events and alarms, not to events and alarms received in the current day.

You can create these rules:

- **Suppression rule:** See Creating Suppression Rules from the Events Page and Suppression Rules from the Orchestration Rules Page for more information.

- **Filtering Rule:** See Creating Filtering Rules from the Events Page and Filtering Rules from the Orchestration Rules Page for more information.

**Important:** The Create Filtering Rule option is not visible if the Agent has sent the event.

- **Alarm rule:** See Creating Alarm Rules from the Events Page and Correlation Rules for more information.

- **Notification rule:** See Creating Notification Rules from the Events Page and Correlation Rules for more information.

### Creating Suppression Rules from the Events Page
You can create suppression rules from the Events page to prevent some events from flooding your system.

USM Anywhere saves the events that match a suppression rule, but does not correlate these suppressed events. By default, USM Anywhere hides these suppressed events. If you want to see these events, click Suppressed in the Search & Filters area. The table displays suppressed events along with all events. See To only display the suppressed events if you want to display just the suppressed events.

**Warning:** Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the Contains, Match and Match, case insensitive operators apply to future events and alarms, not to events and alarms received in the current day.

You can create your own rules from the Suppression Rules page or the Events details page, which is the easiest way to configure the matching conditions.

**To create a Suppression Rule from the Events page**

1. Go to **Activity > Events**.
2. Search the events which you want to include in the suppression rule.
   
   See **Searching Events** for more information.
3. Click the event to suppress.
4. Select **Create Rule > Create Suppression Rule**.
5. You have already suggested property values to create a matching condition. If you want to add new property values, click **Add Condition**.

**Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

**Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

**Important:** Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.
Note: If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

6. (Optional.) Click Add Group to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click Next.

Important: A dialog box opens if there are warning messages. Click Cancel to review the warning messages, or click Accept to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.

10. Modify these two options:

   • **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
• **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

11. Click **Save**.

12. The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

   **Important:** It takes a few minutes for an orchestration rule to become active.

**To only display the suppressed events**

1. Go to **Activity > Events**.

2. In the Search & Filters area, click **Not Suppressed** to remove the **Suppressed: False** filter, and then click **Suppressed** to add the **Suppressed: True** filter.

3. In the upper-left corner of the page, click the **Configure Filters** link to see events suppressed by a certain rule.

4. In the Search filters field, enter **Suppress**.

5. Select the **Suppress Rule Name** filter.

6. Click the ➔ icon to pass the selected filter from the available filters to the selected ones.

7. Click **Apply**.

   The page reloads, and the Suppress Rule Name filter is added at the lower-left corner.

8. Search the Suppress Rule Name filter and click the rule.

   If no rule name displays, it is because the rules are not suppressing the events or the Suppress filter is not enabled

   See **Searching Events** for more information about the icons below the filters.
**Note:** You can save the view for later use. See Event Views for more information about how to create a configuration view.

**To show triggered suppressed events**

1. Go to Settings > Rules to open the All Orchestration Rules page.
2. In the Event Suppression row, click the icon.

   The Events List View page opens. The page includes Rules Name as a filter so that you can see how many events match the selected rule.

**Creating Filtering Rules from the Events Page**

USM Anywhere enables you to make the sensor drops future events that match the rule. These events will be neither correlated nor stored. Through these rules, you can define which event data you are going to store in USM Anywhere. You will pay for the data you use.

**Note:** Filtering rules is not retroactive. The rule applies to future items, but not to to previous items, even if those items follow the rule.

**Important:** You can’t use a correlation list when you create a filtering rule.

**To create a filtering rule from the Events page**

1. Go to Activity > Events.
2. Search the events which you want to include in the filtering rule.
   
   See Searching Events for more information.
3. Click one of them.
4. Select Create Rule > Create Filtering Rule.
5. You have already suggested property values to create a matching condition. If you want to add new property values, click Add Condition.

   **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.


Important: Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.

Note: If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

6. (Optional.) Click **Add Group** to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click **Next**.

![Warning dialog box]

Important: A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.

10. Click **Save**.

The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.
Important: It takes a few minutes for an orchestration rule to become active.

Creating Alarm Rules from the Events Page

USM Anywhere enables you to easily identify existing and emerging threats, which are of interest. Through alarm rules on events, you can organize your threats and only see high-priority alarms, which can be received in an email and will help you to reduce noise and focus on important things.

To create an alarm rule from the Events page

1. Go to Activity > Events.
2. Search the events which you want to include in the alarm rule.
   - See Searching Events for more information.
3. Click one of them.
4. Select Create Rule > Create Alarm Rule.
5. Select a packet type in the Match drop-down list. The first match criteria for all rules must be the packet_type detail field:
   - **Logs**: Use this packet type for event-based rules.
   - **Warnings**: Use this packet type for configuration issues-based rules.
   - **Vulnerabilities**: Use this packet type for vulnerabilities-based rules.

---

1 This packet type refers to configuration issues that are used to identify incorrect uses of certain features. For example, the app for AWS assesses your configuration of AWS to identify insecure use of the AWS security features.
6. You have already suggested property values to create a matching condition. If you want to add new property values, click **Add Condition**.

**Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

**Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

**Important:** Instead of using the `equals` and `equals, case insensitive` operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

**Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See **Determining the Mapping of a Field** for more information.

7. (Optional.) Click **Add Group** to group your conditions.

**Note:** See **Operators in the Orchestration Rules** for more information.

**Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

8. Click **Next**.

![Warning message](image-url)
9. Enter a name for the rule and, if desired, a description to clarify its use in the Description field.

10. Select an intent.

   The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See Intent for more information about the available threat categories.

11. Enter a method.

   If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.

   Note: This is a required field; if you do not complete this field, the Save button remains inactive.

12. Select a strategy.

   The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.

13. Enter a priority.

   See Priority Field for Alarms for more information.

14. Configure a mute value.

   Once an alarm is created, you can set the time that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

15. Modify these two options:

   - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

   - **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.
In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

16. (Optional.) Select the fields that you want to display in the generated alarm.

You can select or remove the fields you want to include in the details of the alarm. A field passes from one column to the other by clicking it.

17. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### Creating Notification Rules from the Events Page

You can create your own notification rules from the **Orchestration Rules** page or from the Events details page, which are the easiest ways to configure the matching conditions.

**To create a Notification Rule from the Events page**

1. Go to **Activity > Events**.
2. Search the events that you want to include in the notification rule. See **Searching Events** for more information.
3. Click one of them.
4. Select **Create Rule > Create Notification Rule**.
5. You have already suggested property values to create a matching condition. If you want to add new property values, click **Add Condition**.

**Note:** If the field is related to the name of a country, you should use the country code defined by the **ISO 3166**.
**Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

**Important:** Instead of using the `equals` and `equals`, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

**Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See [Determining the Mapping of a Field](#) for more information.

6. (Optional.) Click **Add Group** to group your conditions.

**Note:** See [Operators in the Orchestration Rules](#) for more information.

**Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click **Next**.

**Important:** A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.
10. Select a notification method:

- **Amazon SNS**: This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the **first 1,000 email notifications per month to fall into the free messaging tier**. See Sending Notifications Through Amazon SNS in the [USM Anywhere Deployment Guide](#) for more information.

- **Datadog**: This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the [USM Anywhere Deployment Guide](#) for more information.

- **Email**: This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is **limited to a maximum of 200 emails per rolling 24-hour period**. The only user-customizable information available is the email subject line.

  **Note**: The rolling 24-hour, 200-email limit refers to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

- **PagerDuty**: This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the [USM Anywhere Deployment Guide](#) for more information.

- **Slack**: This method makes use of a user-created Slack *Webhook* integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the [USM Anywhere Deployment Guide](#) for more information.

11. Modify these two options:

- **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

  This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.
In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

12. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

## Adding an Event to an Investigation

USM Anywhere enables you to associate events with an investigation.

**Important:** You can link up to 100 events to each investigation.

### To add an event to an investigation from the events details page

1. Go to **Activity > Event**.
2. Locate the event you want to add to the investigation. See **Searching Events** for more information.
3. In the **Investigation** field, click the icon to edit it and enter the title or the number that identifies the investigation.

**Note:** Click **Create New Investigation** if you want to start a new investigation. See **Creating a New Investigation** for more information.

4. Click **Save**.

The connection has been done and you can see it from **Investigations**. See **Evidence on Investigations** for more information.

## Create an Events Report
You can create a PDF or CSV report of the events directly from the events page.

**Important:** AT&T Cybersecurity recommends Google Chrome as the preferred browser for generating reports.

**To create an events report**

1. Go to Activity > Events.
2. You can use filters to define the events content you want to display in your report.

3. Click the Generate Report button to open the Configure Report dialog box.

   The filters selected and displayed for the page view are the ones that are populated in the report.

4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

5. Click the date field if you want to choose a different date range.

   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

   **Note:** This option is not available when generating reports for assets or asset groups.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, or Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

12. (Optional.) Add a description that will be included.

13. Under the Number of records section, choose the maximum number of records to include on the report. For CSV the options are 20, 50, 100, 500, 1000, or 50 K. For PDF the options are 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the⬅ icons.

15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.

Protecting Your Sensor's Performance with EPS Adaptive Response

To protect the health of your system, USM Anywhere monitors the rate of events being sent to your sensor. If that rate, measured in events per second (EPS), threatens to impact your sensor's capacity USM Anywhere will engage EPS Adaptive Response. EPS Adaptive Response enables your system to take more time to process events coming in by throttling your EPS, keeping your system running without risking event loss.

**Note:** See Reaching the Monthly Usage Limit to read more about sensor capacity and USM Anywhere tier limits.

EPS Adaptive Response may cause delays in the correlation of alarms. While activated, events will enter an adaptive processing queue on sensors or the agent pipeline to assist product stability. When deactivated, the queue will be processed at normal speeds. USM Anywhere views events in the user interface (UI) based on the time the actual event occurred and not the time the event was received by the sensor. When EPS Adaptive Response is ended and queued events get forwarded, they will be backfilled into the appropriate timeslots.

**Important:** After EPS Adaptive Response has ended, alarms may be delayed while throttled events are being forwarded.

EPS Adaptive Response Scenarios

There are two scenarios in which EPS Adaptive Response may be engaged:
- **Your sensor's disk space is almost full**: When your sensor's disk space approaches full, throttling engages to preserve remaining disk space. This is enabled for all customers.

- **Your USM Anywhere is projected over tier**: When your USM Anywhere is projected to be over tier, throttling slows down the event ingestion in both sensors and agents until you are back within your tier limits. This is only enabled for heavy usage customers.

  **Note**: Every time EPS Adaptive Response is engaged or disengaged, your USM Anywhere sensor will create a system event. In addition, a system event is created when throttling rates change.

  You may also create custom events around throttling to best suit your environment's needs.

**Sensor Disk Space**

If your sensor's disk volume ever filled up completely, the sensor would stop being able to process events. To prevent this, EPS Adaptive Response slows down your sensor's EPS, giving your system time to process events coming in. As your disk partition continues to fill, the rate of EPS throttling will increase to preserve what remains of your disk space and your sensor's operations. The following table summarizes the throttling rates based on your sensor usage.

**Throttling Rates per Percentage of Sensor Disk Used**

<table>
<thead>
<tr>
<th>Disk Use (%)</th>
<th>Sensor Throttling (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>0.25</td>
</tr>
<tr>
<td>90</td>
<td>0.5</td>
</tr>
<tr>
<td>92</td>
<td>2</td>
</tr>
<tr>
<td>95</td>
<td>5</td>
</tr>
<tr>
<td>98</td>
<td>10</td>
</tr>
<tr>
<td>99</td>
<td>100</td>
</tr>
</tbody>
</table>

**Over Tier Projection**

When your USM Anywhere is projected to go over tier, meaning either 5% over your allotment or over 50GB in total, it will analyze the rate of traffic coming through the sensor and agent data pipeline. Then it will engage EPS Adaptive Response to slow down your data rate and keep your USM Anywhere operational until data ingestion is decreased, or your tier is upgraded.

If you have more than one sensor or agent, USM Anywhere will begin by throttling only the sensor with the highest EPS. This is determined by retrieving your system's EPS per minute for every sensor and maintaining a rolling EPS average. Every hour, your system determines if throttling is necessary, and EPS Adaptive Response will be engaged on any sensor sending more EPS than 75% of this average.
When your USM Anywhere is projected to go over tier, EPS throttling is progressive, starting at 1 ms and increasing up to 250 ms as necessary until data ingestion decreases or your tier changes. Once throttling has been engaged, the projection will be sampled regularly. If the tier decrement is smaller than 2%, then the throttling factor is doubled. Otherwise, it remains the same until throttling is no longer necessary.

**EPS Adaptive Response System Events**

Every time the event throttling value changes in a sensor, a new system event is generated. There are two system event types:

- **EPS throttling has been engaged**: Your sensor’s EPS is being throttled.
- **EPS throttling has ended**: Your sensor’s EPS is no longer being throttled.

Each throttling system event type has a number of possible event keys, specifying which type of event has been triggered.

**EPS Throttling System Events and Their Meanings**

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Key</th>
<th>Event Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor is being throttled</td>
<td>event_action</td>
<td>SENSOR_THROTTLING</td>
</tr>
<tr>
<td></td>
<td>event_name</td>
<td>Sensor is being throttled</td>
</tr>
<tr>
<td></td>
<td>sensor_uuid</td>
<td>Sensor ID</td>
</tr>
<tr>
<td></td>
<td>customheader_0</td>
<td>Throttling value</td>
</tr>
<tr>
<td></td>
<td>customfield_0</td>
<td>Throttling value in milliseconds</td>
</tr>
<tr>
<td>Sensor throttling is over</td>
<td>event_action</td>
<td>SENSOR_THROTTLING</td>
</tr>
<tr>
<td></td>
<td>event_name</td>
<td>Sensor throttling is over</td>
</tr>
<tr>
<td></td>
<td>sensor_uuid</td>
<td>Sensor ID</td>
</tr>
<tr>
<td></td>
<td>customheader_0</td>
<td>Throttling value</td>
</tr>
<tr>
<td></td>
<td>customfield_0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Raw Logs in Events**
USM Anywhere archives raw event data as logs. Raw logs are an invaluable asset for forensic analysis and compliance mandates. You can download raw logs for review and find details about specific incidents, search the logs for instances using a specific IP address, or analyze the patterns of multiple attacks.

USM Anywhere enables you to configure the Raw Log column when viewing events or download raw logs from events.

To add the Raw Log column when viewing events

1. From the Events List view, click the icon to open the Columns Configuration dialog box.
2. Enter raw in the search field of the available columns.
3. Use the icon to pass the Raw Log column from one side to the other.
4. Click Apply.

**Note:** If you want to keep your configuration, you need to save it by selecting **Save View > Save as.** Otherwise, your custom view will not be kept when you move to another page.

To download Raw Logs

1. Go to Activity > Events.
2. Search or use filters to limit the events if needed.
3. In the upper right corner of the page, click Generate Report to open the Create Report dialog box.
4. Click the Download Raw Logs tab.

5. Choose a date range. You can select a predefined range between Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, or Last 90 Days or Custom Range to set a particular date range.
6. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

7. Click Download Logs.
System Events Management

An event is a record of activity, which contains information and that resides in a log file. USM Anywhere collects, normalizes, and enriches logs with additional metadata, which are called events.

USM Anywhere enables you to display system events. These events are any events generated within your environment. They are not actions associated with any of the monitored assets or networks collected by your environment. For instance, the system generates a system event when an asset, a user, or a node is created, updated, or deleted or when you modify your MFA subscription.

This topic discusses these subtopics:

- USM Anywhere System Events List View
- Searching System Events
- Viewing System Event Details
- Regular Events and System Events
USM Anywhere provides a centralized view of your system events. Go to Settings > System Events to see this centralized view.

The system events page displays information on any events generated within your environment. On the left you can find the search and filters options. In the upper side of the page, you can see any filters you have applied, and you have the option to create and select different views of the system events. The main part of the page is the actual list of system events. Each row describes an individual system event.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the \( \times \) icon to hide the filter pane. Click the \( \downarrow \) icon to expand the filter pane.

**Note:** System events older than 30 days are cleared from hot storage on a regular basis.

**List of the default columns in Events**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Time Created</td>
<td>The date and time of the creation of the event. The displayed date depends on your computer's time zone.</td>
</tr>
<tr>
<td>Source User Email</td>
<td>Email of the user that performed the action. For example, when user <a href="mailto:email@alienvault.com">email@alienvault.com</a> logs in, the source email is <a href="mailto:email@alienvault.com">email@alienvault.com</a>.</td>
</tr>
<tr>
<td>Destination User Email</td>
<td>Email of the user that the action is being performed on. For example, if user <a href="mailto:email@alienvault.com">email@alienvault.com</a> modifies or creates user <a href="mailto:new@alienvault.com">new@alienvault.com</a>, then the destination email is <a href="mailto:new@alienvault.com">new@alienvault.com</a>.</td>
</tr>
<tr>
<td>Event Outcome</td>
<td>Indicates if the action was success and completed or if it failed.</td>
</tr>
<tr>
<td>Event Change</td>
<td>It is a small description of what was changed in the system event. It only gets populated for certain actions and indicates what is being changed. Most of these are user changes. For example, when a user is suspended, locked status is reset, MFA is enabled/disabled, or password updated</td>
</tr>
<tr>
<td>Identity Source Address</td>
<td>IP address of the event or computer that it takes place on.</td>
</tr>
</tbody>
</table>

Click the \( \star \) icon to bookmark an item or filter result. Clicking the \( \star \) icon on the secondary menu shows the bookmarked items and provides links to them.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

**Views**

USM Anywhere enables you to define and save a custom System Events view to have your own selected filters.

You can configure the view you want for the list of items in the page.
To create a view configuration

1. Go to **Settings > System Events**.
2. If you want to delimit the search, select the filters you want to apply.
3. Select **Save View > Save as**.
   
   The Save Current View dialog box opens.

   ![Save Current View dialog box](image)

   **Save Current View**

   Save a view of the current filters and table columns. Saved views can be exported as reports.

   **View Name**

   MyView

   [ ] Share View

   [ ] Save

   [ ] Cancel

4. Enter a name for the view.
5. Select **Share View** if you want to share your view with other users.
6. Click **Save**.
   
   The created view is already selected.

To select a configured view

1. From the System Events list view, click **View** above the filters.
2. Click **Saved views** and select the view you want to see.

   ![System Events view](image)

   **Note:** A shared view includes the ![icon] next to its name.

3. Click **Apply**.

To delete a configured view

1. From the System Events list view, click **View** above the filters.
2. Click **Saved views** and click the ![icon] icon next to the saved view you want to delete.
   
   ![Dialog box](image)

   **Dialog box**

   A dialog box displays to confirm the deletion.

   ![Dialog box](image)

   **Note:** You can delete the views you have created.

3. Click **Accept**.

   ![Important](image)

   **Important:** The ![icon] icon does not display if the view is selected.
Searching System Events

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure filters** link located in the upper-left corner of the page. The management of filters is similar to that for assets. See [Managing Filters](#) for more information.

The following table lists the filters you see on the page.

### Filters Displayed by Default in the Main System Events Page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Filter system events triggered in the last hour, last 24 hours, last 7 days, last 30 days, or last 90 days. You can also configure your own period of time by clicking the <strong>Custom Range</strong> option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select <strong>AM</strong> or <strong>PM</strong>.</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Filter suppressed system events.</td>
</tr>
<tr>
<td>Not Suppressed</td>
<td>Filter hiding suppressed system events. The suppressed system events are hidden by default.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Filter system events by the short, user-readable description of the system event.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Filter system events by the associated USM Anywhere sensor.</td>
</tr>
<tr>
<td>Source User Email</td>
<td>Filter system events by the email of the user that performed the action. For example, when user <a href="mailto:email@alienvault.com">email@alienvault.com</a> logs in, the source email is <a href="mailto:email@alienvault.com">email@alienvault.com</a>.</td>
</tr>
<tr>
<td>Destination User Email</td>
<td>Filter system events by the email of the user that the action is being performed on. For example, if user <a href="mailto:email@alienvault.com">email@alienvault.com</a> modifies or creates user <a href="mailto:new@alienvault.com">new@alienvault.com</a>, then the destination email is <a href="mailto:new@alienvault.com">new@alienvault.com</a>.</td>
</tr>
<tr>
<td>Event Outcome</td>
<td>Filter system events by the success of an action.</td>
</tr>
<tr>
<td>Event Change</td>
<td>Filter system events by the description of what was changed in the system event.</td>
</tr>
<tr>
<td>Source Asset</td>
<td>Filter system events by the hostname or IP address of the host that initiates the system event.</td>
</tr>
</tbody>
</table>

The number between the icons of a filter, as well as the number next to it, indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

#### Icons Next to the Filter Title

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔢</td>
<td>Sort the filters alphabetically.</td>
</tr>
<tr>
<td>⬇️</td>
<td>Sort the filters by the number of items that match them.</td>
</tr>
</tbody>
</table>

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the **X** icon next to the filter. Or clear all filters by clicking **Reset**.
Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

Standard Mode
This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

To activate the standard mode when the advanced mode is on
1. Go to Settings > System Events.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray.

Note: If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

Advanced Mode
Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

To activate the advanced mode
1. Go to Settings > System Events.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green.

To perform a search in the advanced mode
1. Go to Settings > System Events.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green.
3. Click the filters that you want to select.
   The selected filters display inside a dashed rectangle.
4. In the lower-left corner of the page, click **Apply Filters**. Or in the upper side of the page, click **Apply**.

The result of your search displays.

**To search using the NOT operator**

1. Go to **Settings > System Events**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click **Not**.

- **Important**: You have to select a filter to see this operator.
- **Note**: The selected filter displays the icon and the filter chiclet is labeled in red.
Important: Some filters don't include the NOT operator (for example, Services or Software).

5. Click Apply.

To search all values of a filter
1. Go to Settings > System Events.
2. In the upper left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

Searching System Events by Using the Search Field

To search System Events using the search field
1. Go to Settings > System Events.
2. Enter your query in the search field.
   
   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   Note: Keep in mind that wildcard characters are considered as literals.
3. Click the icon.
The result of your search displays with the items identified.

Viewing System Event Details

The system event details page provides in-depth information on system events.

To view the details of a system event
1. Go to Settings > System Events.
2. Click the system event to display its details.
   - Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.
3. In the upper right corner, click the previous and next buttons to navigate between items.
4. Click the ◄ icon to close the dialog box.

Regular Events and System Events

USM Anywhere™ User Guide

USM Anywhere provides a centralized view of regular events and system events.

From now on, and during a grace period, the following regular events are also generated as system events:

- Sensor appears offline (see Sensor Disconnected from the USM Anywhere Service for more information)
- Sensor reconnected (see Sensor Disconnected from the USM Anywhere Service for more information)
- Event from asset not received (see Events Created When an Asset Stops Sending Data for more information)
- Event from AlienApp not received (see Events Created When AlienApps Stop Receiving Data for more information)
Warning: Soon the previously listed regular events will be generated only as system events. AT&T Cybersecurity will announce this change in advance. Meanwhile, AT&T Cybersecurity recommends that you disable all orchestration rules in your environment regarding these kinds of regular events and create new orchestration rules based on these system events. See Orchestration Rule for the "Sensor Appears Offline" System Event, Orchestration Rule for the "Sensor Reconnected" System Event, Orchestration Rule for the "Event from Asset Not Received" System Event, and Orchestration Rule for the "Event from AlienApp Not Received" System Event for more information.

Disabling Orchestration Rules

AT&T Cybersecurity recommends that you disable all orchestration rules you have created in your environment regarding these events:

- Sensor appears offline
- Sensor reconnected
- Event from asset not received
- Event from AlienApp not received

To disable an orchestration rule:
1. Go to Settings > Rules.
2. In the enabled column, click the icon of the rule you want to disable.

This turns the icon gray and disables the orchestration rule.

Orchestration Rule for the "Sensor Appears Offline" System Event

AT&T Cybersecurity recommends that you create new orchestration rules regarding the Sensor appears offline system event. The usual way is to create alarm rules or notification rules. See Alarm Rules from the Orchestration Rules Page and Notification Rules from the Orchestration Rules Page for more information.
To create a notification rule for the *Sensor appears offline* system event:

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Notification Rule**.
3. Select System Events in the Match drop-down list.
4. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.

**Note:** You can check the fields from **Settings > System Events**. See **Viewing System Event Details** for more information.
5. (Optional.) Click **Add Group** to group your conditions.

**Note:** See [Operators in the Orchestration Rules](#) for more information.

**Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.
6. Click Next.

7. Enter a name for the rule.

8. (Optional.) Enter a description for identifying this rule.

9. Select a notification method:
   - **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the **USM Anywhere Deployment Guide** for more information.
   - **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the **USM Anywhere Deployment Guide** for more information.
   - **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

   **Note:** The rolling 24-hour 200 email limit applies to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

   - **PagerDuty:** This method is not used to initiate an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the **USM Anywhere Deployment Guide** for more information.
   - **Slack:** This method makes use of a user-created Slack Webhook integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the **USM Anywhere Deployment Guide** for more information.

10. Modify these two options:
   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
Length: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

1. Click Save.

The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### Orchestration Rule for the "Sensor Reconnected" System Event

AT&T Cybersecurity recommends that you create new orchestration rules regarding the Sensor reconnected system event. The usual way is to create alarm rules or notification rules. See Alarm Rules from the Orchestration Rules Page and Notification Rules from the Orchestration Rules Page for more information.

To create a notification rule for the Sensor reconnected system event:

1. Go to Settings > Rules > Orchestration Rules.
2. Select Create Orchestration Rule > Notification Rule.
3. Select System Events in the Match drop-down list.

USM Anywhere™

User Guide
4. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.

**Note:** You can check the fields from **Settings > System Events**. See **Viewing System Event Details** for more information.

---

**Sensor Reconnected**

17 days ago

<table>
<thead>
<tr>
<th>System Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>SENSOR</td>
</tr>
<tr>
<td>TIMESTAMP ARRIVED</td>
</tr>
<tr>
<td>TIME CREATED</td>
</tr>
<tr>
<td>OBJECT TYPE</td>
</tr>
<tr>
<td>NEEDS INTERNAL ENRICHMENT</td>
</tr>
<tr>
<td>SUPPRESSED</td>
</tr>
<tr>
<td>TRANSIENT</td>
</tr>
<tr>
<td>TENANT</td>
</tr>
<tr>
<td>TIMESTAMP TO STORAGE</td>
</tr>
<tr>
<td>UUID</td>
</tr>
<tr>
<td>NEEDS ENRICHMENT</td>
</tr>
<tr>
<td>LABEL</td>
</tr>
</tbody>
</table>
5. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.

**Note:** You can check the fields from **Settings > System Events**. See [Viewing System Event Details](#) for more information.

6. (Optional.) Click **Add Group** to group your conditions.

**Note:** See **Operators in the Orchestration Rules** for more information.

**Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click **Next**.

![1 Warnings, review before continuing](image)

**Important:** A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.

10. Select a notification method:

- **Amazon SNS:** This method requires the setup of an Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit on the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See [Sending Notifications Through Amazon SNS](#) in the **USM Anywhere Deployment Guide** for more information.

- **Datadog:** This method requires the setup of a Datadog API key and additional steps. See [Sending USM Anywhere Notifications to Datadog](#) in the **USM Anywhere Deployment Guide** for more information.

- **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.
• **PagerDuty**: This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the *USM Anywhere Deployment Guide* for more information.

• **Slack**: This method makes use of a user-created *Slack Webhook* integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the *USM Anywhere Deployment Guide* for more information.

1. Modify these two options:

   • **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

   • **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

   In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

2. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See Orchestration Rules for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

---

**Orchestration Rule for the "Event from Asset Not Received" System Event**

AT&T Cybersecurity recommends that you create new orchestration rules regarding the *Event from asset not received* system event.

The usual way is to create alarm rules or notification rules. See Alarm Rules from the Orchestration Rules Page and Notification Rules from the Orchestration Rules Page for more information.

**To create a notification rule for the *Event from asset not received* system event**

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Notification Rule**.
3. Select System Events in the Match drop-down list.
4. Click Add Conditions and select the property values you want to include in the rule to create a matching condition.

Note: You can check the fields from Settings > System Events. See Viewing System Event Details for more information.
5. (Optional.) Click **Add Group** to group your conditions.

- **Note:** See Operators in the Orchestration Rules for more information.
- **Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.
6. Click Next.

![Warning]

**1 Warnings, review before continuing**

Please review warning messages. Your rule could cause performance issues. Are you sure want to proceed?

- **Cancel**
- **Accept**

**Important**: A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

7. Enter a name for the rule.
8. (Optional.) Enter a description for identifying this rule.
9. Select a notification method:
   - **Amazon SNS**: This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the USM Anywhere Deployment Guide for more information.
   - **Datadog**: This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the USM Anywhere Deployment Guide for more information.
   - **Email**: This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

**Note**: The rolling 24-hour 200 email limit applies to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

- **PagerDuty**: This method is used to trigger an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the USM Anywhere Deployment Guide for more information.
- **Slack**: This method makes use of a user-created Slack Webhook integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the USM Anywhere Deployment Guide for more information.

10. Modify these two options:

- **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
**Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

1. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

---

**Orchestration Rule for the "Event from AlienApp Not Received" System Event**

AT&T Cybersecurity recommends that you create new orchestration rules regarding the *Event from AlienApp not received* system event.

The usual way is to create alarm rules or notification rules. See **Alarm Rules from the Orchestration Rules Page** and **Notification Rules from the Orchestration Rules Page** for more information.

To create a notification rule for the Event from AlienApp not received system event:

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Notification Rule**.
3. Select System Events in the Match drop-down list.
4. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.

**Note:** You can check the fields from **Settings > System Events**. See [Viewing System Event Details](#) for more information.
5. (Optional.) Click **Add Group** to group your conditions.

**Note:** See [Operators in the Orchestration Rules](#) for more information.

**Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

### User Guide
6. Click Next.

7. Enter a name for the rule.
8. (Optional.) Enter a description for identifying this rule.
9. Select a notification method:
   - **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the *USM Anywhere Deployment Guide* for more information.
   - **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the *USM Anywhere Deployment Guide* for more information.
   - **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.
     - **Note:** The rolling 24-hour 200 email limit applies to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.
   - **PagerDuty:** This method is to be used in an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the *USM Anywhere Deployment Guide* for more information.
   - **Slack:** This method makes use of a user-created *Slack Webhook* integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the *USM Anywhere Deployment Guide* for more information.
10. Modify these two options:
   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
• **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

1. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

### Console User Events on USM Anywhere

A console user event is a file generated when a user does any action inside USM Anywhere. These actions are create, edit, delete, enable, or disable. A console user event is created when a user does one of these actions in the user interface (UI). This information is important to be compliant with external auditing agencies.

USM Anywhere enables you to view the activity of these console user events. All generated events display in the page. Go to **Settings > Console User Events** to display the page.

This topic discusses these subtopics:

- [USM Anywhere Console User Events List View](#)
- [Searching Console User Events](#)
- [Viewing Console User Events Details](#)
USM Anywhere provides a centralized view of your console user events. Go to **Settings > Console User Events**.

The console user events page displays information on any actions generated within your environment by the user. In the upper side of the page, you can see any filters you have applied. The main part of the page is the actual list of console user events. Each row describes an individual console user event.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the ✗ icon to hide the filter pane. Click the ▼ icon to expand the filter pane.

**Note:** By default, the list displays all console user events generated throughout the last 180 days.

This table includes the list of the default columns in the console user events page.

### List of the Default Columns in the Console User Events page

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Time Created</td>
<td>The date and time of the creation of the event. The displayed date depends on your computer's time zone.</td>
</tr>
<tr>
<td>Username</td>
<td>Email account associated with the person who triggered the event.</td>
</tr>
<tr>
<td>Target</td>
<td>Identification of the modified object.</td>
</tr>
</tbody>
</table>

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Above the list, you also have a filter to sort the list by a specific column.
USM Anywhere includes several filters displayed by default. These filters enable you to search for your items of interest. You can either filter your search, or enter what you are looking for in the search field, which is in the upper-left corner of the page.

**Note:** The management of filters is similar to that for assets. See Managing Filters for more information.

This table includes the filters displayed by default in the main page of the Console User Events page.

### Filters Displayed by Default in the Main Console User Events Page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Filter system events triggered in the last hour, last 24 hours, last 7 days, last 30 days, or last 90 days. You can also configure your own period of time by clicking the <strong>Custom Range</strong> option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select <strong>AM</strong> or <strong>PM</strong>.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Filter system events by the short, user-readable description of the system event.</td>
</tr>
<tr>
<td>Username</td>
<td>Email of the user who triggered the event.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of object,</td>
</tr>
</tbody>
</table>

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

#### Icons Next to the Filter Title

- **A Z** Sort the filters alphabetically.
- **Z A** Sort the filters by the number of items that match them.

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the **X** icon next to the filter. Or clear all filters by clicking **Reset**.

**Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the **X X** icon or clicking the **✓ ✓** icon located in the upper left corner of the page.
**Standard Mode**

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

**To activate the standard mode when the advanced mode is on**

1. Go to .
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray, .

**Note**: If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

**Advanced Mode**

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

**To activate the advanced mode**

1. Go to Settings > Console User Events.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   
   This turns the icon green, .

**To perform a search in the advanced mode**

1. Go to Settings > Console User Events.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   
   This turns the icon green, .
3. Click the filters that you want to select.
   
   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click Apply Filters. Or in the upper side of the page, click Apply.

**To search using the NOT operator**

1. Go to Settings > Console User Events.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.

**Important**: You have to select a filter to see this operator.
**Important:** Some filters don't include the NOT operator (for example, Services or Software).

5. Click Apply.

To search all values of a filter

1. Go to **Settings > Console User Events**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

Searching Console User Events by Using the Search Field

To search Console User Events by using the search field

1. Go to **Settings > Console User Events**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This applies even within the set (for example, "bob@mycompany.com").

**Note:** Keep in mind that wildcard characters are considered as literals.

3. Click the icon.
The result of your search displays with the items identified.

Filter Console User Events by Username

USM Anywhere enables you to search your console user events by username. You have these options to filter events by that field:

- From the Console User Events page by using the username filter
- From the Users List page
To filter console user events by the username from the users list page

1. Go to Settings > Users.
2. Click the ⬇️ icon.

**USM Anywhere™**

**User Guide**
3. Select the option **View account events**.

The console user events page opens displaying the events related to that username.

The Console User Events details page provides in-depth information on Console User Events.
To view the details of a Console User Event

1. Go to **Settings > Console User Events**.
2. Click the console user event to display its details.

```
Console user role updated
Mon, Feb 17 2020, 02:29 PM

Console User Event Details

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>Console user role updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>***</td>
</tr>
<tr>
<td>TYPE</td>
<td>Console User</td>
</tr>
<tr>
<td>TARGET</td>
<td></td>
</tr>
</tbody>
</table>
| NEW VALUE         | `{ "name": "manager",
|                   |   "description": "",
|                   |   "id": "890c848a-e1e8-4ef3-a995-59d68ca5aae3" }` |
```

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

3. Click the item to see an expanded view.
4. In the upper right corner, click the **previous** and **next** buttons to navigate between items.
5. Click the ✗ icon to close the dialog box.
Configuration Issues Management

USM Anywhere assesses your configuration to identify the insecure use of security features, identify detailed information about configuration issues, to understand operational processes, and to remediate the root cause.

**Note:** Configuration Issues are only available for AWS Sensors.

This topic discusses these subtopics:

- Configuration Issues List View ................................................................. 363
- Searching Configuration Issues ............................................................. 366
- Viewing Configuration Issues Details .................................................. 371
- Create a Configuration Issues Report .................................................. 372
- List of Configuration Issues in USM Anywhere .................................... 373
USM Anywhere provides a centralized view of your configuration issues. Go to Environment > Configuration Issues to see this centralized view.

The configuration issues page displays information on configuration issues. On the left you can find the search and filters options. In the upper side of the page, you can see any filters you have applied, and you have the option to create and select different views of the configuration issues. The main part of the page is the actual list of configuration issues. Each row describes an individual configuration issue and includes a check box on the left side of each one for selecting it. You can select all the configuration issues on the same page by clicking the check box in the first column of the header row.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

### List of the Default Columns in Configuration Issues

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>Last date on which the configuration issue was seen in the asset. The displayed date depends on your computer's time zone.</td>
</tr>
<tr>
<td>Category</td>
<td>Category of the configuration issue. Issues with similar impacts have the same category.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Sub-category of the configuration issue. The sub-category explains the particular detail of the issue.</td>
</tr>
<tr>
<td>Asset</td>
<td>Asset associated with the configuration issue.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity of the issue. Values are Low, Medium, or High.</td>
</tr>
<tr>
<td>Description</td>
<td>Text for identifying the configuration issue.</td>
</tr>
<tr>
<td>First Seen</td>
<td>Date of detection of the configuration issue in the asset. The displayed date depends on your computer’s time zone.</td>
</tr>
</tbody>
</table>

Click the icon to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.
- **Find in events**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.
• **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See *Using OTX in USM Anywhere* for more information.

• **Full Details**: See *Viewing Assets Details* for more information.

• **Configure Asset**: See *Editing Assets* for more information.

• **Delete Asset**: See *Deleting the Assets* for more information.

• **Assign Credentials**: See *Managing Credentials in USM Anywhere* for more information.

• **Authenticated Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See *Running Authenticated Asset Scans* for more information.

• Scan with AlienApp: This option enables you to run an asset scan through an AlienApp. See *Running Asset Scans Using an AlienApp* for more information.

• **Run Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See *Running Asset Scans* for more information.

• **Configuration Issues**: This option opens the Assets Details page. The Configuration Issues tab is selected in the page. See *Viewing Assets Details* for more information.

• **Vulnerabilities**: This option opens the Assets Details page. The Vulnerabilities tab is selected in the page. See *Viewing Assets Details* for more information.

• **Alarms**: This option opens the Assets Details page. The Alarms tab is selected in the page. See *Viewing Assets Details* for more information.

• **Events**: This option opens the Assets Details page. The Events tab is selected in the page. See *Viewing Assets Details* for more information.

You can configure the view you want for the list of configuration issues. See *Views* for more information.

Click **Generate Report** button to open the Configure Report dialog box. See *Create a Configuration Issues Report* for more details.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

**Views**

USM Anywhere enables you to define and save a custom Configuration Issues view to have your own selected filters.

You can configure the view you want for the list of items in the page.
To create a view configuration

1. From the Configuration Issues list view, select the filters you want to apply.
2. Select Save View > Save as.
   
The Save Current View dialog box opens.

3. Enter a name for the view.
4. Select Share View if you want to share your view with other users.
5. Click Save.
   
The created view is already selected.

To select a configured view

1. From the Configuration Issues list view, click View above the filters.
2. Click Saved views and select the view you want to see.

   ![Note: A shared view includes the sharing icon next to its name.]

3. Click Apply.

To delete a configured view

1. From the Configuration Issues list view, click View above the filters.
2. Click Saved views and click the delete icon next to the saved view you want to delete.
   
   A dialog box displays to confirm the deletion.
Note: You can delete the views you have created.

3. Click Accept.

Important: The icon does not display if the view is selected.

Configuration Issues from the Assets Main Page

To explore configuration issues from assets

1. Go to Environment > Configuration Issues.
2. Filter assets by clicking Has Configuration Issues. See Searching Assets for more information.
3. Click the icon and select Configuration Issues. The asset details page opens with the list of configuration issues.

Searching Configuration Issues

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the Configure filters link located in the upper-left corner of the page. The management of filters is similar to that for assets. See Managing Filters for more information.

Filters Displayed by Default in the Main Configuration Issues Page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Filter configuration issues triggered in the last hour, the last 24 hours, last 7 days, or last 30 days. You can also configure your own period of time by clicking the Custom Range option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select AM or PM.</td>
</tr>
<tr>
<td>Active/Inactive</td>
<td>Filter the active or inactive configuration issues.</td>
</tr>
</tbody>
</table>
**Filters Displayed by Default in the Main Configuration Issues Page (Continued)**

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Filter configuration issues by category of configuration issue. Issues with similar impacts have the same category.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Filter configuration issues by sub-category of the configuration issue. The sub-category explains the particular detail of the issue.</td>
</tr>
<tr>
<td>Severity</td>
<td>Filter configuration issues by severity of the issue. Values are Low, Medium, or High.</td>
</tr>
<tr>
<td>Asset</td>
<td>Filter configuration issues by asset associated with the configuration issue.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>Filter configuration issues by asset group.</td>
</tr>
</tbody>
</table>

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

**Icons Next to the Filter Title**

- ![Sort Alphabetically](image) Sort the filters alphabetically.
- ![Sort by Count](image) Sort the filters by the number of items that match them.

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the ![X](image) icon next to the filter. Or clear all filters by clicking **Reset**.

**Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.
Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

USM Anywhere enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

**Standard Mode**

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.
To activate the standard mode when the advanced mode is on

1. Go to Environment > Configuration Issues.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray, X.

**Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

Advanced Mode

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

**To activate the advanced mode**

1. Go to Environment > Configuration Issues.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   
   This turns the icon green, ☑.

**To perform a search in the advanced mode**

1. Go to Environment > Configuration Issues.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   
   This turns the icon green, ☑.
3. Click the filters that you want to select.
   
   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click **Apply Filters**. Or in the upper side of the page, click **Apply**.
   
   The result of your search displays.
To search using the NOT operator

1. Go to Environment > Configuration Issues.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.

**Important:** You have to select a filter to see this operator.

**Note:** The selected filter displays the icon and the filter chiclet is labeled in red.

5. Click Apply.

**To search all values of a filter**

1. Go to Environment > Configuration Issues.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.
To search Configuration Issues using the search field

1. Go to Environment > Configurations Issues.
2. Enter your query in the search field.
   
   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   **Note:** Keep in mind that wildcard characters are considered as literals.

3. Click the search icon.

The result of your search displays with the items identified.

### Viewing Configuration Issues Details

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

The configuration issues details page provides in-depth information on configuration issues.

**To view the details of a configuration issue**

1. Go to Environment > Configuration Issues.
2. Click the configuration issue to display its details.

   Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.
You can see the configuration issues details, then a description, and the associated asset. Click the ▶️ icon if you want more information. See Viewing Assets Details for more information.

3. In the upper right corner, click the previous and next buttons to navigate between items.
4. Click the ❌ icon to close the dialog box.
5. Click the configuration issue title to expand its details.

Create a Configuration Issues Report

You can create a PDF or CSV report of the configuration issues directly from the configuration issues page.

Important: AT&T Cybersecurity recommends Google Chrome as the preferred browser for generating reports.

To create a configuration issues report

1. Go to Environment > Configuration Issues.
2. You can use filters to define the configuration issues content you want to display in your report.

3. Click the Generate Report button to open the Configure Report dialog box. The filters selected and displayed for the page view are the ones that are populated in the report.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

**Note:** This option is not available when generating reports for assets or asset groups.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, or Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the Number of records section, choose the maximum number of records to include on the report. For CSV the options are 20, 50, 100, 500, 1000, or 50 K. For PDF the options are 20, 50, 100, 500, 1000, or 2500.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ⬅ icons.
15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
16. Click Run to run the report.

**List of Configuration Issues in USM Anywhere**

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

This table includes all configuration issues you can find in USM Anywhere:
<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Protocol (Port)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global access to administration port</td>
<td>SSH</td>
<td>TCP (22)</td>
<td>Global access to the SSH port has been defined within this security group. This should be restricted to the IP Range of the company.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>DNS (UDP)</td>
<td>UDP (53)</td>
<td>Global access to the DNS port has been defined within this security group.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>DNS (TCP)</td>
<td>TCP (53)</td>
<td>Global access to the DNS port has been defined within this security group.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>Mini SQL</td>
<td>TCP (4333)</td>
<td>Global access to the MSQL port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>SQL Server (UDP Port)</td>
<td>UDP (1434)</td>
<td>Global access to the SQL Server port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>SQL Server (TCP Port)</td>
<td>TCP (1433)</td>
<td>Global access to the SQL Server port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>PostgreSQL Server</td>
<td>TCP (5432)</td>
<td>Global access to the PostgreSQL port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>MySQL Server</td>
<td>TCP (3306)</td>
<td>Global access to the MySQL port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>Syslog</td>
<td>UDP (514)</td>
<td>Global access to the Syslog port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Protocol (Port)</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>rsync</td>
<td>TCP (873)</td>
<td>Global access to the rsync port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>MongoDB (UDP)</td>
<td>UDP (27017)</td>
<td>Global access to the MongoDB port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>MongoDB (TCP)</td>
<td>TCP (27017)</td>
<td>Global access to the MongoDB port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>CouchDB (UDP)</td>
<td>UDP (5984)</td>
<td>Global access to the CouchDB port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to internal port</td>
<td>CouchDB (TCP)</td>
<td>TCP (5984)</td>
<td>Global access to the CouchDB port has been defined within this security group. This should be an internally facing port only.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>VNC Server</td>
<td>TCP (5900)</td>
<td>Global access to the VNC Server port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>VNC Listener</td>
<td>TCP (5500)</td>
<td>Global access to the VNC Listener port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>Windows RPC</td>
<td>TCP (135)</td>
<td>Global access to the Windows RPC port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>Windows Remote Desktop</td>
<td>TCP (3389)</td>
<td>Global access to the Windows Remote Desktop port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
</tbody>
</table>
### List of Configuration Issues in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Protocol (Port)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global access to administration port</td>
<td>Telnet</td>
<td>TCP (23)</td>
<td>Global access to the Telnet port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>X11 (TCP)</td>
<td>TCP (6000)</td>
<td>Global access to the X11 port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to administration port</td>
<td>X11 (UDP)</td>
<td>UDP (6001)</td>
<td>Global access to the X11 port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>SMTP</td>
<td>TCP (25)</td>
<td>Global access to the SMTP port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>FTP</td>
<td>TCP (21)</td>
<td>Global access to the FTP port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>FTP Data</td>
<td>TCP (20)</td>
<td>Global access to the FTP (data) port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>CIFS</td>
<td>UDP (445)</td>
<td>Global access to the CIFS port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>NetBios (Named Services)</td>
<td>UDP (137)</td>
<td>Global access to the NetBios (Named Services) port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>NetBios (Datagram Services)</td>
<td>UDP (138)</td>
<td>Global access to the NetBios (Datagram Services) port has been defined within this security group. This should be restricted to a company owned CIDR.</td>
</tr>
</tbody>
</table>
List of Configuration Issues in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Protocol (Port)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP globally permitted</td>
<td>ICMP</td>
<td>ICMP</td>
<td>ICMP is globally permitted.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>All TCP Ports Open</td>
<td>TCP (1)</td>
<td>All TCP ports have been explicitly permitted by this security group. Access to your system should be restricted to the minimal set of TCP ports you require to access for operation. In addition, ensure ports that are for administrative access or do not require global access should be restricted to a company owned CIDR.</td>
</tr>
<tr>
<td>Global access to service port</td>
<td>All UDP Ports Open</td>
<td>UDP (1)</td>
<td>All UDP ports have been explicitly permitted by this security group. Access to your system should be restricted to the minimal set of UDP ports you require to access for operation. In addition, ensure ports that are for administrative access or do not require global access should be restricted to a company owned CIDR.</td>
</tr>
</tbody>
</table>

USM Anywhere Scheduler

The Job Scheduler page provides a list of all jobs that are defined in your USM Anywhere environment. Many jobs are predefined (out-of-the-box) items for log collection and asset scans, and some of these require enablement to run according to the defined schedule. You can also define your own custom jobs to schedule automatic log collection, asset scans, and asset group scans. See USM Anywhere Scheduler Best Practices for more information.

The Job Scheduler Page

The Job Scheduler page includes navigation and filtering elements to help you locate the jobs you want to review. When you go to Settings > Scheduler, the page displays all jobs by default. You can select one of the job types in the left navigation to display only the jobs of that type:
• **Log Collection**: Select this display option to review the list of scheduled log collection jobs. See Log Collection from Your Data Sources for more information.

• **Asset Scans**: Select this option to review the list of scheduled asset scan jobs. This option displays both asset scan, authenticated asset scan, and asset discovery jobs. See Scheduling Asset Scans from Assets, Scheduling Authenticated Asset Scans from Assets, and Running an Asset Discovery for more information.

• **Asset Group Scans**: Select this option to review the list of scheduled asset group scan jobs. This option displays both asset group scan and authenticated asset group scan jobs. See Running Asset Groups Scans, and RunningAuthenticated Asset Groups Scans for more information.

• **User Scans**: Select this option to review the list of scheduled user scan jobs. These jobs detect users in your environment for User Behavior Analytics.
USM Anywhere Scheduler Best Practices

USM Anywhere provides automatic repeatable actions that are collectively called *jobs*, which you can run in your environment. The jobs are initiated on a schedule stored in your provisioned USM Anywhere cloud instance. All jobs are directly assigned to a sensor, and acted upon by the assigned sensor. The cloud instance doesn’t perform job activities; it only schedules them and collects the output of the job for processing.

Go to **Settings > Scheduler** to open the Scheduler page and display all jobs by default.

The scheduler specifies when a job is sent to the assigned sensor for processing based on the job schedule. Preloaded log collection jobs can't be edited. These jobs don't have the icon associated with it, but they can be enabled or disabled. These jobs have settings that are created and managed by USM Anywhere.

Log Collection jobs run endpoint-specific API calls against target systems. Some log collection jobs are sensor-type specific because they query endpoints specific to the sensor type in use. For example, the Scan Azure Audit Sharepoint Events job is only active for Azure Sensors.

Many of these jobs are associated with an AlienApp selection. Go to **Data Source > AlienApps** to view the available AlienApps. Keep in mind that assigning multiple sensors to perform API calls to the same endpoint can cause unnecessary duplication of data and effort, therefore must be avoided.

**Note:** You can enable AlienApps on the AlienApp page, but it does not automatically enable the job to run. See **USM Anywhere Scheduler** for more information.

Asset Scans are used for asset discovery. This app has multiple actions and scan profiles. See **Scheduling Asset Scans from Assets** and **Scheduling Asset Scans from the Job Scheduler Page** for more information. The Asset Scans section also include asset discoveries performed through
API calls. Some examples of this include the discover S3 buckets job for AWS Sensors, the
discover virtual machines job for VMware Sensors, and the scan Azure IIS log locations job for
Azure Sensors.

Asset Group Scans are performed for vulnerability scanning. This app also has multiple scan
profiles. See Scheduling Asset Group Scans from Asset Groups and Scheduling Asset Groups
Scans from the Job Scheduler Page for more information.

Asset Scans and Asset Group Scans are user-created jobs. No such jobs come pre-loaded into a
system image. All of these jobs can be edited, enabled and disabled.

Performance Issues Associated with Scheduled Jobs

Log Collection jobs are initially preset at installation and can’t be modified by a user, regardless of
the role. They can only be enabled or disabled. Additional Log Collection jobs can be user defined
and their action and time frames are set by a user at that time. These settings can be edited.

Keep in mind the following points when scheduling your jobs because they have a direct impact
on the performance of a sensor and USM Anywhere cloud instance:

• When specifying a Classless Inter-Domain Routing (CIDR) block for jobs that require it, limit it
to a /24 or smaller network segment. Avoid using a /16 CIDR block size. The smaller the CIDR
block number used, the larger the network IP address range it will process. These are some
sample IP ranges:
  • /16 notation will access 64,000 IP addresses
  • /24 notation will access 256 IP addresses
  • /28 notation will access 16 IP addresses

• If multiple user-defined scheduled jobs are required for the environment, spread them over a
24-hour period, and avoid having more than one scan job type running at any given time. This
holds true for all jobs regardless of the sensor or sensors in use. Although the scan jobs may
be readily run on any given sensor, all sensor data is forwarded to the USM Anywhere cloud
instance and can, cumulatively, cause performance issues.

• Scheduling an Asset Scan or Asset Group Scan job to run more than once a day is coun-
terproductive and directly affects system performance. This is also true for AD Scanner jobs.
The best practice is to run them, at most, no more than once a day, or, every other day, and
overlap them on alternate days. Additionally, initiate the job at off-hours where sensor and
USM Anywhere cloud instance activity is lowest.

• Vulnerability scans should be run weekly or at even larger intervals. This job checks for soft-
ware vulnerabilities on installed servers. Unless continuous software updates are being per-
formed in the environment, scanning no more than once a week is sufficient. This job can also
be initiated manually if immediate results are required.

• Try to space jobs at least one hour apart on any given day. At least two hours is recom-
mended. Do not “stack” more than two to three jobs for any start time.
Ensure job start time intervals are larger than the time it takes for the job to complete. If not, this will cause the job to continuously run and put a constant load on the sensor.

If multiple AWS Sensors are in the same account subscription, only one AWS log collection job is required as any given AWS Sensor has visibility to all AWS regions associated with the account. AWS log collection jobs that explicitly span all regions and streams are noted in the description field of the job. Although not noted there, all AWS EC2 Scan jobs will traverse all regions as well. The processing of multiple regions by such a job can't be limited in the job settings.

Managing Jobs in the Scheduler

The Job Scheduler enables you to configure specific jobs to run automatically in your environment on a set schedule, keeping your USM Anywhere up to date on the latest changes in your environment. Visit the Job Scheduler page at Settings > Scheduler to view a list of all jobs that are defined in your USM Anywhere environment and to manage the jobs that are scheduled to run in your environment.

Sort and Filter the Displayed Jobs

To change the sort order of the displayed list, click the column label for the field that you want to use to sort the list. Use the filters in the upper side of the list to change the displayed list so that it includes only the jobs you want to see.
These are the Job Scheduler filters:

- **Filter by:** Enter a search string for the name of the app or the job name to display only matching jobs.

- **Sensor:** If you have more than one deployed USM Anywhere Sensor, select a Sensor to display only the jobs that are configured for it. You also have the option All Sensors to display all sensors you have in your environment.

- **Job Type:** Set this option to display only the jobs of the selected type. The available items are based on the jobs currently displayed on the page:
  - All Types
  - Collection
  - Scan
  - Configuration
  - Asset Discovery
  - User Scan

- **Task Status:** Set this option to display only jobs for the selected status, Enabled or Disabled. You also have the option All Tasks.

- **Clear Filters:** Click this button to remove filtering options and display all items for the category selected in the left navigation.

When you locate a scheduled job in the list, you can select it to expand the details for the job and review its history.
Enable Defined Jobs

When most logs in your Amazon Web Services (AWS) or Microsoft Azure account are enabled, USM Anywhere automatically discovers them and they can start generating events, based on AWS CloudTrail, Amazon Simple Storage Service (S3), AWS Elastic Load Balancing (ELB) access logs, Azure security event logs, and others. But, because these out-of-box log collection and asset scan jobs deploy as disabled initially, you must decide which jobs you want to activate and enable them.

You can disable or enable a predefined or custom job in the Job Scheduler page.

To enable scheduled jobs

1. Go to Settings > Scheduler to open the Job Scheduler page.
2. Locate the jobs with which you want to enable to collect events or asset information, and click the ☑️ icon.

   This turns the ☑️ icon green. To disable an already-enabled job, toggle the icon to its original status.

### Job Scheduler

Jobs collect information about your environment and execute actions based on a repeating schedule. Learn more about scheduling jobs

<table>
<thead>
<tr>
<th>Filter by</th>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>SCHEDULE</th>
<th>LAST RUN</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Box</td>
<td>Collect Box Admin Events</td>
<td>Box App Data Collection Job</td>
<td>Every 20 minutes</td>
<td>-</td>
</tr>
<tr>
<td>AWS</td>
<td>S3</td>
<td>Collect S3 access logs</td>
<td>S3 Access Logs Job</td>
<td>Every 5 minutes</td>
<td>-</td>
</tr>
<tr>
<td>AWS</td>
<td>Load Balancing</td>
<td>Collect Elastic Load Balancing events</td>
<td>Every 20 minutes</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>Discover S3 buckets</td>
<td>Discover S3 buckets with access logging enabled</td>
<td>Every 20 minutes</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Cisco AMP</td>
<td>Pull events from Cisco AMP</td>
<td>Pull events from Cisco AMP</td>
<td>Every 20 minutes</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>ConnectWise</td>
<td>Update the Configurations catalog</td>
<td>Trigger the update of the Configurations catalog every 60 minutes</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConnectWise</td>
<td>Update the Ticket database</td>
<td>Trigger the update of the Ticket database every 5 minutes</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 - 14 of 14
Modify Defined Jobs
You can only change the parameters of out-of-the-box jobs related to USM Anywhere AlienApps. Other USM Anywhere defined jobs cannot be modified.

To make changes to an AlienApp defined job
1. Locate the job in the Job Scheduler list.
2. In the row for the job, click the pencil icon.
3. In the Edit Job dialog box, change the parameters for the job as needed.

Note: The Name and Schedule fields are editable.

4. Click Save.

Add a New Custom Job
USM Anywhere includes defined jobs to perform many of the standard log collection and scanning actions that you will need to monitor your networks. These jobs are predefined to run using a recurrence according to industry best practices. However, if you need to define a scheduled job to perform log collection, asset scans, or asset group scans, you can add a new job directly on the Job Scheduler page.

To create a new job
1. Go to Settings » Scheduler to open the Job Scheduler page.
2. In the upper-right of the page, click New Job.
   - If you have selected Log Collection in the left navigation panel, this button is labeled Create Log Collection Job. This limits the options in the dialog to those that define a log collection job.
   - If you have selected Asset Scans or Asset Group Scans in the left navigation panel, this button is labeled Create Scan Job. This limits the options in the dialog to those that define an asset scan, asset group scan, or asset discovery job.
3. 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.

4. Select an **Action Type**:
   - Active Directory Scanner
   - Amazon Web Services
   - Asset Scanner
   - Authenticated Asset Scanner
   - Azure
   - Forensics and Response App

5. Select a sensor if you have more than one installed in your environment.
6. Use the **App Action** option to select the job to run. The selected app determines the actions that are available.

7. In the Schedule section, specify when USM Anywhere runs the job:
Managing Jobs in the Scheduler

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

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

b. Set the interval options for the increment.

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

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

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

c. Set the start time.

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

8. Click **Save**.
Modify or Delete a Custom Job

You cannot change or delete the parameters of the out-of-the-box jobs in USM Anywhere. You can only enable or disable the predefined jobs. However, you can make changes to the scheduled jobs that you have defined, such as changing the schedule parameters to run the job more or less frequently. If a custom job is no longer needed, you can delete it.

To make changes to a custom job
1. Locate the job in the Job Scheduler list.
2. In the row for the job, click the icon.
3. In the Edit Job dialog box, change the parameters for the job as needed. See Add a New Custom Job for more information about these options.
4. Click Save.

To delete a custom job
1. Locate the job in the Job Scheduler list.
2. In the row for the job, click the icon.
3. Click Accept to confirm.

Scheduling Active Directory Scans from the Job Scheduler Page
To effectively manage your Microsoft Windows systems, USM Anywhere can perform scans through an Active Directory (AD) server to collect inventory information. When you configure your VMware Sensor, Microsoft Hyper-V Sensor, or Microsoft Azure Sensor, you can define the credentials that USM Anywhere will use to perform AD scans through the sensor. When you configure these credentials, USM Anywhere performs an initial AD asset scan. You can also schedule a job to perform scans through the Active Directory Scanner and collect updated information about the assets managed by your AD server. The scan returns information for each computer in the AD domain in the following format:

Name : WIN2K12-DC  
DistinguishedName : CN=WIN2K12-DC,OU=Domain Controllers,DC=ECORP,DC=local  
DNSHostName : WIN2K12-DC.ECORP.local  
OperatingSystem : Windows Server 2012 R2 Standard  
OperatingSystemServicePack :  
OperatingSystemVersion : 6.3 (9600)  
IPv4Address : 10.20.30.15

The Active Directory Scanner runs a PowerShell (version 5.1 or later) command through Windows Remote Management (WinRM) (version 2.0 or later). See Granting Access to Active Directory for USM Anywhere for information about configuring the AD server to allow access for USM Anywhere.

To schedule an AD scan job

1. Go to Settings > Scheduler.
2. In the left navigation menu, click Asset Scans.
3. On the right side of the page, click Create Scan Job.

This opens the Schedule New Job dialog box.

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. In Action Type, select **Active Directory Scanner**.
   
   More options display.

6. If you have more than one deployed USM Anywhere Sensor, select the sensor you want to use to run the scan.
   
   This should be the sensor that is associated with the asset that you want to specify as the target.

7. In App Action, select **Get Active Directory Asset Information**.

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

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

b. Set the interval options for the increment.

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

---

**Schedule**

- **Week**
  - Monday
  - Tuesday
  - Wednesday
  - Thursday
  - Friday
  - Saturday
  - Sunday

Start time: 01:00 UTC Time Zone

---

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

---

**Schedule**

- **Month**
  - Day 1 of every 1 month(s)
  - Third Friday of every 1 month(s)

Start time: 01:00 UTC Time Zone

---

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

c. Set the start time.

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

10. Click **Save**.
Granting Access to Active Directory for USM Anywhere

If you want to run Active Directory (AD) scans in USM Anywhere, you need to configure your AD server assets to grant access to the USM Anywhere Sensor. You also need to configure credentials in USM Anywhere to make an authenticated connection.

This process contains three tasks:

- Create a dedicated administrator account in AD on all the hosts you want to scan. This is used by USM Anywhere to log into that host system to perform a scan.
- Activate Windows Remote Management (WinRM) in the domain controller and in all the hosts you want to scan.
- Apply the AD account credentials for those assets in USM Anywhere.

**Note:** See [Microsoft's guide on authentication for remote connections](https://docs.microsoft.com/en-us/windows-server/administration/remote-access/using-remote-control-winrm) for more information on Microsoft Windows authentication permissions.

Create a Dedicated AD Account

When configuring your VMware Sensor, Hyper-V Sensor, or Azure Sensor, you can define AD credentials that USM Anywhere uses to perform an AD scan through the sensor. These are the credentials that you define in the Credentials page and assign to the asset to support a scheduled Active Directory scan job. It is a best practice to use a dedicated account for this purpose.

**To create a new dedicated account in AD**

1. Log in to your domain controller administrator account.
2. Open **Active Directory Users and Computers**.
3. Create a new user called either `alienvault_usm_anywhere` or any other name that's easy to associate with USM Anywhere.
4. Add the user you've just created to the Domain Admins group.

Activate WinRM to Enable Windows PowerShell Remoting

For Microsoft Windows systems, USM Anywhere uses the WinRM framework to execute the corresponding commands. Therefore, if WinRM is unavailable on a target Windows system through the account credentials, USM Anywhere won't be able to connect. You must satisfy the following requirements:

- WinRM version 2.0 or later.
- PowerShell version 5.1 or later. The Active Directory Scanner runs a PowerShell command through WinRM, which requires PowerShell 5.1 or later to be installed on your machine.

To activate WinRM, you can use a group policy to configure the domain controller and all the hosts in your AD. (For reference, see this [How to enable PowerShell Remoting via Group Policy](https://docs.microsoft.com/en-us/windows-server/administration/remote-access/using-remote-control-winrm) article.)

Alternatively, if you prefer to activate WinRM manually in each system you want to scan, use this procedure to activate a Windows RM listener on port 5985.

**To start the WinRM service**

1. Open the Windows Command Prompt using administrator privileges and run the command `winrm qc`.

   **Important:** Only the members of the Remote Management Users and Administrators groups can log in through WS-Management.

2. Accept the default settings.

   The command starts the WinRM service and configures a listener for the port 5985.

3. Create a firewall rule to allow incoming connections to port 5985.
For more information about WinRM, you can refer to these Microsoft articles:


**Manage Credentials for Your AD Servers**

Before you run an AD scan from USM Anywhere, 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. See [Creating Credentials](#) on how to create credentials and [Assigning Credentials to Assets](#) on how to assign them to assets.

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

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

**Scheduling Asset Scans from the Job Scheduler Page**

USM Anywhere provides a simple way to include scans for scheduling using its web user interface (UI).

To schedule an asset scan job from the Job Scheduler page:

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the left navigation panel, click **Asset Scans**.
3. Click **Create Scan Job**.
   - The Schedule New Job dialog box opens.
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Asset Scanner. Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, leave Scan, which is the default option. This option discovers services, operating systems (OSes), hostnames, IP and media access control (MAC) addresses, and vulnerabilities of known hosts.
6. The Asset field displays the name of the asset to scan. You can't modify this field.
7. Select the scan profile that you want to run:
Discovery: This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)

Complete: This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)

Vulnerability Discovery: Performs general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.

Extended Vulnerability Discovery: Performs a Vulnerability Discovery scan, which actively discovers more about the network.

Intensive Vulnerability Discovery: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

8. Select Set Debug Mode if you want to log the results of the scan or if you have a problem with a scan. This option is disabled by default.

**Note:** The Set Debug Mode option must be used only for debugging purposes because it needs a large amount of disk space for the file or files that it generates. Only AT&T Cybersecurity Technical Support should review these files. You can contact this department for more information.

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

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

   b. Set the interval options for the increment.

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

   Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.
Important: USM Anywhere restarts the schedule on the first day of the month if the option "Every x days" is selected.

c. Set the start time.

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

10. Click Save.

The job now displays in the job scheduler list.

To schedule an authenticated asset scan job from the Job Scheduler page
1. Go to Settings > Scheduler to open the Job Scheduler page.
2. In the left navigation panel, click Asset Scans.
3. Click Create Scan Job.

The Schedule New Job dialog box opens.
1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Authenticated Asset Scanner. Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, Scan is the default option. This option discovers services, operating systems, hostnames, IP and MAC addresses, and vulnerabilities of known hosts.
6. The Asset field displays the name of the asset to scan. You can't modify this field.
7. In the Schedule section, specify when USM Anywhere runs the job:
a. Select the increment as **Minute, Hour, Day, Week, Month, or Year**.

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

b. Set the interval options for the increment.

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

![Weekly Schedule](image)

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

![Monthly Schedule](image)

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

c. Set the start time.

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

8. **Click Save.**

The job now displays in the job scheduler list.

### Scheduling Asset Groups Scans from the Job Scheduler Page

USM Anywhere provides a simple way to include scans for scheduling using its web user interface (UI).

**To schedule an asset group scan job from the Job Scheduler page**

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the left navigation panel, click **Asset Group Scans**.
3. Click **Create Scan Job**.
The Schedule New Job dialog box opens.

1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select Asset Scanner. Depending on the USM Anywhere Sensor that you have installed, this field can include different options.
4. Select a USM Anywhere Sensor in case you have more than one installed.
5. Select the **App Action:**
   - **Asset Discovery**
     - Discovers assets in your environment, detects changes in assets, and discovers malicious assets in the network.
Select Existing Asset Group: In the Enter asset group name field, search for the asset groups to scan. These asset groups are already existing, and you can search for them by entering the name of the asset group or by browsing for them.

Create New Asset Group to Scan Using CIDR Block: You can create a new asset group from a Classless Inter-Domain Routing (CIDR) block. You need to indicate the CIDR block and the network name you want to scan. This option discovers new assets and scans the discovered assets.

Important: Use the Create New Asset Group to Scan Using CIDR Block option for creating new CIDR-based asset groups without leaving the scheduler form. After clicking Save, a new asset group based on the selected CIDR is created.

Your scan job will have the Select Existing Asset Group option selected and the CIDR-based asset group assigned automatically.

Important: Make sure when you use a virtual private network (VPN) using a Cisco Firewall, that arp-proxy is enabled in the firewall. Otherwise, all the assets will be reported using the same media access control (MAC) address, and USM Anywhere will consider all of them to be different interfaces for the same asset.

Asset Group Scan

Discovers services, operating systems, hostnames, IP and MAC addresses, and vulnerabilities of known hosts. This option scans the assets that are already in the group.

The Asset Group field displays the name of the asset group to scan. You can't modify this field.

6. In the App Action field, the Asset Group Scan is the default option.
7. Select the scan profile that you want to run:

Discovery: This profile scans the known ports and services searching for the most-used ports. (There are 457 ports.)

Complete: This profile scans all TCP and UDP ports to find the possible ports in a deployment. (There are 65535 ports.)

Vulnerability Discovery: Performs general network discovery and checks for specific known vulnerabilities. It only reports results if they are found.

Extended Vulnerability Discovery: Performs a Vulnerability Discovery scan, which actively discovers more about the network.
**Intensive Vulnerability Discovery**: Performs several tasks to discover vulnerabilities, which uses up a significant number of resources on the targeted machine. Because of this, sensitive targets may perceive a brief disruption on their services.

8. (Optional.) Select the assets you want to exclude from the scan.

9. Select **Set Debug Mode** if you want to log the results of the scan or if you have a problem with a scan. This option is disabled by default.

**Note:** The Set Debug Mode option must be used only for debugging purposes because it needs a large amount of disk space for the file or files that it generates. Only AT&T Cybersecurity Technical Support should review these files. You can contact this department for more information.

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

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

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

   b. Set the interval options for the increment.

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

   ![Schedule Example]

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

   ![Schedule Example]

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

   c. Set the start time.

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

11. Click **Save**.
The job now displays in the job scheduler list.

To schedule an authenticated asset group scan job from the Job Scheduler page:

1. Go to **Settings > Scheduler** to open the Job Scheduler page.
2. In the left navigation panel, click **Asset Group Scans**.
3. Click **Create Scan Job**.
4. The Schedule New Job dialog box opens.

#### Schedule New Job

**Name**

Name

**Description**

Optional

**Action Type**

Authenticated Asset Scanner

**Schedule**

Day

- Every 1 day(s)
- Every weekday

Start time: **00** — **00** **UTC Time Zone**

1. Enter a name for identifying the job.
2. (Optional.) Enter a description.
3. In the Action Type field, select **Authenticated Asset Scanner**.
4. Select a sensor in case you have more than one installed.
5. In the App Action field, Asset Group Scan is the default option.
6. In the Asset Group field, you can either enter the asset group name or browse asset groups.
7. In the Schedule section, specify when USM Anywhere runs the job:
   a. Select the increment as **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

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

   b. Set the interval options for the increment.

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

   ![Schedule example](image)

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

   ![Schedule example](image)

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

   c. Set the start time.

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

8. Click **Save**.

The job now displays in the job scheduler list.

**Scheduling User Discovery Jobs from the Job Scheduler Page**

USM Anywhere provides a simple way to enable scheduled user scans for user behavior analytics (UBA). Your USM Anywhere instance includes preconfigured scans for each of the user sources UBA supports.
User Behavior Analysis Standard Jobs

There are several apps in USM Anywhere that support the creation of scheduled jobs for user behavior monitoring.

Amazon Web Services

If you have a deployed Amazon Web Services (AWS) Sensor, the AWS Sensor app provides support for the predefined user discovery jobs that USMAnywhere uses to monitor AWS Identity and Access Management (IAM) activity. You can also use the app to define custom jobs.

Azure

If you have a deployed Microsoft Azure Sensor, the Azure Sensor app provides support for the predefined Azure Active Directory (AD) user discovery jobs that USM Anywhere uses to monitor your Azure AD users, either as an actor in the Azure cloud or as an identity provider. You can also use the app to define custom jobs.

The AWS user discovery job is enabled by default and runs every 20 minutes to collect AWS users. See Azure Log Discovery and Collection in USM Anywhere in the USM Anywhere Deployment Guide for more information about jobs for the Azure Sensor app.

You can verify that your app is properly configured to collect user data by viewing the app status.
If you are using Microsoft Active Directory to authenticate users in your environment, the Azure AD Sensor app provides support for the predefined user discovery job that scans for both assets and users authenticated via Microsoft Active Directory.

You can execute a new Microsoft Active Directory scan either from the Getting Started Wizard during your sensor's deployment, or at any time from the sensor details page. In addition, you can schedule a custom job to collect users regularly.

See Running Active Directory Scans in the USM Anywhere Deployment Guide for more information about jobs for this app.
If you are using Okta in your environment to authenticate users, the Okta Sensor app provides support for the predefined user discovery job that scans for users authenticated via Okta.

**Collect Okta Users**

**SCHEDULE PARAMETERS**

- SENSOR: USMA-Sensor-GCP
  - Google Cloud Platform

**SCHEDULE HISTORY**

<table>
<thead>
<tr>
<th>EVENT ACTION</th>
<th>EVENT NAME</th>
<th>FINISHED</th>
<th>FINISHED RELATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OktaUsersCollector</td>
<td>This job (OktaUsersCollector) has failed: The configuration (org, API-key) inserted is incorrect</td>
<td>Tue, Apr 21 2020, 02:00 PM</td>
<td>14 minutes ago</td>
</tr>
</tbody>
</table>

You can confirm your Okta app is configured to collect user data by checking the app status.

---

If you are using Microsoft Office 365 in your environment to authenticate users, the Office 365 Sensor app provides support for the predefined user discovery job that scans for users authenticated via Office 365.

**Office 365**

**SCHEDULE PARAMETERS**

- SENSOR: AWS-Sensor
  - AWS

**SCHEDULE HISTORY**

You can confirm your Office 365 app is configured to collect user data by checking the app status.
Note: Because of the nature of Google G Suite scans, no preconfigured scan is available for G Suite users.

If you are using Google G Suite in your environment to authenticate users and would like to set up a scheduled job to discover them, you must create a new job for that purpose.

To configure a scheduled job to discover G Suite users, use the following values:

- **Name**: An identifying name for the new job
- **Description**: A description of the new job
- **Action Type**: G Suite
- **App Action**: Find G Suite users
- **Domain**: The domain this job will scan
- **Schedule**: The frequency with which this scan job will run (most scan jobs run every 20 minutes)

See USM Anywhere Scheduler for detailed instructions on how to create new scheduled jobs.

G Suite

Important: You must have a privileged GCP user account for your user discovery jobs to run successfully.

If you are using Google Cloud Platform (GCP) in your environment to authenticate users, the GCP Sensor app provides support for the predefined user discovery job that scans for users authenticated via GCP.
USM Anywhere provides a simple way to include scans for scheduling using its web user interface (UI). Go to the Job Scheduler page at Settings > Scheduler and click Log Collection to view a list of all jobs that are defined in your USM Anywhere environment and to manage the jobs that are scheduled to run in your environment.

Depending on your deployed sensor, you can collect different kind of logs:

- Azure Log Discovery and Collection in USM Anywhere
- AWS Log Discovery and Collection in USM Anywhere

AWS Log Discovery and Collection in USM Anywhere

Amazon Web Services (AWS) customers have access to service-specific log files to gain insight into how each AWS service is operating. In addition to application logs, AWS services generate various log files in different formats. With a deployed AWS Sensor, USM Anywhere can collect both logs from AWS, but the procedures are slightly different:

- Use a predefined scheduler job
  
  USM Anywhere can automatically discover AWS CloudTrail logs, the Amazon Simple Storage Service (S3) access logs, and some Amazon CloudWatch logs when they are enabled within your AWS account. There are predefined scheduler jobs in USM Anywhere to collect these logs but they are disabled by default. Go to Settings > Scheduler > Log Collection for the full list. You need to enable each job based on which log you want to collect. See Collect AWS CloudTrail Logs on an AWS Sensor, Collect Amazon S3 Access Logs and Collect ELB Access Logs for more information.

- Use a customer-defined scheduler job
  
  If none of the predefined jobs collect from your log location, you can create a new job under Settings > Scheduler > Log Collection. Depending on where your logs are stored, USM Anywhere provides two ways to collect them:
**Amazon CloudWatch Logs:** If you choose to use Amazon CloudWatch Logs in your AWS environment, USM Anywhere can collect CloudWatch logs directly. See Collect AWS CloudWatch Logs on an AWS Sensor for more information. For example, you can collect the Amazon Virtual Private Cloud (VPC) flow logs using this method.

**Amazon S3 bucket:** If you choose to store logs in an Amazon S3 bucket instead, USM Anywhere can also collect logs directly from an Amazon S3 bucket. See Collect Other Logs from an Amazon S3 Bucket for more information.

---

### Configure Amazon GuardDuty for the AWS Sensor

You can leverage your Amazon GuardDuty service within the AWS Sensor to translate the raw log data into normalized events for analysis.

Amazon GuardDuty service is automatically detected when a new AWS Sensor is deployed. However, it still needs to be enabled for USM Anywhere to receive information from it.

**To enable Amazon GuardDuty for your AWS Sensor**

1. Go to **Settings > Scheduler**.
2. Search for **GuardDuty** in the Job Scheduler **Filter By** field.
3. In the row for the GuardDuty job, click **v** icon.

---

### Collect AWS CloudTrail Logs on an AWS Sensor

Amazon Web Services (AWS) CloudTrail provides a complete audit log for all actions taken with the Amazon API, either through the web user interface (UI), the AWS Command Line Interface (CLI), or an AWS software development kit (SDK). Ongoing monitoring of this log gives you visibility of end user and automated actions in your environment. This helps you quickly detect abuse, such as a user trying to make changes to an AWS account that are inconsistent with their privileges.

USM Anywhere automatically detects AWS CloudTrail and retrieves your AWS CloudTrail logs across all regions within a single AWS account. USM Anywhere also provides you the credentials to securely access your AWS CloudTrail logs. When a new trail is detected, a new job is automatically created and enabled to capture the logs in that trail. Similarly, if a trail is deleted, the existing job that was previously collecting logs is automatically deleted.

As the AWS Sensor collects this raw log data, USM Anywhere uses its AWS CloudTrail data source to normalize the data and generate meaningful events. Depending on the size and activity in your AWS account, this log collection can produce an excessive number of events. See Managing Collected CloudTrail Event Logs for a list of possible CloudTrail events. Similarly, if your AWS instance includes organizations, you may create a trail that will log all events for any AWS accounts assigned to an organization.

**Note:** If you choose not to enable AWS CloudTrail, USM Anywhere processes all stored logs at initial startup. See the Amazon documentation for information about enabling AWS CloudTrail. After that initial processing, log collection jobs run every five minutes to ensure that logs are captured and can generate meaningful events in a timely manner.
Note: Sometimes you may see that the CloudTrail events in USM Anywhere display a different username compared to the raw log. This is because CloudTrail provides different types of user identities, one of which is **AssumedRole**. When the user identity type is set to AssumedRole, it means that the user credential is temporary and the username you see in the raw log is not the actual username. See [Amazon documentation](#) for more information.

### To enable AWS CloudTrail for your AWS Sensor

1. Go to **Settings > Scheduler**.
2. Search for **CloudTrail** in the Job Scheduler **Filter By** field.
3. In the row for the CloudTrail job, click the ✔️ icon to enable the AWS CloudTrail jobs.

   This turns the ✔️ icon green.

---

**Collect Amazon CloudWatch Logs**

Amazon CloudWatch Logs monitors applications and systems using log data, aggregating and storing application logs. CloudWatch Logs is useful because you can easily configure it to process additional metadata with the log files.

**Important:** If you choose to enable CloudWatch Logs in your Amazon Web Services (AWS) environment, you should make sure that you are not collecting more data than you need because this service incurs AWS costs based upon usage. See the [CloudWatch pricing information](#) to plan and configure your usage.
If not already done, install and configure the Amazon CloudWatch agent to collect logs from Amazon Elastic Compute Cloud (EC2) instances. See Amazon documentation for instructions.

USM Anywhere provides some CloudWatch log collection jobs out of the box, but they are disabled by default. You can enable them under Settings > Scheduler. When enabled, these jobs monitor certain log groups and collect logs from CloudWatch every five minutes. You must configure your CloudWatch agent to use these log group names and to keep the log types the same within a given log group.

### USM Anywhere Log Collection Jobs and CloudWatch Log Groups

<table>
<thead>
<tr>
<th>USM Anywhere Log Collection Job Name</th>
<th>CloudWatch Log Group Name</th>
<th>Default File Path</th>
<th>Date Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudWatch - Apache-Access-Logs</td>
<td>Apache-Access-Logs</td>
<td>/var/log/apache2/access.log</td>
<td>%d/%b/%Y:%H:%M:%S</td>
</tr>
<tr>
<td>CloudWatch - Linux-Audit-Logs</td>
<td>Linux-Audit-Logs</td>
<td>/var/log/audit/audit.log</td>
<td>Use the default</td>
</tr>
<tr>
<td>CloudWatch - Linux-Auth-Logs</td>
<td>Linux-Auth-Logs</td>
<td>/var/log/auth.log</td>
<td>%b %d %H:%M:%S</td>
</tr>
<tr>
<td>CloudWatch - Osquery-Logs</td>
<td>OSQuery-Logs</td>
<td>/var/log/osquery/osqueryd.results.log</td>
<td>Use the default</td>
</tr>
</tbody>
</table>

If you want to collect logs from other log groups, ensure that all streams in the same group are of the same type so that USM Anywhere can use a designated data source to parse the collected raw log data. You can then set up a CloudWatch log collection job for each log group.

#### To create a new CloudWatch log collection job

1. Go to Settings > Scheduler.
2. In the left navigation menu, click Log Collection.

   **Note:** You can use the Sensor filter at the top of the list to review the available log collection jobs on your AWS Sensor.

3. Click Create Log Collection Job.

   **Note:** If you have recently deployed a new USM Anywhere Sensor, it can take up to 20 minutes for USM Anywhere to discover the various log sources. When it discovers the logs, you must manually enable the AWS log collection jobs you want before the system collects the log data.
The Schedule New Job dialog box opens.

1. 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.

2. In the Action Type option, select Amazon Web Services.

3. In the App Action option, select Monitor CloudWatch.

USM Anywhere™
User Guide
4. Enter the **Region Name**, **Group Name**, and **Stream Name** information for your AWS account. Region name can be an asterisk (*) to monitor all regions for a given group.

5. In Source Format, select either of the following log formats:

- **syslog**: All messages transmitted to USM Anywhere are processed with the assumption that they are syslog formatted. When you choose syslog as the source format, the data source selection is bypassed and USM Anywhere uses the auto-detect hints from the data sources to match the incoming messages to the correct data source.

- **raw**: Use for non-syslog formatted data.

If you select this option, you must choose the data source that USM Anywhere will use to parse all of the streams in the group. For example, to collect Amazon Virtual Private Cloud (VPC) flow logs, select the **VPC Flow Logs** data source.
Important: If a group contains streams of mixed log formats, USM Anywhere parses all of them with the data source that you chose, which produces undesired results. In this case, you need to configure CloudWatch to separate the streams into different groups so that each contains only a single log type that can be mapped to the correct data source.

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

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

   b. Set the interval and options for the increment.
   The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.
Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.

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

c. Set the start time.

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

7. Click **Save**.

   USM Anywhere detects any enabled jobs with the same configuration and asks you to confirm before continuing. This is because having two jobs with the same configuration generates duplicate events and alarms.

**Collect Amazon S3 Access Logs**

Amazon Simple Storage Service (S3) is object storage with a simple web service interface that you can use to store and retrieve any amount of data from anywhere on the web. Organizations running an Amazon Web Services (AWS) environment typically use it as the primary storage for their cloud-native applications, as a bulk repository, as a target for backup and recovery, and as a long-term archive location.

When enabled, Amazon S3 can provide complete access logs for all actions taken in an Amazon S3 bucket. This gives you insight into who is accessing the data, and what actions are being taken. See Amazon's documentation to learn how to enable S3 access logging.

**Note:** In AWS, you must enable Amazon S3 access logging in every Amazon S3 bucket that you want to monitor.

With a deployed AWS SNV sensor, USM Anywhere automatically discovers the Amazon S3 access logs when you have enabled them within your AWS account. All you need to do is to enable the log collection job in USM Anywhere.

**To enable Amazon S3 access logs collection in USM Anywhere**

1. Go to **Settings >> Scheduler**.
2. In the left navigation pane, click **Log Collection**.
3. Locate the **Discover S3 buckets** job and click the icon.
This turns the icon green (✅). To disable an already-enabled job, toggle the icon to its original status.

After you have enabled log collection, USM Anywhere automatically discovers your Amazon S3 access logs every 20 minutes. They will now begin generating events and you can see them in the Amazon S3 Dashboard.

Collect ELB Access Logs

Elastic Load Balancing (ELB) is an important feature in Amazon Web Services (AWS) because it automatically distributes incoming application traffic across multiple targets. AWS ELB access logs provide insight into who is accessing your web resources. They also help you identify common abuse patterns and use of automated hacking tools such as web application scanners.

USM Anywhere supports log discovery in two types of load balancers:

- **AWS Application Load Balancer**: You must enable Application Load Balancer logs for every AWS ELB that you want to monitor. See the Amazon documentation to learn how to enable Application Load Balancer access logging in AWS.

- **AWS Classic Load Balancer**: You must enable Classic Load Balancer logs for every AWS ELB that you want to monitor. See the Amazon documentation to learn how to enable Classic Load Balancer access logging in AWS.

Collecting AWS Application Load Balancer Access Logs

Once you have enabled Application Load Balancer access logging in AWS, you must also configure a scheduled job to monitor the Amazon Simple Storage Service (S3) bucket for the AWS Application Load Balancer. Only after this has been completed will USM Anywhere be able to automatically discover your ELB access logs.

To create an AWS Application Load Balancer access log collection in USM Anywhere

1. Go to Settings > Scheduler.
2. Click New Job.
3. Configure your new scheduled job to collect access logs
   - **Action Type**: Amazon Web Services
   - **App Action**: Monitor S3 Bucket
   - **Bucket Name**: The name of the S3 bucket you want to monitor
Collecting AWS Classic Load Balancer Access Logs

The AWS Sensor automatically detects Classic Load Balancer access logs after you have enabled them in AWS. After they're enabled in AWS, all you need to do is to enable the log collection job in USM Anywhere.

To enable AWS Classic Load Balancer access log collection in USM Anywhere

1. Go to Settings > Scheduler.
2. In the left navigation pane, click Log Collection.
3. Locate the Discover Elastic Load Balancer (ELB) job and click the icon.

This turns the icon green ( ). To disable an already-enabled job, toggle the icon to its original status.

After you have enabled log collection, USM Anywhere automatically discovers your AWS Classic Load Balancer access logs every 20 minutes. They will now begin generating events and you can see them in the AWS Load Balancer dashboard.

In addition to the resource-specific logging that Amazon Web Services (AWS) provides, individual applications you run in the AWS environment often generate their own log files. You can forward these logs to an Amazon Simple Storage Service (S3) bucket and configure USM Anywhere to collect logs from that Amazon S3 bucket. USM Anywhere does not restrict the number of logs you can collect, but AWS does set limits on the number of logs it can return in each operation.

For example, to collect logs from AWS Web Application Firewall (WAF), you first need to follow AWS documentation to configure AWS WAF logging to store logs in an Amazon S3 bucket. Then configure a scheduler job in USM Anywhere to collect logs from the bucket.

Note: USM Anywhere accepts any file type when collecting log files. For compressed files, it looks for the file extension .gz, .zip, or .bz2 and uses the standard java.util or Apache Commons library to read the files. All other files are read as plain text.
To collect logs from an Amazon S3 bucket

1. Go to **Settings > Scheduler**.
2. In the left navigation menu, click **Log Collection**.

   **Note:** You can use the Sensor filter at the top of the list to review the available log collection jobs on your AWS Sensor.

3. Click **Create Log Collection Job**.

   - **Note:** If you have recently deployed a new USM Anywhere Sensor, it can take up to 20 minutes for USM Anywhere to discover the various log sources. After it discovers the logs, you must manually enable the AWS log collection jobs you want before the system collects the log data.

   The Schedule New Job dialog box opens.

   - **Note:** The **Schedule New Job** dialog box is not visible in the image.

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. In the Action Type option, select **Amazon Web Services**.

6. In the App Action option, select **Monitor S3 Bucket**.
7. Enter the **Bucket Name** and **Path**.

The bucket name is the name of the Amazon S3 bucket as configured in your AWS account, such as `alienvault-test-0726` in the screenshot below.

The path is the path prefix within the Amazon S3 bucket, such as `sub-folder1` in the screenshot below. This does not include the bucket name.
Logs from the directory and its subdirectories are collected.

If you have selected Elastic Load Balancer (ELB), Application Load Balancer (ALB), or Cloudtrail sources, then you need to use, inside the path field, the same prefix you have introduced in your AWS configuration. If the prefix field is empty in your AWS configuration, then you must leave the path field inside USM Anywhere empty.

8. In Source Format, select either of the following log formats:
   - **syslog**: Standard format for transmitting log data to USM Anywhere.
   - **raw**: Use for non-syslog formatted data.

9. In the Schedule section, specify when USM Anywhere runs the job:
   a. Select the increment as **Minute, Hour, Day, Week, Month, or Year**.
   
   **Warning**: After a frequency change, monitor the system to check its performance. For example, you can check the system load and CPU. See **USM Anywhere System Monitor** for more information.

   b. Set the interval options for the increment.

   The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.
Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.

10. Click **Save**.

USM Anywhere detects any enabled jobs with the same configuration and asks you to confirm before continuing. This is because having two jobs with the same configuration generates duplicate events and alarms.

11. In the AWS console, restart the AWS Sensor instance so that it detects the new configuration. You can confirm that the scheduled job is collecting logs by going back to **Settings > Scheduler > Log Collection** and expanding the job you’ve created. Each log collection event will be listed under Schedule History.

### Moving Logs from an Amazon EC2 Instance to an Amazon S3 Bucket

In Amazon Elastic Compute Cloud (EC2), it can be difficult to create direct network connections between isolated parts of your environment. Amazon S3 provides a convenient way to move application logs from an Amazon EC2 instance to an Amazon S3 bucket. Amazon S3 buckets are used to store objects that consist of data and metadata that describes the data. You then configure the AWS Sensor to retrieve and process the log files.

You’ll want to synchronize logs from your instance with an Amazon S3 bucket. There are multiple ways to do this. The easiest method is to use the AWS Command Line Interface (CLI) as documented by Amazon. You then create a script similar to the following example and configure it to run periodically as a cron job.

```
aws s3 sync "<path_to_log>" "S3://<bucket_name>/<storage_path>/
```

### Azure Log Discovery and Collection in USM Anywhere

With a USM Anywhere Sensor deployed in your Microsoft Azure environment, referred to as the Azure Sensor, USM Anywhere can discover and collect logs in two different ways.

An Azure Sensor is pre-configured to automatically discover and collect these types of Azure resource logs (previously referred to as diagnostic logs):

- Azure Monitor (Insight)
- Azure Security Alerts
- Azure Internet Information Services (IIS) logs
- Azure SQL Server logs
- Azure Web Apps logs
- Azure Windows logs

See [Collect Azure Resource Logs](#) for more information.
Furthermore, if you stream data to Azure Event Hubs, you can connect an Azure Sensor to your event hub and collect the following logs:

- Azure Active Directory (AD) logs, including audit logs and sign-in logs
- Azure Monitor logs
- Azure SQL Database logs
- Microsoft Defender Advanced Threat Protection (ATP) logs

See Collect Logs from Azure Event Hubs for more information.

### Collect Azure Resource Logs

Microsoft Azure resource logs (previously referred to as diagnostic logs) provide insight into operations performed within an Azure resource, such as Microsoft Azure Internet Information Services (IIS) or Microsoft Azure SQL Server. USM Anywhere discovers and collects these logs through the Azure APIs. A USM Anywhere Sensor deployed in your Azure environment is preconfigured to automatically discover logs from your Azure storage account. You can enable or disable the predefined jobs from the Azure Sensor Setup Wizard (see Azure Log Collection) or within the USM Anywhere scheduler (see USM Anywhere Scheduler).

To supplement the default log location or to add log collection for Microsoft Azure Web Apps, you can create custom log collection jobs that operate through the Azure Sensor app.

**Note:** What an Azure log job collects depends on whether you granted contributor permissions to one of your resources or to your entire Azure subscription for the USM Anywhere application. Depending on the Azure credentials configured for the deployed Azure Sensor, the sensor could have access to individual resource groups or the whole subscription. See Creating an Application and Obtaining Azure Credentials for more information.

### Microsoft Azure Monitor (Insight)

Microsoft Azure Monitor (formerly Azure Insights) provides base-level infrastructure metrics and logs for most services in Azure. It helps you to track user activities within an Azure subscription, including when users log on, deploy or shut down virtual machines (VMs), and more. Through the Microsoft Azure Monitor Representational State Transfer (REST) API, USM Anywhere captures those logs and creates events.

You need to perform a specific configuration of Azure Monitor in the Azure console for USM Anywhere to collect the Azure-related logs. You need to enable the archive to a storage account option on the Azure subscription, which then enables USM Anywhere to automatically detect and create a job for the Azure-related jobs. When you complete the Log Collection step for your Azure Sensor setup, you can enable this default job, which runs every 20 minutes.
You can also enable or disable this default job in the USM Anywhere Scheduler page. When you select the job in this page, you can review the history for the scheduled job.

### Job Scheduler

Jobs collect information about your environment and execute actions based on a repeating schedule. [Learn more about scheduling jobs](#).

<table>
<thead>
<tr>
<th>SENOR</th>
<th>APP</th>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>SCHEDULE</th>
<th>LAST RUN</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>USM-Azure-Sensor</td>
<td>Azure</td>
<td>AT&amp;T Cybersecurity For...</td>
<td>Checks for new Azure Insight logs and processes them</td>
<td>Every 5 minutes</td>
<td>2 minutes ago</td>
<td>off</td>
</tr>
<tr>
<td>USM-Azure-Sensor</td>
<td>Azure</td>
<td>Azure</td>
<td>Checks for new Azure Insight logs and processes them</td>
<td>Every 5 minutes</td>
<td>2 minutes ago</td>
<td>on</td>
</tr>
</tbody>
</table>

### Process Azure Insight Logs

#### Schedule Parameters

<table>
<thead>
<tr>
<th>SENSOR</th>
<th>USM-Azure-Sensor</th>
</tr>
</thead>
</table>

#### Schedule History

<table>
<thead>
<tr>
<th>EVENT ACTION</th>
<th>EVENT NAME</th>
<th>FINISHED</th>
<th>FINISHED RELATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>processAzureInsightLogs</td>
<td>Azure Insight Events: Processed 84 new events.</td>
<td>Fri, Feb 05, 2021, 01:05 PM</td>
<td>a few seconds ago</td>
</tr>
<tr>
<td>processAzureInsightLogs</td>
<td>Azure Insight Events: Processed 0 new events.</td>
<td>Fri, Feb 05, 2021, 01:00 PM</td>
<td>6 minutes ago</td>
</tr>
<tr>
<td>processAzureInsightLogs</td>
<td>Azure Insight Events: Processed 0 new events.</td>
<td>Fri, Feb 05, 2021, 12:55 PM</td>
<td>11 minutes ago</td>
</tr>
</tbody>
</table>
Microsoft Azure Security Center is an Azure service that continuously monitors your Azure environment and applies analytics to automatically detect a wide range of potentially malicious activity. It surfaces these detections as security alerts. Security Center performs this function by collecting data from your VMs, which is enabled for all VMs in your subscription by default. You can also customize this data collection in the Security Center policy.

You do not need to perform a specific configuration of the Azure Security Center alerts in the Azure console to be able to collect these logs. USM Anywhere automatically detects these logs and creates a job for Azure Security Center alerts logs. When you complete the Log Collection step for your Azure Sensor setup, you can enable this default job, which runs every 20 minutes.

You can also enable or disable this default job in the USM Anywhere Scheduler page. When you select the job in this page, you can review the history for the scheduled job.

### Job Scheduler

Jobs collect information about your environment and execute actions based on a repeating schedule. Learn more about scheduling jobs.

<table>
<thead>
<tr>
<th>SENSOR</th>
<th>APP</th>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>SCHEDULE</th>
<th>LAST RUN</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>USM-Azure-Sensor Azure</td>
<td>AT&amp;T Cybersecurity For...</td>
<td>at</td>
<td>Checks for new Azure IIS logs and processes them</td>
<td>Every day</td>
<td>2 years ago</td>
<td>✗</td>
</tr>
<tr>
<td>USM-Azure-Sensor Azure</td>
<td>Azure Inspect</td>
<td>Azure</td>
<td>Checks for new Azure Security Alerts and processes them</td>
<td>Every 5 minutes</td>
<td>2 minutes ago</td>
<td>✓</td>
</tr>
<tr>
<td>USM-Azure-Sensor Azure</td>
<td>Azure Security Alerts</td>
<td>Azure</td>
<td>Checks for new Azure IIS logs and processes them</td>
<td>Every 5 minutes</td>
<td>2 minutes ago</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Process Azure Security Alerts

**SCHEDULE PARAMETERS**

<table>
<thead>
<tr>
<th>SENSOR</th>
<th>USM-Azure-Sensor Azure</th>
</tr>
</thead>
</table>

**SCHEDULE HISTORY**

<table>
<thead>
<tr>
<th>EVENT ACTION</th>
<th>EVENT NAME</th>
<th>FINISHED</th>
<th>FINISHED RELATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>processAzureSecurityAlerts</td>
<td>Collecting Azure Security alerts.</td>
<td>Fri, Feb 05, 2021, 05:05 PM</td>
<td>a few seconds ago</td>
</tr>
</tbody>
</table>

### Azure IIS Logs

**Warning:** If there are network restrictions in your environment restricting access to the storage account, those restrictions must allow access to the sensor.

For individual VMs running IIS with Azure diagnostics enabled, you can designate storage for the IIS logs. USM Anywhere automatically detects these logs in Azure Storage containers and Azure software development kits (SDKs). For each Azure Storage container locations with Azure IIS logs that it detects, USM Anywhere creates a default log collection job. When you complete the Log Collection step for your Azure Sensor setup, you can enable these default jobs, which run every five minutes.

**Note:** This type of IIS implementation is different than Azure Web Apps, which is a platform service and uses a different logging configuration. See Azure Web Apps Logs for information about collecting logs for web apps.

You can also enable or disable this default job in the Job Scheduler. When you select the job in this page, you can review the history for the scheduled job. You could choose to disable this default job based on the IIS log locations that USM Anywhere discovers, and create a custom Azure IIS log collection job for a location that you specify.
When you configure the new job, set the App Action option to **Process Azure IIS Logs**. You must also specify the **Resource Group**, **Storage Account**, and **Blob Container** for the custom log collection job. See [Create a New Azure Log Collection Job](#) for more information about scheduling an Azure log collection job.

**Azure SQL Server Logs**

For individual VMs running an Azure SQL Server with Azure diagnostics enabled, you can designate storage for the IIS logs. You must configure this to use Microsoft Azure Table storage. To simplify the tracking of related security issues, USM Anywhere treats the SQL service as an asset, and maps events and other security issues directly with the SQL service. When it detects Azure Table storage locations with Azure SQL Server logs, USM Anywhere creates a default log collection job for each. When you complete the **Log Collection step** for your Azure Sensor setup, you can enable these default jobs, which run every five minutes.

**Important:** The Azure SQL Server job is deprecated. Use the Event Hub Integration to collect Azure SQL Server logs. See [Collect Logs from Azure Event Hubs](#) for more information.

---

**USM Anywhere™ User Guide**
If you want to supplement this automatic Azure log collection in USM Anywhere, you can create an additional Azure SQL Server log collection job.

When you configure the new job, set the App Action option to Process Azure SQL Server Logs. You must also specify the Resource Group, Storage Account, and Table Container for the custom log collection job. See Create a New Azure Log Collection Job for more information about creating a new Azure log collection job.

Warning: If there are network restrictions in your environment restricting access to the storage account, those restrictions must allow access to the sensor.

Important: When configuring Azure Web Apps logs, you must use the World Wide Web Consortium (W3C) format and select the following fields:

date, time, s-sitename, cs-method, cs-uri-stem, cs-uri-query, s-port, cs-username, c-ip, cs(User-Agent), cs(Cookie), cs(Referer), cs-uri-scheme, sc-status, sc-win32-status, sc-bytes, cs-bytes, time-taken

Unlike the other supported Azure logs, the USM Anywhere Sensor does not perform an automatic discovery job for Web Apps to look for the storage location. If you want USM Anywhere to collect the log data for your Web Apps, you must create a new log job and specify the storage location parameters.
When you configure the new job, set the App Action option to **Process Azure Web Apps Logs**. You must also specify the Resource Group, Storage Account, and Blob Container for the custom log collection job. See Create a New Azure Log Collection Job for more information about creating a new Azure log collection job.

**Warning:** If there are network restrictions in your environment restricting access to the storage account, those restrictions must allow access to the sensor.

For individual VMs running Microsoft Windows with Azure diagnostics enabled, Azure stores the Windows Events logs by default. USM Anywhere automatically detects these logs through Azure APIs and Azure SDKs. When it detects Azure Storage container locations with Azure Windows logs, USM Anywhere creates a default log collection job for each. When you complete the Log Collection step for your Azure Sensor setup, you can enable these default jobs, which run every five minutes.

If you want to supplement this automatic Azure log collection in USM Anywhere, you can create an additional Azure Windows log collection job.
When you configure the new job, set the App Action option to **Process Azure Windows Logs**. You must also specify the Resource Group, Storage Account, and Blob Container for the custom log collection job. See **Create a New Azure Log Collection Job** for more information about creating a new Azure log collection job.

**Enable Diagnostics for Azure Web Apps**

1. Log in to your account at [https://portal.azure.com/](https://portal.azure.com/).
2. Go to your Azure Web App and select **Settings** > **Diagnostics logs**.
3. For **Application Logging (Blob)**, click **On** and set the parameters:
   - Set the **Level** for the logging.
   - For **Storage Settings**, click **+** and select the **Storage Account** and **Container**.
     *This is the storage account and container that Azure will use to store logs for the Web App. Make note of this information because you will need it to set up a log collection job in USM Anywhere. You can click **+ Storage Account** to create a new storage account or container, or select an existing one.*
4. For Web server logging, select **Storage**.
5. Click **Storage Settings** and select the same storage account and container that you set for the application logging.

6. Click **Save**.

**Create a New Azure Log Collection Job**

USM Anywhere automatically creates log collection jobs for Azure Monitor and security logs. It also creates jobs for Internet Information Services (IIS), Microsoft Azure SQL Server, and Microsoft Windows if it detects storage locations for these log types. When you complete the **Log Collection step** for the Azure Sensor, you can enable these default jobs. You can review these jobs and their details in the **Scheduler** but you cannot modify the parameters of these default jobs.

**Note:** What an Azure log job collects depends on whether you granted contributor permissions to one of your resources or to your entire Azure subscription for the USM Anywhere application. Depending on the Azure credentials configured for the deployed Azure Sensor, the sensor could have access to individual resource groups or the whole subscription. See **Creating an Azure Application and Obtaining Azure Credentials** for more information.

To supplement the automatic Azure log collection in USM Anywhere and to set up log collection for Azure Web Apps, add new Azure log collection jobs.

**Important:** Before your scheduled jobs can collect logs, you may also have to perform specific configuration steps outside of USM Anywhere in your environment. See **Collect Azure Resource Logs** for detailed descriptions of the configuration steps your environment might require.
To schedule a new job to collect and process Azure logs:

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 Azure Sensor.

3. Click **Create Log Collection Job**.

   - A job list is displayed.

   **Note:** If you have recently deployed a new USM Anywhere Sensor, it can take up to 20 minutes for USM Anywhere to discover the various log sources. After it discovers the logs, you must manually enable the Azure log collection jobs you want before the system collects the log data.

The Schedule New Job dialog box opens.

4. Enter the name and description for the job.

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

5. In the Select App option, select **Azure**.

6. In the App Action option, select the action for Azure log type that you want to schedule for collection.
See Collect Azure Resource Logs to review details about the Azure log types that USM Anywhere can collect.

7. Depending on the selected app action (log type), specify the Resource Group, Storage Account, and Container for the logs.

You can obtain this information by logging into the Azure console and reviewing the configuration for your diagnostic and storage resources.

**Note:** For Azure IIS logs, Azure Web Apps logs, and Azure Windows logs, you must specify a binary large object (BLOB) container used for the log storage. For the Azure SQL Server log type, you must specify the table container used for the log storage.

The Azure SQL Server job is deprecated. Use the Event Hub Integration to collect Azure SQL Server logs. See Collect Logs from Azure Event Hubs for more information.

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

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

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

b. Set the interval options for the increment.

The selected increment determines the available options. For example, on a weekly increment, you can select the days of the week to run the job.
Or on a monthly increment, you can specify a date or a day of the week that occurs within the month.

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

c. Set the start time.

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

9. Click Save.

Collect Logs from Azure Event Hubs

Microsoft Azure Event Hubs is a data and event processing service for Microsoft Azure. The integration between USM Anywhere and Azure Event Hubs enables the Azure Sensor to receive and process information from an event hub so that you can manage them in your USM Anywhere environment.

Warning: To process and display the custom events received from the Azure Event Hubs as generic events, USM Anywhere needs these custom events in a specific format. The correct format is an array as a value of a "records" key in JSON format. For example `{ "records": [ {<event-content>} ] }`.

Important: Be sure to review the Azure requirements page for any environmental requirements specific to Azure Event Hubs before implementing the streaming of your logs to Azure Event Hubs.

The Azure Sensor can process different types of logs sent through Azure Event Hubs, including but not limited to the following:

- Azure Active Directory (AD) logs, including audit logs and sign-in logs
- Azure Application Gateway logs
- Azure Monitor logs
- Azure SQL Database logs
- Microsoft Defender Advanced Threat Protection (ATP) logs
- Microsoft Intune logs

Stream Logs to Azure Event Hubs

Before configuring the Azure Event Hubs integration in USM Anywhere, you must stream the logs you want to be analyzed to Azure Event Hubs. Make sure to stream your logs to the same event hub, because each Azure Sensor can only collect from a single event hub.
To stream logs to Azure Event Hubs

1. Log in to the Azure portal.
2. Create an event hub. See Microsoft Azure Quickstart: Create an event hub using Azure portal for instructions.
3. Go to the event hub you just created and click Shared access policies in the sidebar.
4. Create or edit a policy, and then select Manage, Send, and Listen. Streaming to Event Hubs requires these permissions.
5. Copy the connection string listed in the policy under Connection string-primary key.

You need to enter this string when configuring the Event Hubs connection in USM Anywhere.

6. Configure streaming for the logs you want to collect. For example:

   **Note:** Make sure to enable Stream to an event hub and select the Event Hub you just created as the destination.

   - **Azure AD logs:** See Stream Azure Active Directory Logs to an Azure Event Hub for instructions from Microsoft.
   - **Azure Application Gateway logs:** See Enable Logging for Application Gateway for instructions from Microsoft.
   - **Azure Monitor logs:** See Create Diagnostic Settings to Send Logs for instructions from Microsoft.
   - **Azure SQL Database logs:** See Set up auditing for your database for instructions from Microsoft. Make sure to select Event Hub as the destination.
   - **Microsoft Defender ATP logs:** See Configure Microsoft Defender ATP to stream Advanced Hunting events to your Azure Event Hubs for instructions from Microsoft.
   - **Microsoft Intune logs:** See Send log data to storage, event hubs, or log analytics in Intune for instructions from Microsoft.

Set Up Azure Event Hubs Connection in USM Anywhere

After completing the initial setup of your Azure Event Hubs, return to your USM Anywhere Sensors page to enable the Azure Event Hubs connection in USM Anywhere.

To enable Azure Event Hubs in USM Anywhere

1. Go to Data Sources > Sensors and open the Azure Sensor.
2. Click the Configurations tab.
3. Complete the three fields:
• **Event Hub Name:** The name of the event hub created during initial setup.

• **Event Hub Connection String:** A string containing unique configuration data about your Azure Event Hubs implementation. This string was discovered during the previous procedure.

• **Event Hub Consumer Group:** The name of your Event Hub consumer group. You can locate this name by opening your Event Hub overview in the Azure portal and scrolling to the bottom of the page.

4. (Optional.) Select **Process generic events** to collect events for which USM Anywhere currently does not have a parser. These events will display as "GENERIC event" under Activity > Events.

5. Click **Save**.

6. Click the **Event Hub** tab to check the connection status and the number of events processed by each data source.

**Viewing Azure Event Hubs Connectivity in USM Anywhere**

The Event Hub tab on the Azure Sensor page provides a glimpse into the health of your sensor's connection to Azure Event Hubs. This page contains the name of your event hub, its connectivity status, and the number of events being processed by USM Anywhere.

**To view your Azure Event Hubs connection**

1. Go to the **Sensors** page and open your Azure Sensor.
2. Click the **Event Hub** tab.

These are the connectivity statuses you may see:

• **Connecting:** Azure Event Hubs is currently connecting to the sensor.

• **Processing:** Azure Event Hubs is successfully connected.

• **Shutting Down:** Azure Event Hubs has begun the shutdown process to allow a different event hub to connect to the sensor.

• **Shutdown:** The sensor is not currently connected to an event hub.

• **Error:** The connection has experienced an error.
Rules Management

Every networked environment generates thousands of logs from assorted systems. USM Anywhere enables you to manage those logs and, through the use of rules, you can prevent and frustrate attacks. The management of the different USM Anywhere rules helps you to make the most of your environment.

Keep in mind that setting up a rule base is an iterative process. That means it happens relatively slowly and needs to be tuned over a period of time. There are always new attacks and new indicators to monitor.

USM Anywhere includes these rules:

- Correlation rules: These are predefined rules, which are developed by AT&T Cybersecurity. See Correlation Rules for more information.
- Orchestration rules: You can create and customize these rules to add specific policies for a particular event or alarm. See Orchestration Rules for more information. These are the orchestration rules:
  - Suppression rules: Use these rules to suppress events or alarms that create noise in your system. See Suppression Rules from the Orchestration Rules Page for more information.
  - Filtering rules: Use these rules to make the sensor drop future events that match the rule. See Filtering Rules from the Orchestration Rules Page for more information.
  - Alarm rules: Use these rules to identify existing and emerging threats. See Alarm Rules from the Orchestration Rules Page for more information.
  - Notification rules: Use these rules to create your own rules and receive notifications. See Notification Rules from the Orchestration Rules Page for more information.
  - Response action rules: Use these rules to respond to an event or an alarm running an AlienApp. See Response Action Rules from the Orchestration Rules Page for more information.
Orchestration Rules

USM Anywhere enables 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.

**Warning:** Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the Contains, Match and Match, case insensitive operators apply to future events and alarms, not to events and alarms received in the current day.

USM Anywhere includes these orchestration rules:

- Suppression rules: See Suppression Rules from the Orchestration Rules Page
- Filtering rules: See Filtering Rules from the Orchestration Rules Page
- Alarm rules: See Alarm Rules from the Orchestration Rules Page
- Notification rules: See Notification Rules from the Orchestration Rules Page
- Response action rules: See Response Action Rules from the Orchestration Rules Page

**Note:** USM Anywhere follows a specific order for applying orchestration rules. See Orchestration Rules Workflow for more information.

The order of the conditions is significant because USM Anywhere follows a specific order when it evaluates the rule conditions, reading them from left to right. If your rule includes the packet_type and plugin_device fields, these should always occur first in the order.

You can also create orchestration rules from the details of an event or alarm. The functionality works the same way and the dialog box is similar when you are creating a rule either from a detail page of an event or alarm or from the settings page.

**Important:** The easiest way to configure an orchestration rule is from the Alarm and the Events details pages. See Creating Notification Rules from the Alarms Page, Creating Alarm Rules from the Events Page, and Creating Notification Rules from the Events Page for more information.

See Example: Creating an Orchestration Rule if you want to see an example of an orchestration rule.
AlienApp™ Orchestration Rules

Some of the AlienApps available in USM Anywhere enable you to automate and orchestrate response actions in third-party security tools, which simplifies and accelerates your threat detection and incident response processes. With a configured integration, these AlienApps include support for app actions in orchestration rules:

- The AlienApp for Carbon Black Endpoint Detection and Response (EDR)
- The AlienApp for Cisco Umbrella
- The AlienApp for Palo Alto Networks PAN-OS

The *USM Anywhere™ AlienApps™ Guide* provides detailed information about creating orchestration rules for a configured AlienApp.

Orchestration Rules Workflow

USM Anywhere follows a specific order for applying orchestration rules:

1. **Filtering rules**: These rules are essential to control the traffic of your events. USM Anywhere does not process nor save events that match a filtering rule.

2. **Suppression rules**: USM Anywhere saves the events that match a suppression rule, but does not correlate these suppressed events. By default, USM Anywhere hides these suppressed events. If you want to see these events, click **Suppressed** in the Search & Filters area. The table displays suppressed events along with all events. See [To only display the suppressed events](#) if you want to display just the suppressed events.

3. **Notification, alarm, and response action rules**: USM Anywhere processes and correlates all events that match one of these rules.

This diagram summarizes the workflow of orchestration rules:
Orchestration Rules Best Practices

USM Anywhere enables you to create and customize your own orchestration rules to add specific policies for a particular event or alarm. A rule is made of these three items:

- An alarm or event data that details the item (see Viewing Alarm Details and Viewing Event Details for more information).
- The match item (see Operators in the Orchestration Rules for more information).
- The match criteria value.

**Note:** All rules should have at least two match criteria for efficient processing.

Recommendations for Creating an Orchestration Rule

Use these recommendations when creating an orchestration rule:

- If `packet_type == log` is used in the rule, the second rule match criteria must be the data source plugin name (`plugin == ‘plugin_name’`) used to normalize the event details. This enhances rules processing efficiency. If possible, the third match criteria should be the event name (`event_name == ‘<event_name>’`).

- Avoid using the case-insensitive version of rule match operators. Some rule fields do not accept this as a valid operator and will return a rule status warning when your rule is created.

**Note:** Correlation lists are not valid for use with filtering rules.

- Rules operate by using Boolean logic, and are processed from left to right of the formulated rule data. Use the most restrictive match criteria up front to minimize rules processing for failed matches. If your rule includes the `packet_type` and `plugin_device` fields, these should always occur first in the orchestration rule.

- Minimize the number of match criteria used for simplicity.

- Consolidate rules into a smaller number of rules.

- In order of precedence, the `equals (==)` operator is better than the `contains` operator.

- Avoid using the regular expression (regex) based on the `match (~)` operator, because it is not very efficient and can cause performance issues. Properly formatted rules using the `contains` operator provides equivalent functionality. If this operator is required, make it the last set of criteria in the rule.

- For all rules based on events, do not create a rule format where the first operator in the rule is the `or` operator. All events will validate against the rule. For example, don't do this:

  ```
  (packet_type == “log” OR <any other match criteria>.
  ```
The use of the `or` operator in the rule matches `every` event normalized and causes the rule type to always be processed. For filtering rules, all processed events are deleted or discarded. This action is terminal and all deleted or discarded data by the rule can't be recovered by USM Anywhere.

- Suppression of an event or alarm terminates correlation actions of subsequent rules. This means that suppressed events will not correlate against alarm or notification rules, so alarms and notifications will not be generated. Suppressed alarms will not correlate against alarm notification rules either, so notifications will not be generated.

- The use of filter rules does not reduce processing load on the sensor. Filter rules are only intended to reduce network traffic to the control node and event data storage in the service tier.

All events received via syslog by a sensor are processed to create the full event details of the event. Correlation of filtering rules is done at the last stage of this process, at which time events that match a filter rule are discarded. Events that do not match a filter rule are sent to a sensor back-end process that uploads event information to the control node. To reduce the impact of additional processing of these events on a sensor node, it is important to be specific in configuring what messages are sent from sources such as firewall, network switches, or routers. Configure these devices to filter out unnecessary raw log information at that stage of events.

- An excessive number of orchestration filter rules on a sensor node will have a negative effect on the sensor node's resource usage. Every event processed by a sensor node must be matched up against all filter rules until a rule matches (and, therefore, the event is discarded) or all rules fail to match (in which case the event is post-processed for upload to the control node). All sensors get the same copies of filter rules from the control node regardless of sensor type. The use of the plugin data source name early in the rule helps minimize event processing under these conditions. Combine multiple rules into a single rule to reduce the number of items processed.

- Alarm Suppression rules have limited visibility to the event details of the events that triggered the alarm. Use of event details in match criteria may disable the ability of the rule to validate true. As an example, the use of event packet payload information (`packet_payload contains <some string>`) will not produce a true condition; therefore, the rule will not trigger an alarm suppression.

- All user roles can view the rules page. Users with manager and analyst roles can create, edit, enable, and disable orchestration rules and correlation lists. Orchestration rules and correlation lists can only be deleted by the user who created the rule or the list.

- Keep in mind, when you use the syntax `event_field >> variable` that the event field can't be empty. If the event field is empty, there will be false positives.

**Orchestration Rules Creation**

Before creating an orchestration rule, it is necessary to understand what an orchestration rule is, the different orchestration rules you can create, and how an orchestration rule operates. See Orchestration Rules and Orchestration Rules Workflow before creating an orchestration rule.
There are two ways of creating an orchestration rule:

- From the detail of an alarm or event, select the create rule option.
  
  See Creating Rules from Alarms and Creating Rules from Events for specific information.

- From the orchestration rules page, go to Settings > Rules > Orchestration Rules, click Create Orchestration Rule, and select the rule you want to create.
  
  See Alarm Rules from the Orchestration Rules Page, Filtering Rules from the Orchestration Rules Page, Notification Rules from the Orchestration Rules Page, Response Action Rules from the Orchestration Rules Page, and Suppression Rules from the Orchestration Rules Page for the specific information on each rule.

To create an orchestration rule from an alarm or an event

1. Go to Activity > Alarms or Activity > Events.
2. Locate the alarms or events you want to include in the rule.
3. Click an alarm or event to see its details.
4. Click Create Rule:
   - If you are displaying an alarm, you can choose between a suppression or a notification rule.
   - If you are displaying an event, you can choose between an alarm, filtering, notification, or suppression rule.
5. You have already suggested property values to create a matching condition, but you can add new property values by clicking Add Condition.

   **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

   **Important:** Instead of using the `equals` and `equals`, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

   **Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

6. (Optional.) Click Add Group to group your conditions.

   **Note:** See Operators in the Orchestration Rules for more information.
Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

7. Click **Next**.

Important: A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

8. Enter a name for the rule.

9. (Optional.) Enter a description for identifying this rule.

10. Depending on the selected rule, you should fill in different fields.

11. Modify these two options:

    - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

    - **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

    This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.
In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

12. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### To create an orchestration rule from the orchestration rules page

1. Go to **Settings > Rules > Orchestration Rules**, click **Create Orchestration Rule**, and select the rule you want to create:
   - Suppression Rule (see **Suppression Rules from the Orchestration Rules Page** for more information)
   - Filtering Rule (see **Filtering Rules from the Orchestration Rules Page** for more information)
   - Alarm Rule (see **Alarm Rules from the Orchestration Rules Page** for more information)
   - Notification Rule (see **Notification Rules from the Orchestration Rules Page** for more information)
   - Response Action Rule (see **Response Action Rules from the Orchestration Rules Page** for more information)

2. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.

**Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

**Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

**Important:** Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.
3. (Optional.) Click Add Group to group your conditions.

Note: If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

Note: See Operators in the Orchestration Rules for more information.

Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

4. Click Next.

Important: A dialog box opens if there are warning messages. Click Cancel to review the warning messages, or click Accept to continue creating the rule.

5. Enter a name for the rule.

6. (Optional.) Enter a description for identifying this rule.

7. Depending on the selected rule, you should fill in different fields.

8. Modify these two options:

   • **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
**Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

9. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

### Orchestration Rule Validation

When orchestration rules are active, USM Anywhere inspects and validates them to show you how well the rule is working. The rule status is indicated in a column.

Be sure to check your rule’s validation, and make recommended or necessary changes to optimize the rule based on the validation status. See **Orchestration Rule Validation** for more information.
Orchestration Rules Processing

All orchestration rules, including event filter rules, are processed on the control node. A sensor node will only process orchestration filter rules. Event filter rules are reapplied on the control node because event enrichment for the event on the control node can modify or add to event details with items not found on the sensor node during normalization.

See Orchestration Rules Workflow to learn more about the specific order that USM Anywhere applies to orchestration rules.

Managing Orchestration Rules

USM Anywhere enables you to manage your own orchestration rules. To view orchestration rules, go to Settings > Rules > Orchestration Rules. The All Orchestration Rules page opens. The page displays the list of rules and includes these parts:

- At the top of the page, you can see a banner if there is at least one rule that has errors. This yellow banner is recommended for reviewing and fixing rules with any error. Errors can impact system stability and must be reviewed immediately.
- Below the banner, you can see the filters that you can apply. You can filter by name, by rule status, and by orchestration rule.
- The main part of the page is the list of rules, where each row describes an individual rule. You can enable, disable, edit, and delete a rule. You can also choose a rule by selecting the checkbox to the left of the rule. Select all rules at the same time by selecting the first checkbox in the column. Enable (✓) and disable (✗) rules by using the buttons below the enabled column. You can also see the details of a rule by clicking it. The icon is available for the Event Suppression and Create an Alarm rows.
The following table lists the columns you see on the page.

### Columns on the All Orchestration Rules page

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Rule Status</td>
<td>Status notification of the rule. Each rule is classified by its severity. Values are (in increasing severity): info, warning, and error.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of rule.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Conditions applied by the rule.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Date and time on which that rule has been modified.</td>
</tr>
<tr>
<td>Triggered</td>
<td>Column displays when you apply an all orchestration rules filter. If you have filtered by Alarm rules, the number below the column indicates the times that rule has triggered an alarm. If you have filtered by any other rule, the number indicates the hits value, how often a rule has matched its criteria against an event.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Icons to enable or disable the rule.</td>
</tr>
</tbody>
</table>
Columns on the All Orchestration Rules page (Continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📊</td>
<td>Icons to edit or delete the rule.</td>
</tr>
<tr>
<td>📋</td>
<td>Icon available for the Event Suppression and Create an Alarm rows. Depending on the selected option, the Events List View page or the Alarms List View page opens.</td>
</tr>
</tbody>
</table>

**Orchestration Rules Details**

USM Anywhere provides visibility on how your rules behave. Click any rule on the All Orchestration Rules page to display the details.

**Test of Max**

`{packet_type == 'log' AND plugin == 'Linux BIND'}`

<table>
<thead>
<tr>
<th>Evaluations vs. Hits</th>
<th>Last Hour</th>
<th>Last Day</th>
<th>Last 7 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rules Status**

The rule has not matched for 1 week. Please verify if this rule is still in use or if the rule conditions are properly set.

**Rules History**

<table>
<thead>
<tr>
<th>USER</th>
<th>ACTION</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rule updated</td>
<td>Tue, Nov 02 2021, 01:41 PM CET</td>
</tr>
<tr>
<td></td>
<td>Rule updated</td>
<td>Tue, Nov 02 2021, 01:41 PM CET</td>
</tr>
<tr>
<td></td>
<td>Rule created</td>
<td>Mon, Aug 09 2021, 05:44 PM CET</td>
</tr>
</tbody>
</table>

**Note:** The default time range for the trend chart is 24 hours. You can click Last Hour, Last Day, or Last 7 Days to change the time range.

You can see the following information:
• **Evaluations vs. Hits:** This graph shows the progress of the rule triggers over the last 7 days, 24 hours, or 1 hour.

• **All Systems:** This combo box displays when you have expanded a filtering rule. Choose between the control node or the sensor. Choose the All Systems option if you want to display the data of both control node and sensor.

![Graph showing Evaluations vs. Hits](image)

- **Average Duration:** The rule evaluation's average duration in milliseconds.
- **Evaluations:** How often a rule has been evaluated.
- **Alarms Triggered:** How often the rule has executed the associated action. This number might be different than Hits if the rule has a mute period assigned.

![Important: Field only displays when you have expanded an alarm rule](image)

- **Total Evaluation Rate:** How often the rule is evaluated against the total number of events. Rules are only evaluated if the event contains all the fields specified in the rule criteria, so providing detailed criteria might reduce the ingestion rate and, therefore, improve the performance.

- **Hits:** How often a rule has matched its criteria against an event.
- **Created:** The date of creation and email of the user.
- **Updated:** The data of the update and email of the user.
- **Rules Status:** Status notification of the rule. Each rule is classified by its severity. Values are (in increasing severity): info, warning, and error.
- **Rules History:** This table shows the user who has made an action related with an orchestration rule, the action, and the date of creation.
Orchestration Rules Management
USM Anywhere enables you to manage your own orchestration rules from the All Orchestration Rules page.

To filter orchestration rules by name
1. Go to Settings > Rules > Orchestration Rules.
2. Click the box next to Filter by.
3. Enter your search.

To filter orchestration rules by rule status
1. Go to Settings > Rules > Orchestration Rules.
2. Click the combo box next to Rule Status.
3. Select All Rules, Enabled, or Disabled.

To edit an orchestration rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click Next.
5. Click Save.

To delete an orchestration rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to delete.
3. Confirm by clicking Accept.

To enable an orchestration rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to enable.

To disable an orchestration rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to disable.
To enable all orchestration rules

1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Enable All Rules.

To disable all suppression rules

1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Disable All Rules.
4. Confirm by clicking Accept.

To show triggered alarms rules or suppressed events

1. Go to Settings > Rules > Orchestration Rules to open the All Orchestration Rules page.
2. In the row, click the icon.

This icon is available for the Event Suppression and Create an Alarm rows.

Depending on the selected option, the Events List View page or the Alarms List View page opens. The page includes Rules Name as a filter so that you can see how many alarms or events match the selected rule.

Orchestration Rule Validation

When orchestration rules are active, USM Anywhere inspects and validates them to show how well the rule is working.

The orchestration rule validation process is engaged whenever a new rule is created or an existing rule is updated. Additionally, active rules are validated periodically for the duration of the time they are active. The orchestration rule validation process checks your rule against a set of tests, called rule checks, which evaluate how well your orchestration rule will perform, and checks it for common errors. For example, this validation process keeps you from creating a rule that will collect nothing (or everything).

Note: Any time you create a new rule or edit an existing rule, be sure to review your rule's validation and make recommended or necessary changes to optimize the rule based on the validation status.

For every rule check that your orchestration rule fails, you are shown a status notification, which explains in detail what should be improved in your rule. Each status notification is classified by its severity into four statuses (in increasing severity): ok, info, warning, and error. While an info-level status notification may indicate that optimizing the rule would be useful, a warning-level status notification indicates a more critical problem that should be addressed. An error-level status notification will prevent you from saving the new rule until it is fixed.
Viewing Your Rule’s Validation Status

To view the validation status of your orchestration rules, go to Settings > Rules > Orchestration Rules. The rule’s status is indicated by a column on the Orchestration Rules main page. If you would like to view just the rules that have a specific status, you can filter by validation statuses from the All Orchestration Rules page.

To read a detailed breakdown of your rule’s validation, click the rule. This opens a window listing the details that apply to your rule, with an icon indicating each status notification’s severity. From this view, you can see a clear list of all the changes you can make to optimize your rule. You can also see any changes that are required for your rule to function.
Understanding How Validation Is Assessed and Applied

When more than one validation check applies to an orchestration rule, USM Anywhere considers the most severe of those the rule's validation status. For example, in the screenshot, you can see that a warning, info, and error notifications were all triggered by the "Alarm without Condition" rule, so its overall validation status is error.

The following table shows the list of validation statuses.

Understanding How Validation Is Assessed and Applied

When more than one validation check applies to an orchestration rule, USM Anywhere considers the most severe of those the rule's validation status. For example, in the screenshot, you can see that a warning, info, and error notifications were all triggered by the "Alarm without Condition" rule, so its overall validation status is error.

The following table shows the list of validation statuses.
List of Orchestration Rule Validation Statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO</td>
<td>🔄</td>
<td>There are minor issues in this rule's definition that might affect your rule's operation.</td>
</tr>
<tr>
<td>WARNING</td>
<td>🚨</td>
<td>There are issues in this rule's definition that might negatively impact your system.</td>
</tr>
<tr>
<td>ERROR</td>
<td>X</td>
<td>This rule will present undesired behavior on your system.</td>
</tr>
</tbody>
</table>

Rule Validation Lifecycle

Your rule's validation status will persist as long as the rule checks that apply to it are active. Status checks are either static or dynamic. Static checks evaluate your rule against common mistakes when your rule is first created, while dynamic checks analyze your rule's behaviors and are assessed every 10 minutes while your rule is active.

Both static and dynamic checks show up as status notifications on your orchestration rule.

Static Checks

These checks evaluate your rule against common mistakes such as the presence of a data source or packet type, in addition to validating fields like IP and operator. Some of the static checks will prevent users from creating or updating a rule if they fail.

Rules are evaluated immediately against static checks when they are created or updated. Static checks don't have a predetermined lifetime and will persist until the triggering condition is fixed or removed from the rule. They will be ignored in scheduled purge tasks used to clean invalid rule checks.

**Note:** Static checks help prevent you from creating a rule that is invalid or a rule that risks capturing everything or nothing.

Dynamic Checks

These checks will analyze your rule's behaviors, like their match ratio or how quickly they are processed. They are evaluated as long as your orchestration rule is active.

Active rules are evaluated against dynamic checks every 10 minutes with the help of a scheduler task. Dynamic checks have a predetermined lifetime of 7 days. During those 7 days, another scheduler task runs every 6 hours to confirm whether those dynamic checks still apply to your rule. If the conditions for that check haven't been seen on your rule for 7 days, the check and its related status will be removed from your rule.

Suppression Rules from the Orchestration Rules Page
About Suppression Rules

USM Anywhere includes suppression rules which enable you to manage false positive alarms and events. After you have confirmed that these issues do not pose a security threat, create a suppression rule to prevent them from displaying in the user interface (UI), and avoid noise in your system.

**Warning:** Orchestration rules only apply to future events and alarms. There is no longer an exception for suppression rules.

Suppression rules using the Contains, Match and Match, case insensitive operators apply to future events and alarms, not to events and alarms received in the current day.

You can create a suppression rule from the details page of an event (Viewing Event Details) or from the details page of an alarm (Viewing Alarm Details). This functionality works the same way, and the Create Rule dialog box is similar when you are creating a rule either from a detail page or from the system configuration window.

**Important:** The easiest way to configure a suppression rule is from the Events details page (see Creating Suppression Rules from the Events Page) or from the Alarms details page (see Creating Suppression Rules from the Alarms Page).

**Note:** USM Anywhere saves the events that match a suppression rule, but does not correlate these suppressed events. By default, USM Anywhere hides these suppressed events. If you want to see these events, click Suppressed in the Search & Filters area. The table displays suppressed events along with all events. See To only display the suppressed events if you want to display just the suppressed events.

**Note:** The suppression rule you create will apply to future items. It also will apply to items of the current day, up to 10 K events/alarms.

See Example: Creating a Suppression Rule for Sudo Events and Example: Creating a Suppression Rule for VPC Flow Logs if you want to see an example of a suppression rule.

Managing Suppression Rules

USM Anywhere enables you to manage your own suppression rules from the All Orchestration Rules page.
To create a suppression rule from the orchestration rules page

1. Go to Settings > Rules > Orchestration Rules.
2. Select Create Orchestration Rule > Suppression Rules.

3. Click Add Conditions and select the property values you want to include in the rule to create a matching condition.

   **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

   **Important:** Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.

   **Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

4. (Optional.) Click Add Group to group your conditions.

   **Note:** See Operators in the Orchestration Rules for more information.

   **Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.
5. Click **Next**.

![Dialog box](image)

**Important:** A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

6. Enter a name for the rule.
7. (Optional.) Enter a description for identifying this rule.
8. Modify these two options:
   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.
These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

9. Click Save.

The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### To filter suppression rules by name

1. Go to Settings > Rules > Orchestration Rules.
2. Click the box next to Filter by.
3. Enter your search.

### To filter suppression rules by rule status

1. Go to Settings > Rules > Orchestration Rules.
2. Click the combo box next to Rule Status.
3. Select All Rules, Enabled, or Disabled.

### To edit a suppression rule

1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click Next.
5. Click Save.

### To delete a suppression rule

1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to delete.
3. Confirm by clicking Accept.

### To enable a suppression rule

1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to enable.
To disable a suppression rule

1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to disable.

To enable all suppression rules

1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Enable All Rules.

To disable all suppression rules

1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Disable All Rules.
4. Confirm by clicking Accept.

Example: Creating a Suppression Rule for Sudo Events

In this example, we are going to create a suppression rule to avoid having a lot of sudo events. You can create this rule whenever you trust the origin host, or because you need to do maintenance. This way you will avoid noise in your list of events.

Note: You can also create your own rules from the Events page, which is an easier way to configure the matching conditions. See Creating Suppression Rules from the Events Page for more information.
To create a suppression rule for avoiding Sudo events

1. Go to Settings > Rules > Orchestration Rules.
2. Select Create Orchestration Rule > Create Suppression Rules.
3. Select these property values:
   - Rule Conditions
     - AND
     - OR
     - Remove Group
     - Data Source
     - Tag
     - CURRENT RULE:
       
4. Click Next.
5. Enter a name for the rule, (for example, **Suppress Sudo Events**).

6. (Optional.) Enter a description for identifying this rule.

7. Modify these two options:
   
   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

   ![Occurrences and Length](image)

   In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

8. Click **Save**.

   The suppression rule has been created. You can see it from **Settings > Rules > Orchestration Rules**. See **Suppression Rules from the Orchestration Rules Page** for more information.

   ![Important: It takes a few minutes for an orchestration rule to become active.](image)

**Example: Creating a Suppression Rule for VPC Flow Logs**

In this example, we are going to create a suppression rule to suppress VPC Flow Logs events. This way you will avoid noise in your list of events.
To create a VPC Flow Logs Suppression Rule

1. Go to Activity > Events.
2. Enter VPC in the search field.
3. Click the icon.
4. Select one of the events.
5. Select Create Rule > Create Suppression Rule.
6. These property values are selected:

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

   - **Packet Type**: Equals Log
   - **Event Name**: Equals REJECT
   - **DataSource Type**: Equals VPC
   - **Source IP Address**: Equals 52.233.156.52, 72.233.64

   **CURRENT RULE**
   packet_type == log AND event_name == REJECT AND plugin_device_type == VPC AND source IP in [52.233.156.52, 72.233.64]

   **RULE VERIFICATION**
   No Errors or warnings

7. Click Next.

1 Warnings, review before continuing

Please review warning messages. Your rule could cause performance issues. Are you sure want to proceed

[Accept]
8. Enter a name for the rule, for example Suppress VPC Flow Logs.

9. (Optional.) Enter a description for identifying this rule.

10. Modify these two options:

   - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

   - **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

   ![Occurrences and Length Table]

   In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

11. Click **Save**.

   The suppression rule has been created. You can see it from **Settings > Rules > Orchestration Rules**. See *Suppression Rules from the Orchestration Rules Page* for more information.

   **Important**: It takes a few minutes for an orchestration rule to become active.
USM Anywhere enables you to make the sensor drop future events that match the rule. These future events are neither correlated nor stored. Through these rules, you are able to define which event data you are going to store in USM Anywhere. You pay for the data you use, so discarded event information is not stored and does not count against the service-level tier of an account. This rule runs on a sensor and control node. The action of this rule has no recovery, so you must be careful when creating the rule. This action can cause a user-generated data loss environment.

**Note:** Filtering rules are not retroactive. The rule applies to future items and it does not apply to previous items, even if those items follow the rule.

**Important:** You can't use a correlation list when you create a filtering rule.

To create a rule for filtering events

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Filtering Rules**.
3. Click **Add Condition** and select the property values you want to include in the rule to create a matching condition. **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

**Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

**Important:** Instead of using the `equals` and `equals, case insensitive` operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

**Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See [Determining the Mapping of a Field](#) for more information.

4. (Optional.) Click **Add Group** to group your conditions.
5. Click **Next**.

6. Enter a name for the rule.

7. (Optional.) Enter a description for identifying this rule.

8. Click **Save**.

   The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

### To test the match criteria of a filter rule

1. Create a test event suppression rule.
2. Add the desired match criteria for the target filter rule action.
3. Enable the rule.
4. Go to Settings > Rules > Orchestration Rules to verify that the rule is working as desired.
5. In the All Orchestration Rules page, click the icon of the filter rule you want to test.

   The events, which triggered the rule and are suppressed, display.

6. Create a filtering rule with the exact same match criteria if the event information displayed is correct. If the event information displayed is not correct, modify the suppression rule match criteria until the correct values are found that suppresses the correct event data. Then generate the filter rule.
To filter filtering rules by name
1. Go to Settings > Rules > Orchestration Rules.
2. Click the box next to Filter by.
3. Enter your search.

To filter filtering rules by rule status
1. Go to Settings > Rules > Orchestration Rules.
2. Click the combo box next to Rule Status.
3. Select All Rules, Enabled, or Disabled.

To edit a filtering rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click Next.
5. Click Save.

To delete a filtering rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to delete.
3. Confirm by clicking Accept.

To enable a filtering rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to enable.

To disable a filtering rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to disable.

To enable all filtering rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Enable All Rules.

To disable all filtering rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Disable All Rules.
4. Confirm by clicking Accept.

Alarm Rules from the Orchestration Rules Page
USM Anywhere enables you to easily identify existing and emerging threats, that are of interest. Through alarm rules, you can organize your threats and only see high-priority alarms, which can be received in email, and will help you to reduce noise and focus on important things.

**Note:** You can also create alarm rules from the details of an event. See [Creating Alarm Rules from the Events Page](#) for more information.

**To create an alarm rule**

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Alarm Rules**.
3. Select a packet type in the Match drop-down list.
   - The first match criteria for all rules must be the packet_type detail field:
     - **Logs:** Use this packet type for event-based rules.
     - **Warnings:** Use this packet type for configuration issues-based rules.
     - **Vulnerabilities:** Use this packet type for vulnerabilities-based rules.
4. Click **Add Conditions** and select the property values you want to include in the rule to create a matching condition.
   - **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.
   - **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

---

¹This packet type refers to configuration issues that are used to identify incorrect uses of certain features. For example, the app for AWS assesses your configuration of AWS to identify insecure use of the AWS security features.
Important: Instead of using the `equals` and `equals, case insensitive` operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

### Note:
If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

5. (Optional.) Click **Add Group** to group your conditions.

### Note:
See Operators in the Orchestration Rules for more information.

### Note:
The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

6. Click **Next**.

A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

7. Enter a name for the rule and, if desired, a description to clarify its use in the Description field.

8. Select an intent.

The intent describes the context of the behavior being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See Intent for more information about the available threat categories.

9. Enter a method.

If known, it is the method of attack or incident associated with the indicator that generated the alarm.

### Note:
This is a required field; if you do not complete this field, the Save button remains inactive.

10. Select a strategy.

The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.

11. Enter a priority.

See Priority Field for Alarms for more information.
12. Configure a mute value.

Once an alarm is created, you can set the time that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

13. Modify these two options:

- **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

![Occurrence Length Table](image)

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

14. (Optional.) Select the fields that you want to display in the generated alarm.

You can select or remove the fields you want to include in the details of the alarm. A field passes from one column to the other by clicking it.

15. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

---

**To filter alarm rules by name**

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the box next to **Filter by**.
3. Enter your search.

**To filter alarm rules by rule status**

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the combo box next to **Rule Status**.
3. Select **All Rules are enabled**, or **All rules are disabled**.

**To edit an alarm rule**

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the **edit** icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click **Next**.
5. Click **Save**.
To delete an alarm rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to delete.
3. Confirm by clicking Accept.

To enable an alarm rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to enable.

To disable an alarm rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to disable.

To enable all alarm rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Enable All Rules.

To disable all alarm rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Disable All Rules.
4. Confirm by clicking Accept.

Notification Rules from the Orchestration Rules Page

Notification rules are a mechanism to generate a specified notification method when the match criteria is met. One major difference between notification rules and other rules is that it does not have the mute operator available. These rules always generate a notification whenever the match criteria is met and never go silent.

You can create your own notification rules from the Orchestration Rules page or from the Events details page, which is the easiest way to configure the matching conditions. See Creating Notification Rules from the Events Page for more information.
To create a notification rule from the Orchestration Rules page:

1. Go to Settings > Rules > Orchestration Rules.
2. Select Create Orchestration Rule > Notification Rule.
3. Click Add Conditions and select the property values you want to include in the rule to create a matching condition.
   - **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.
   - **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.
   - **Important:** Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.
   - **Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.
4. (Optional.) Click Add Group to group your conditions.
   - **Note:** See Operators in the Orchestration Rules for more information.
   - **Note:** The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.
5. Click Next.

6. Enter a name for the rule.

7. (Optional.) Enter a description for identifying this rule.

8. Select a notification method:
   
   - **Amazon SNS**: This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the USM Anywhere Deployment Guide for more information.
   
   - **Datadog**: This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the USM Anywhere Deployment Guide for more information.
   
   - **Email**: This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

   **Note**: The rolling 24-hour 200 email limit applies to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

   - **PagerDuty**: This method is not set up in an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the USM Anywhere Deployment Guide for more information.
   
   - **Slack**: This method makes use of a user-created Slack Webhook integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the USM Anywhere Deployment Guide for more information.

9. Modify these two options:
   
   - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

10. **Click Save.**

The created rule displays in the list of rules. You can see it from Settings > Rules > Orchestration Rules. See Orchestration Rules for more information.

**Important:** It takes a few minutes for an orchestration rule to become active.

**To filter notification rules by name**
1. Go to Settings > Rules > Orchestration Rules.
2. Click the box next to Filter by.
3. Enter your search.

**To filter notification rules by rule status**
1. Go to Settings > Rules > Orchestration Rules.
2. Click the combo box next to Rule Status.
3. Select All Rules, Enabled, or Disabled.

**To edit a notification rule**
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click Next.
5. Click Save.

**To delete a notification rule**
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to delete.
3. Confirm by clicking Accept.

**To enable a notification rule**
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to enable.
To disable a notification rule
1. Go to Settings > Rules > Orchestration Rules.
2. Click the icon of the rule you want to disable.

To enable all notification rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Enable All Rules.

To disable all notification rules
1. Go to Settings > Rules > Orchestration Rules.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click Disable All Rules.
4. Confirm by clicking Accept.

Response Action Rules from the Orchestration Rules Page

To create a response action rule
1. Go to Settings > Rules > Orchestration Rules.
3. Click Add Condition and select the property values you want to include in the rule to create a matching condition.

Note: If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

Note: The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.
Important: Instead of using the `equals` and `equals`, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the `in` or `contains` operators.

Note: If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.

4. (Optional.) Click Add Group to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

Note: The current rule box shows you the syntax of your rule, and the rule verification box reviews that syntax before saving the rule.

5. Click Next.

6. Enter a name for the rule.

7. (Optional.) Enter a description for identifying this rule.

8. Select an Action Type:
   - **AT&T Cybersecurity Forensics and Response App**: See Collecting Forensics and Response Data in the USM Anywhere Deployment Guide for more information.
   - **Authenticated Asset Scanner**: See Performing Vulnerability Scans for more information.
   - **Agent Query**: You can run a rule via an agent query. There are several ad-hoc queries, which are in your environment by default. These queries generate events which can be used for a forensic investigation, so you can focus on fast response and remediation. See The AlienVault Agent for more information.

9. Select an App Action. The options vary depending on the selected action type.

10. Modify these two options:
   - **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

Important: A dialog box opens if there are warning messages. Click Cancel to review the warning messages, or click Accept to continue creating the rule.
- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

1. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

---

To filter response action rules by name

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the box next to **Filter by**.
3. Enter your search.

To filter response action rules by rule status

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the combo box next to **Rule Status**.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit a response action rule

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the **edit** icon of the rule you want to edit.
3. Modify the data of the items that need to be modified.
4. Click **Next**.
5. Click **Save**.

To delete a response action rule

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the **trash** icon of the rule you want to delete.
3. Confirm by clicking **Accept**.

To enable a response action rule

1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the **enable** icon of the rule you want to enable.
To disable an response action rule
1. Go to **Settings > Rules > Orchestration Rules**.
2. Click the icon of the rule you want to disable.

To enable all response action rules
1. Go to **Settings > Rules > Orchestration Rules**.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click **Enable All Rules**.

To disable all response action rules
1. Go to **Settings > Rules > Orchestration Rules**.
2. In the list of rules, select the first checkbox in the first column to select all the rules.
3. Click **Disable All Rules**.
4. Confirm by clicking **Accept**.

Determining the Mapping of a Field

You can determine the mapping of a field by adding the request in the condition of an orchestration rule. From an asset that has an assigned integration or from AlienApps, you can determine the mapping between the property value and its property key. Once you know the property key, you can add the field as a condition in your rule.

USM Anywhere™
User Guide
To determine the mapping of a field from AlienApps:

1. Go to **Data Sources > AlienApps**.
2. Click the **Available Apps** tab and locate the integration.
3. Click the icon next to Data Sources Details and copy all the text within the Data pane.
4. Open a text editor and paste the copied text.
5. Search the property key inside the copied text and copy the property value that maps with that property key.

**Note:** In this example the field is “customfield_11”. This is only for this integration; the same field from another integration may be mapped to another field.
7. Select Create Orchestration Rule > Notification Rules.
8. Click Add Conditions and paste the property value.
9. Choose an operator and enter the value.

**Note:** The fields found in the integration code may be different from the fields used in the rule conditions. In the example, "customfield_11" is actually the "Custom Field 11" in rule conditions.
10. Click Next.

11. Enter a name for the rule.
12. Select a notification method:
   - **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the *USM Anywhere Deployment Guide* for more information.
   - **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the *USM Anywhere Deployment Guide* for more information.
   - **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.
     
     **Note:** The rolling 24-hour, 200-email limit refers to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.
   - **PagerDuty:** This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the *USM Anywhere Deployment Guide* for more information.
   - **Slack:** This method makes use of a user-created Slack Webhook integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the *USM Anywhere Deployment Guide* for more information.

13. Modify these two options:
   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
• **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

14. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

To determine the mapping of a field from assets

1. Go to **Environment > Assets**.
2. Locate the asset that has the integration assigned.
3. Next to the asset name, click the icon and select Full Details.
4. Click the AlienApps tab.

<table>
<thead>
<tr>
<th>Asset Groups (1)</th>
<th>Software (0)</th>
<th>Services (0)</th>
<th>AlienApps (1)</th>
<th>Alarms (0)</th>
<th>Events (0)</th>
<th>Vulnerabilities (0)</th>
<th>Configuration Issues (0)</th>
<th>Scan History</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>VERSION</td>
<td>FORMAT</td>
<td>DEVICE</td>
<td>USA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon AWS CloudTrail</td>
<td>0.49</td>
<td>JSON</td>
<td>CloudTrail</td>
<td>In Use</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Click the icon next to Data Sources Details.

6. Copy all the text under the Data pane.
7. Open a text editor and paste the copied text.
8. Search the property key inside the copied text and copy the property value that maps with that property key. For example, search the property key fromPort. This property key maps with customfield_11.

**Note:** In this example the field is “customfield_11”. This is only for this integration; the same field from another integration may be mapped to another field.

9. Go to **Settings > Rules > Orchestration Rules**.
10. Click **Create Orchestration Rule > Notification Rules**.
    See Notification Rules from the Orchestration Rules Page for more information.
11. Click **Add Condition** and paste the property value.
12. Choose an operator and enter the value.
13. Click **Next**.

14. Enter a name for the rule.

15. Select a notification method:
   - **Amazon SNS**: This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1,000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the **USM Anywhere Deployment Guide** for more information.
   - **Datadog**: This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the **USM Anywhere Deployment Guide** for more information.
   - **Email**: This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

**Note**: The fields found in the integration code may be different from the used in the rule conditions. In the example, "customfield_11" is actually the "Custom Field 11" in rule conditions.
16. Modify these two options:

- **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

![Occurrences and Length](image)

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

17. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

### Example: Creating an Orchestration Rule

**USM Anywhere™**

**User Guide**

In this example, you will create an orchestration rule to generate an alarm when an access to a specific path is detected in a web server.

To create an orchestration rule for generating an alarm when an access to a specific path is detected in a web server:

1. Go to **Settings > Rules > Orchestration Rules**.
2. Select **Create Orchestration Rule > Alarm Rules**.
3. Select a packet type in the Match drop-down list.

The first match criteria for all rules must be the packet_type detail field:
• **Logs**: Use this packet type for event-based rules.

• **Warnings**: Use this packet type for configuration issues-based rules\(^1\).

• **Vulnerabilities**: Use this packet type for vulnerabilities-based rules.

---

\(^1\)This packet type refers to configuration issues that are used to identify incorrect uses of certain features. For example, the app for AWS assesses your configuration of AWS to identify insecure use of the AWS security features.
5. Click Next.

![Warning Message]

**Important:** A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

6. Enter a name for the rule (for example, *Secret Path Accessed*).

7. (Optional.) Enter a description for identifying this rule.

8. Select an intent.

   The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See **Intent** for more information about the available threat categories.

9. Enter a method.

   If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.

   **Note:** This is a required field; if you do not complete this field, the Save button remains inactive.

10. Select a strategy.

    The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.

11. Enter a priority.

    See **Priority Field for Alarms** for more information.

12. Configure a mute value.

    Once an alarm is triggered, you can set a time that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

13. Modify these two options:

   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
• **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

14. **(Optional.)** Select the fields that you want to display in the generated alarm.

You can select or remove the fields you want to include in the details of the alarm. A field passes from one column to the other by clicking it.

15. **Click Save.**

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

**Important**: It takes a few minutes for an orchestration rule to become active.

Operators in the Orchestration Rules

USM Anywhere enables you to use operators in orchestration rules to match specific events or alarms. The following table lists the orchestration rules operators, its meaning, and an example.

**USM Anywhere™ User Guide**
<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign or Equal</td>
<td>Assigns a value if empty. Or if the variable is populated, it will act like Equals.</td>
<td>Note: USM Anywhere completes the value according to the field you have selected. The structure is always &quot;var&quot; followed by the field name. In the example above, the first condition assigns the destination IP address to [var_destination_address], a variable, and the second condition looks for the source IP address that equals the same variable. Essentially, when both conditions are met, you will see events or alarms whose destination IP address is the same as their source IP address.</td>
</tr>
<tr>
<td>Assign or Equal, case insensitive</td>
<td>Assigns a value if empty. Or if the variable is populated, it acts like Equals, ignoring case considerations.</td>
<td></td>
</tr>
<tr>
<td>Contains</td>
<td>Checks for the presence of a substring in a string.</td>
<td></td>
</tr>
<tr>
<td>Contains, case insensitive</td>
<td>Checks for the presence of a substring in a string, ignoring case considerations.</td>
<td></td>
</tr>
<tr>
<td>Equals</td>
<td>Compares the field to the specified value.</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>Meaning</td>
<td>Example</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Equals, case insensitive</td>
<td>Compares the field to the specified value, ignoring case considerations.</td>
<td>Select from property values below to create a matching condition. Learn more about creating rules.</td>
</tr>
<tr>
<td>Greater than</td>
<td>Returns true if the left operand is greater than the right operand.</td>
<td>Select from property values below to create a matching condition. Learn more about creating rules.</td>
</tr>
<tr>
<td>In</td>
<td>Searches for character and numeric values that are equal to one from a list of values, separated by commas.</td>
<td>Select from property values below to create a matching condition. Learn more about creating rules.</td>
</tr>
<tr>
<td>In, case insensitive</td>
<td>Searches for character and numeric values that are equal to one from a list of values, separated by commas, ignoring case considerations.</td>
<td>Select from property values below to create a matching condition. Learn more about creating rules.</td>
</tr>
<tr>
<td>In List</td>
<td>Returns true if the value is included in the correlation list (see Example: Creating an Alarm Rule Using a Correlation List).</td>
<td>Select from property values below to create a matching condition. Learn more about creating rules.</td>
</tr>
<tr>
<td>Operator</td>
<td>Meaning</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>In List, case insensitive</td>
<td>Returns true if the value is included in the correlation list, ignoring case considerations.</td>
<td><img src="current_rule_1.png" alt="Example screenshot" /></td>
</tr>
<tr>
<td>Is Empty</td>
<td>Finds elements that have an empty value (it is the same as the Equals but with an empty string).</td>
<td><img src="current_rule_2.png" alt="Example screenshot" /></td>
</tr>
<tr>
<td>Is Not Empty</td>
<td>Finds elements that do not have a value.</td>
<td><img src="current_rule_3.png" alt="Example screenshot" /></td>
</tr>
<tr>
<td>Is In CIDR</td>
<td>Find elements that are included in the given IP range (using CIDR notation).</td>
<td><img src="current_rule_4.png" alt="Example screenshot" /></td>
</tr>
<tr>
<td>Is Not In CIDR</td>
<td>Finds elements that are not included in the given IP range (using CIDR notation).</td>
<td><img src="current_rule_5.png" alt="Example screenshot" /></td>
</tr>
<tr>
<td>Operator</td>
<td>Meaning</td>
<td>Example</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Less than</td>
<td>Returns true if the left operand is less than the right operand.</td>
<td></td>
</tr>
<tr>
<td>Match</td>
<td>Finds elements that match a specified pattern <strong>using regular expressions</strong>.</td>
<td></td>
</tr>
<tr>
<td>Match, case insensitive</td>
<td>Finds elements that match a specified pattern using regular expressions, ignoring case considerations.</td>
<td></td>
</tr>
</tbody>
</table>

USM Anywhere™
User Guide
<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Equals</td>
<td>The value of the specified field does not match the specified value.</td>
<td><img src="image" alt="Operator Not Equals" /></td>
</tr>
<tr>
<td>Not Equals, case insensitive</td>
<td>The value of the specified field does not match the specified value, ignoring case considerations.</td>
<td><img src="image" alt="Operator Not Equals, case insensitive" /></td>
</tr>
</tbody>
</table>

### Using Regular Expressions in USM Anywhere

The **Match and Match, case insensitive** operators enable you to use regular expressions (regex) to define a pattern to match the content of a field.

**Important:** USM Anywhere uses the **Java Regular Expression Syntax**, which is different from JavaScript, Perl, Gnu, and other flavors of regex, so be sure to read their documentation and familiarize yourself with the differences.

It is highly recommended that you find and use a tool to test your regular expressions before saving them into rules. Some popular examples include **Java Regular Expression Tester** or **RegexPlanet**.

When using regular expressions in USM Anywhere, keep the following in mind:

- The expression pattern must be delimited with the forward slash "/" character. For example:
  
  `/Router -.*/`

- Use a backslash (\") to escape special characters that would otherwise be interpreted as regex syntax, which includes the "\" character itself. For example:
  
  `/[C:\\Windows\System\]/.\`  

**Note:** Since the backslashes are not used as literals in Java code, but are carried as data in strings in the system, you do not need to double-escape them like you would if you were putting a regex pattern into a Java literal in coding.

- You can use capture and grouping syntax such as \1, $1, or (?:).
- Modifiers such as /i, /x, /m, and /s are not supported.

### Possible Messages When Creating Rules

When you are creating a rule, you can get some of these messages.
### Rules Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>This Message Is Displayed When</th>
</tr>
</thead>
<tbody>
<tr>
<td>At least one criterion is required besides packet type</td>
<td><em>Packet Type</em> is the unique criterion in the rule condition.</td>
</tr>
<tr>
<td>All condition fields must have a value</td>
<td>The condition value is missing.</td>
</tr>
<tr>
<td>Case insensitive operator does not apply to numbers</td>
<td>You select a <em>case insensitive</em> operator and the condition value is a number.</td>
</tr>
<tr>
<td>A regular expression must be used with &quot;Match&quot; operator (example: ~ /value/)</td>
<td>You select the <em>Match</em> operator and the condition value has to be a valid regexp.</td>
</tr>
<tr>
<td>A variable expression must be used with &quot;Assign or Equal&quot; operator (example: &gt;&gt; varname)</td>
<td>You select the <em>Assign or Equal</em> operator and the condition value must be a valid variable name between brackets.</td>
</tr>
<tr>
<td>Some characters used could be part of a regular expression</td>
<td>Your condition value contains *, +, [ or ], but the <em>Match</em> operator is not selected.</td>
</tr>
</tbody>
</table>

### Orchestration Rules Examples

This page includes examples of orchestration rules that you can use as a guide when you create your own orchestration rules. The examples use the allowed operators in USM Anywhere. See [Operators in the Orchestration Rules](https://example.com) and [Orchestration Rules Best Practices](https://example.com) for more information.

Rules processing is a Boolean query of rules operators. Processing is performed left to right until the rule is either validated (the stated rule action is taken) or invalidated (the processing terminates). The entire rule does not have to be processed, and any additional query operators after this point are discarded.

**Example 1: Use the OR Boolean Operators**

Match criteria sections in any rule are read and processed from left to right until they are either validated or invalidated. Use extreme care with the application of OR, OR NOT, and AND NOT operators. These can cause a value group to be validated true under all conditions if not properly handled. The outcome of any criteria match operation using the OR operator in the grouped items is not dependent on any other portion of the group to validate or invalidate the group. If any of the match criteria processed in the group validates *TRUE*, the entire group validates *TRUE*.

Conversely, the use of the AND operator creates conjoined operations where the group validates true or false based on the outcome of the entire match criteria in the group. All criteria in a group with an AND operator will be processed to determine a *TRUE* or *FALSE* outcome.

In the following example, a condition appears using OR OR NOT OR NOT, the intent is to validate the statement as *TRUE* if the username is *NOT Joe* OR *NOT Bill* OR *NOT Bob*. This string looks like a correctly formatted rule for that intent:

```
packet_type == 'log' AND .... AND (! source_username == 'Joe' OR ! source_username == 'Bill' OR ! source_username == 'Bob')
```

This condition group will validate *TRUE* regardless of the source_username in the event. This is because if any of the three match criteria sections in the OR OR NOT OR NOT condition group is true, the entire group validates true, so if the source_username value is "Bill", the condition group of the rule validates *TRUE* because the first rule section criteria is met. The second or third sections of the rule are never processed. The proper way to format the rule is to use the AND operator so that each element in the group requires individual validation. The proper formatting for this is the following:

```
packet_type == 'log' AND .... AND source_username != 'Joe' AND source_username != 'Bill' AND source_username != 'Bob'
```

Once the rules processor hits the OR operator, it validates the rule criteria and performs the rule action. Any match criteria that follows the OR is not seen.

You can get different results depending on the type of rule you create:
If it is an alarm rule, every event creates an alarm.

- If it is a suppression rule, every event is suppressed. Keep in mind that suppressed events are not correlated for alarms. See Suppression Rules from the Orchestration Rules Page for more information.
- If it is a notification rule, every event causes a notification action.
- If this is a filter rule, every event is filtered and discarded from your environment. You can't recover these events.

**Example 2: Use the Same Criteria in Two Different Rules**

When you create a rule, ensure that the rule doesn't match criteria with additional operators of a different rule. For example, look at these two rules:

(packet_type == 'log' AND event_severity == 'ERROR' AND event_category == 'System' AND event_subcategory == 'Microsoft-Windows-WindowsUpdateClient')

(packet_type == 'log' AND event_severity == 'ERROR' AND event_category == 'System' AND event_subcategory == 'Microsoft-Windows-WindowsUpdateClient' AND source_username == 'SYSTEM' AND source_ntdomain == 'NT AUTHORITY')
If the second rule is triggered, the first rule is also triggered, which causes duplicate rule actions. The second rule is essentially the first rule but with more operators.

Example 3: Merge Rules with the Same Format
When you have multiple rules with the same format, you can merge rules and match the difference. For example, instead of having two separate rules, such as this:

(packet_type == 'log' AND access_control_outcome == 'Deny' AND source_username == 'VALUE_1')

and this:

(packet_type == 'log' AND access_control_outcome == 'Deny' AND source_username == 'VALUE_2')

Or you can merge these rules into this one:

(packet_type == 'log' AND access_control_outcome == 'Deny' AND source_username == 'VALUE_1' OR source_username == 'VALUE_2')

Or you can merge the rules into this one:

(packet_type == 'log' AND access_control_outcome == 'Deny' AND source_username in ('VALUE_1', 'VALUE_2'))

Example 4: Don't Use Rules Criteria of the Same Value Type
Don't use rules criteria of the same value type because they are essentially one and the same in the rule definition. Each "rule_attack_id" item in the above will have a "rule_attack_tactic" and "rule_attack_technique" values that are unique to it. By specifying the single detail of "rule_attack_id == 'T1050'", the other match details can be safely removed for rules clarity and rules processing efficiency. Note that the creation of the three match criteria is a normal action of the rules generator.

For USM Anywhere, this rule:

(packet_type == 'alarm' AND rule_id == 'Windows New service installed' AND source_ntdomain == 'FINICITY' AND rule_attack_id == 'T1050' AND rule_attack_tactic in ('Persistence', 'Privilege Escalation') AND rule_attack_technique == 'New Service')

is better to write as follows:

(packet_type == 'alarm' AND rule_id == 'Windows New service installed' AND source_ntdomain == 'FINICITY' AND rule_attack_id == 'T1050')
Example 5: Avoid the Use of the regex "match" (~) Criteria

Don't use the regex "match" (~) operator because it can cause a performance issue with the server using it.

Instead of this rule:

```
(packet_type == 'log' AND event_name == 'PowerShell: EventID 400' AND log ~ /C:\Scripts\script.ps1/)
```

You can use this rule:

```
(packet_type == 'log' AND event_name == 'PowerShell: EventID 400' AND log contains 'C:\Scripts\script.ps1')
```

Or you can use this rule:

```
(packet_type == 'log' AND event_name == 'PowerShell: EventID 400' AND log contains 'C:\Scripts\script.ps1')
```

For data ingestion from syslog sources, the "raw_log" is the entire syslog packet received for processing. This is the syslog format:

```
<PRI> date/timestamp device hostname/IP address event message/packet payload
```

The "event message/packet_payload" is the information with the headers stripped off.

For processing purposes, both rules are almost equivalent but packet_payload is the preferred detail to use. Network-based intrusion detection system (NIDS) traffic inspection does not use syslog.

Example 6: Simplify Your Rules

When you have a rule that uses the same operator multiple times, you can simplify it. Look at this example:

```
(packet_type == 'log' AND ( event_name == 'Value1 OR event_name == 'Value2' OR event_name == 'Value3'))
```

You can simplify the rule by removing the "OR" operator:

```
(packet_type == 'log' AND event_name in ('Value1', 'Value2', 'Value3'))
```

Additionally, USM Anywhere doesn't validate a rule in the case of matching the same event detail information against different match values.

```
(alarm_source_countries == 'US' AND alarm_source_countries == 'CA')
```

This event detail has a single set value in the normalized event. It can never validate against multiple values when using the AND operator.

You can instead implement these two rules:

```
(alarm_source_countries == 'US' OR alarm_source_countries == 'CA')
```

Or this rule:

```
(alarm_source_countries == 'US' OR alarm_source_countries == 'CA')
```

Example 7: Boolean Operators Read from Left to Right

Boolean operators in any rule are read and processed from left to right up to the point where the rule is validated (rule action is taken) or invalidated (rule processing terminates). Any additional conditions after the rule has been either validated or invalidated will not be processed.

For example:

```
... AND (match_field != value1 OR match_field != value2)
```

In the previous example, the use of the "!=" and "OR" operator sets the entire section to TRUE for all values of "match_field". It will never be processed as FALSE, so any subsequent rule matching operators after this rule section will be processed.

Here's another example:
In this previous example, the rule portion of `(file_permission != 'shared_internally' OR file_permission != 'private')` gives the result of true if either of the operators are true. Therefore, if the detail “file_permission” has a value of ‘private’, the entire rule section is still validated as true because the match criteria “file_permission != ‘shared_internally’” is true. The correct implementation would be to use the AND operator at the end, so that the last section of the rule reads `(file_permission != 'shared_internally' AND file_permission != 'private')`.

Example 8: Values Separated by a Comma

When there are two values separated by a comma in an alarm or an event detail, the match criteria will fail if it’s matching against only a portion of the detail value. The rule will incorrectly auto-populate using the in operator and not the equals (==) operator. This is due to the comma found in the detail data field. The correct operator to use is the equals (==) operator.

See the RULE ATTACK TACTIC Persistence,Privilege Escalation example from the alarms detail page.

RULE ATTACK TACTIC Persistence,Privilege Escalation

This match criteria is incorrectly auto-populated with the in operator and will always fail:

```
rule_attack_tactic in (Persistence','Privilege Escalation')
```

The comma has separated the match string into two unique values that can never validate. The actual match value is a single string, with the comma included.

It should read like this:

```
rule_attack_tactic == (Persistence',Privilege Escalation')
```

Note that the single quotes establishes it as a single string value and are automatically added by the rules generator.

Example 9: Make Use of Correlation Lists to Simplify a Rule

If a rule has a match detail item value with the equals (==) operator that is used to match a large number of field values, the rule can be simplified and made easier to maintain and update by using a correlation list instead.

```
Note: The use of correlation lists is not supported for filter rules. This option is not visible in the user interface (UI) for filter rules creation.
```

For example:

```
(user == 'name1' OR user == 'name2' OR user == 'name3' OR user == 'name4' OR user == 'name5')
```

This can be simplified by first creating a correlation list populated with the values of ‘name1’, ‘name2’, ‘name3’, name4’, and ‘name5’. If this correlation list is named as “Valid_Users”, you could substitute the example rule with a simpler one such the following:

```
(user -> [[Valid_Users]])
```

In the revised rule above, the “->” operator is for items in the list of "Valid_Users."

See Correlation lists for more information.
Correlation is the processing of the event stream to identify important events or patterns of events within large volumes of data. The logic to identify these events is encapsulated in a correlation rule. The AT&T Alien Labs™ Security Research Team creates correlation rules, which associate multiple events from one or more data sources to identify potential security threats. These rules identify patterns associated with malicious activity. Alarms are generated by an explicit call within these rules.

These correlation rules are created by the Security Research Team and you are not able to modify them. However, you can use orchestration rules to modify the way USM Anywhere treats events. See Orchestration Rules for more information.

**Important:** The "Suspicious Behavior - OTX Indicators of Compromise" correlation rule generates alarms if the pulse comes from the AlienVault OTX account.

**What Is Correlation?**

Correlation is a process performed by the correlation engine in USM Anywhere. It identifies potential security threats by detecting behavior patterns across different types of assets, which produce disparate yet related events. Correlation links different events, turning data into more useful information.

The logs received and processed by USM Anywhere carry important information such as what your users are doing, what data is being accessed, how your system and network are performing, and if there are any security threats or attacks taking place. However, reading logs has these disadvantages:

- Logs vary from system to system or even from version to version on the same system.
- Logs have limited perspective because each system sees events from its own perspective.
- Logs are static, fixed points in time without the full context or sequence of related events.

The correlation process provides answers to these challenges, putting the events into full context. For example, a network firewall sees packets and network sessions, while an application sees users, data, and requests. While different systems report logs of similar activities, the way in which they articulate these activities is quite different. With the help of correlation rules, USM Anywhere can correlate the two types of events, generating an alarm if a threat exists.

Event correlation enables the security analysts and the incident responders to do the following:

- Make informed decisions on how to respond to security threats
- Validate the effectiveness of existing security controls
- Measure and report compliance
- Detect policy violations

**Correlation Rule Structure**

This is the structure of correlation rules: Intent – Strategy – Method.

The structure uses a three-tiered model for describing an observed behavior:

- **Intent:** The first tier is the "intent" of the behavior. This roughly maps to the "intrusion kill chain" to provide an understanding of the context of the behavior.
- **Strategy:** The second tier is the strategy the attacker took, used to describe the methodology employed.
- **Method:** The third tier is the "method" of the behavior, used to describe the details of the particular methodology.

**Intent**
The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete.

From highest to lowest, these are the threat categories:

<table>
<thead>
<tr>
<th>Intent</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Compromise</td>
<td>Behavior indicating a compromised system.</td>
</tr>
<tr>
<td>Exploitation &amp; Installation</td>
<td>Behavior indicating a successful exploit of a vulnerability, backdoor, or remote access trojan being installed on the system.</td>
</tr>
<tr>
<td>Delivery &amp; Attack</td>
<td>Behavior indicating an attempted delivery of an exploit. This can include detection of malicious email attachments, network-based detection of known attack payloads, or analysis-based detection of known attack strategies such as an SQL injection.</td>
</tr>
<tr>
<td>Reconnaissance &amp; Probing</td>
<td>Behavior indicating an actor attempting to discover information about your organization. This is broad-based, including everything from port scans to social engineering to open-source intelligence.</td>
</tr>
<tr>
<td>Environmental Awareness</td>
<td>Behavior and status about the environment being monitored. This includes information about services running, behavior of users in the environment, and the configuration of the systems.</td>
</tr>
</tbody>
</table>

**Strategy**

The strategy describes the broad-based strategy or behavior that is detected. It is a description of the strategy the malicious user is using to achieve their goal. For example, when trying to exploit a known vulnerability in a web browser, the attacker is launching a "Client-Side Attack - Known Vulnerability".

**Method**

The method describes the approach that the actor employs. To further the previous example, the method would provide additional detail on the target of the attack and the vulnerability "Firefox - CVE-2008-4064".

**USM Anywhere Correlation Rules**

USM Anywhere provides built-in rules and adds more every week through the AT&T Alien Labs™ Threat Intelligence Subscription. Some of these rules are generic, which means that the rule can match data from different data sources. For example, the following rule matches data from different application firewalls:

<table>
<thead>
<tr>
<th>Delivery &amp; Attack</th>
<th>Web Server Attack - Persistent XSS</th>
<th>Multiple XSS attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRATEGY DESCRIPTION</td>
<td>ATTACK TACTIC</td>
<td>RULE</td>
</tr>
<tr>
<td>An attacker is targeting your web servers with a XSS injection attack. This attack attempts to exploit the input validation of your web application to inject JavaScript into data fields that are reflected into a :JSESSIONID cookie on the login page.</td>
<td>Initial Access</td>
<td>plugin_device == &quot;Firewall&quot; AND plugin_device_type == Application AND plugin_device_plugin == &quot;Firewall&quot; AND customfield_0 CONTAINS &quot;CROSS_SITE_SCRIPTING_INJECTION&quot; AND source.categorical == &quot;source&quot;</td>
</tr>
</tbody>
</table>

Some rules are more specific, which means that the rule only matches a particular data source. For example, the following rule only matches data from Watchguard XTM:
Note: When a more specific rule exists in USM Anywhere, it takes precedence over the generic rule.

To see correlation rules
1. Go to Settings > Rules > Correlation Rules.
2. You can use the search field above the table to search for a rule by entering the search text in the field and then clicking the search icon.
3. Click the rule to expand the details of the rule.
   You can see the strategy, the method, and the rule itself.

Important: Correlation rule details are not visible to users with a trial license.

4. Click the alarm icon to open the Alarms List view page.
   The page includes Rules Name as a filter so that you can see how many alarms match the selected rule.

Note: The mute length indicates during how long that rule is not going to generate an alarm.

Operators in the Correlation Rules

USM Anywhere provides built-in rules and adds more every week through the AT&T Alien Labs™ OTX Subscription. These rules are the result of the combination of operators and USM Anywhere fields.

Correlation Rules: Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td><strong>Equals</strong>: Compares the field to the specified value.</td>
<td>plugin_device == 'GuardDuty'</td>
</tr>
<tr>
<td>==*</td>
<td><strong>Equals, case insensitive</strong>: Compares the field to the specified value, ignoring case considerations.</td>
<td>event_activity ==* 'Executable download'</td>
</tr>
<tr>
<td>&gt;&gt;</td>
<td><strong>Assign or equal</strong>: For use with variables, it will assign a value if empty or if the variable is populated it will act like ==.</td>
<td>source_canonical &gt;&gt; [source]</td>
</tr>
<tr>
<td>&gt;&gt;*</td>
<td><strong>Assign or equal, case insensitive</strong>: For use with variables, it will assign a value if empty or if the variable is populated it will act like ==*.</td>
<td>source_username &gt;&gt;* [username]</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than.</td>
<td>user_id &gt; 500</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than.</td>
<td>user_id &lt; 505</td>
</tr>
<tr>
<td>Operator</td>
<td>Meaning</td>
<td>Example</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>in</td>
<td>List contains: Will return true if the list contains the value. This will perform a <code>==</code> comparison for every value in the list returning true on the first match.</td>
<td>event_subcategory in ('Microsoft-Windows-MountMgr', 'MountMgr')</td>
</tr>
<tr>
<td>in*</td>
<td>List contains, case insensitive: Will return true if the list contains the value. This will perform a <code>==*</code> comparison for every value in the list returning true on the first match.</td>
<td>event_name in* ('Update route in route table','Update route table for VPC')</td>
</tr>
<tr>
<td>~</td>
<td>Match: Takes a regular expression delimited by '?' as the argument.</td>
<td>hostname ~/.<em>.</em>.eng/</td>
</tr>
<tr>
<td>~*</td>
<td>Match case insensitive: Takes a regular expression delimited by '?' as the argument.</td>
<td>(source_process_commandline ~/[a-z0-9]{15,45}].[a-z0-9]{1,15}.[a-z0-9]{1,4}/ )</td>
</tr>
<tr>
<td>=&gt;</td>
<td>Checks the value against a list filled with previous events values. Will validate the condition if the element is not already included in the list.</td>
<td>source_country =&gt; [countries]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>And: Can be used to chain two comparisons, will return true if both comparisons evaluate to true.</td>
<td>rep_device_rule_id == '15457' &amp;&amp; source_username &gt;&gt;* [username]</td>
</tr>
<tr>
<td>!</td>
<td>Not: Will negate the return value of the expression directly following it.</td>
<td>source_country != &quot;</td>
</tr>
<tr>
<td>or</td>
<td>Or: Alternative to</td>
<td></td>
</tr>
<tr>
<td>and</td>
<td>And: Alternative to &amp;&amp;.</td>
<td>event_subcategory == 'Microsoft-Windows-Sysmon' AND rep_device_rule_id == '1'</td>
</tr>
<tr>
<td>!-&gt;</td>
<td>Not in List: Checks that a value is not contained in a correlation list.</td>
<td>source_name !-&gt; [[SAFE_NAMES]]</td>
</tr>
<tr>
<td>!-&gt;*</td>
<td>Not in List, case insensitive: Checks that a value is not contained in a correlation list, ignoring case considerations.</td>
<td>source_name !-&gt;* [[SAFE_NAMES]]</td>
</tr>
</tbody>
</table>

---

**USM Anywhere™ User Guide**

USM Anywhere enables you to create correlation lists. Use a correlation list to group values together to apply to a single rule. So instead of creating a rule for each value, you can save time and effort by creating a correlation list and using it in a rule.

When creating correlation lists for rules, you can use a standard field, such as `event_name` or `event_description`. A helpful use for correlation lists is the creation of user blacklist, whitelists, or both, like `event_names`. Or you can enter anything you want in the items of the correlation lists, but only up to 500 characters per item. There is a limit of 1000 items per correlation list.

To see an example of an alarm rule using a correlation list, see Example: Creating an Alarm Rule Using a Correlation List.
To create a correlation list

1. Go to Settings > Rules > Correlation Lists.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>USER</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalCorrelationList</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>GLOBAL_Known_AWS_Instance_Types</td>
<td></td>
<td>AT&amp;T Cybersecurity</td>
</tr>
<tr>
<td>GLOBAL_Known_AWS_Regions</td>
<td></td>
<td>AT&amp;T Cybersecurity</td>
</tr>
<tr>
<td>GLOBAL_Known_AWS_Users</td>
<td></td>
<td>AT&amp;T Cybersecurity</td>
</tr>
<tr>
<td>GLOBAL_Known_Cross_Account_Acce...</td>
<td></td>
<td>AT&amp;T Cybersecurity</td>
</tr>
</tbody>
</table>

2. Click New List.

3. Enter a name for the correlation list in the Name field and, if desired, a description to clarify its use in the Description field.

**Important:** The valid characters for the correlation list name are uppercase letters (A-Z), lowercase letters (a-z), numerical digits (0-9), and underscore (_). You can enter up to 64 characters.
4. Click **Add Item** to include items in your list.

**Important:** The list items are restricted to a string format to match the formats of the tested event detail items.

5. Click **Save**.

To add a new item to a list:

1. Go to **Settings > Rules > Correlation Lists**.
2. Click the list to expand the details of the list.
3. Click **Add Item**.

The Add Item dialog box opens.

4. Enter the value and click **Save**.

**User Guide**
To modify a correlation list
1. Go to Settings > Rules > Correlation Lists.
2. Click the icon of the list you want to modify.
3. Modify the data of the items that need to be modified.
4. Click Save.

To delete a correlation list
1. Go to Settings > Rules > Correlation Lists.
2. Click the icon of the list you want to delete.
3. Click Delete.

To modify an item of a list
1. Go to Settings > Rules > Correlation Lists.
2. Click the list to expand the details of the list.
3. Click the icon of the item you want to modify.
4. Modify the item and click the ✔️ icon.

To delete an item of a list
1. Go to Settings > Rules > Correlation Lists.
2. Click the list to expand the details of the list.
3. Click the 🗑️ icon of the item you want to delete.

Example: Creating an Alarm Rule Using a Correlation List

Role Availability

USM Anywhere™ User Guide

In this example, an orchestration rule is created to generate an alarm whenever a user, who is included in a correlation list, generates an event.

Note: See Correlation Lists for more information.

To create an orchestration rule for generating an alarm when a user, included in a correlation list, generates an event
1. Go to Settings > Rules > Correlation Lists.
2. Click New List.
3. Enter a name for the correlation list in the Name field and, if desired, a description to clarify its use in the Description field.

Important: The valid characters for the correlation list name are uppercase letters (A-Z), lowercase letters (a-z), numerical digits (0-9), and underscore (_). You are allowed to enter from 1 to 64 characters.

4. Click Add Item to include the user names to your list.
5. Click Save.
7. Click **Create Orchestration Rule > Alarm Rules**.

8. Select a packet type in the Match drop-down list.

   The first match criteria for all rules must be the packet_type detail field:

   - **Logs**: Use this packet type for event-based rules.
   - **Warnings**: Use this packet type for configuration issues-based rules.
   - **Vulnerabilities**: Use this packet type for vulnerabilities-based rules.

9. Click **Add Conditions** and select these property values.

   **Username**: Use the value **In List, Case Insensitive**.

---

1 This packet type refers to configuration issues that are used to identify incorrect uses of certain features. For example, the app for AWS assesses your configuration of AWS to identify insecure use of the AWS security features.
10. Click **Next**.

**Important:** A dialog box opens if there are warning messages. Click **Cancel** to review the warning messages, or click **Accept** to continue creating the rule.

11. Enter a name for the rule (for instance "Alarm for undesirable users") and, if desired, a description to clarify its use in the Description field.

12. Select an intent.

The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See **Intent** for more information about the available threat categories.

13. Enter a method.

If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.

**Note:** This is a required field; if you do not complete this field, the Save button remains inactive.

14. Select a strategy.

The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.

15. Enter a priority.

See **Priority Field for Alarms** for more information.

16. Configure a mute value.

Once an alarm is created, you will see the icon that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

17. Modify these two options:

- **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

  This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

<table>
<thead>
<tr>
<th>Occurrences</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

18. **(Optional.)** Select the fields that you want to display in the generated alarm.

You can select or remove the fields you want to include in the details of the alarm by clicking the and the icons.

19. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.
Important: It takes a few minutes for an orchestration rule to become active.
USM Anywhere delivers vulnerability assessment as part of a complete package of security monitoring and management capabilities for efficient threat detection. USM Anywhere does this to improve security in your network, you first need to know what is vulnerable.

This topic discusses these subtopics:

<table>
<thead>
<tr>
<th>Subtopic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Vulnerability Assessment</td>
<td>510</td>
</tr>
<tr>
<td>System Settings for Authenticated Scans</td>
<td>513</td>
</tr>
<tr>
<td>Managing Credentials in USM Anywhere</td>
<td>518</td>
</tr>
<tr>
<td>Performing Vulnerability Scans</td>
<td>539</td>
</tr>
<tr>
<td>Viewing Vulnerabilities Scan Results</td>
<td>542</td>
</tr>
<tr>
<td>Searching Vulnerabilities</td>
<td>550</td>
</tr>
<tr>
<td>Viewing Vulnerabilities Details</td>
<td>556</td>
</tr>
<tr>
<td>Available Remediation Patches for Vulnerabilities</td>
<td>564</td>
</tr>
<tr>
<td>Labeling the Vulnerabilities</td>
<td>565</td>
</tr>
<tr>
<td>Create a Vulnerabilities Report</td>
<td>569</td>
</tr>
<tr>
<td>USM Anywhere Scans Best Practices</td>
<td>571</td>
</tr>
</tbody>
</table>
USM Anywhere delivers vulnerability assessment as part of a complete package of security monitoring and management capabilities for efficient threat detection. USM Anywhere does this to improve security in your network. To generate a vulnerability assessment, you first need to know what is vulnerable.

Vulnerability assessment is a functionality of USM Anywhere used for defining, identifying, classifying, and prioritizing the vulnerabilities in your system. The universal open and standardized method for rating IT vulnerabilities and determining the urgency of response is the Common Vulnerability Scoring System (CVSS). This method assigns severity scores to vulnerabilities. Scores range from 0 to 10, with 10 being the most severe.

USM Anywhere works on both CVSS version 3 (CVSSv3) and the previous version 2 (CVSSv2) for scoring.

About Vulnerability Assessment in USM Anywhere

USM Anywhere detects vulnerabilities in assets and controls these scanning functions:

- Running and scheduling vulnerability scans (see Performing Vulnerability Scans for more information)
- Generating and examining reports (see Viewing Vulnerabilities Scan Results for more information)

USM Anywhere detects vulnerabilities using an authenticated scan, where the USM Anywhere Sensor initiates a credentialed SSH (in Linux systems) or Microsoft Windows Remote Management (WinRM) (in Windows systems) connection to the asset, and remotely runs a series of commands for host-based assessment.

Vulnerability detection is based on an implementation of the Security Content Automation Protocol (SCAP) and the Open Vulnerability and Assessment Language (OVAL) 5.11.2 schema version. The National Vulnerability Database (NVD) is the U.S. government's content repository for SCAP. The OVAL schema is maintained by The MITRE Corporation and developed by the public OVAL Community website at http://oval.mitre.org.

AT&T Alien Labs™ Open Threat Exchange® (OTX™) queries NVD and MITRE every hour looking for the latest vulnerabilities. Every time you run a vulnerability scan, USM Anywhere queries OTX for updating the vulnerabilities information.

For Linux variants, USM Anywhere performs a series of generic UNIX and independent schema tests in addition to flavor-specific tests for IBM AIX, FreeBSD, Hewlett Packard Enterprise HP-UX, and Linux. For Windows, USM Anywhere performs a series of Windows schema and independent schema tests.
About Vulnerability Severity

Discovering a vulnerability by itself is important, but can be of little use without the ability to estimate the associated severity to an asset. For this reason, USM Anywhere assigns a severity to each vulnerability found in the system and according to the severity score of the CVSS.

The following table shows the CVSS v2.0 and v3.0 ratings.

CVSS v2.0 and v3.0 Ratings

<table>
<thead>
<tr>
<th>Severity</th>
<th>v2 Score Range</th>
<th>v3 Score Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>n/a</td>
<td>0.0</td>
</tr>
<tr>
<td>Low</td>
<td>0.0-3.9</td>
<td>0.1-3.9</td>
</tr>
<tr>
<td>Medium</td>
<td>4.0-6.9</td>
<td>4.0-6.9</td>
</tr>
<tr>
<td>High</td>
<td>7.0-10.0</td>
<td>7.0-8.9</td>
</tr>
<tr>
<td>Critical</td>
<td>n/a</td>
<td>9.0-10.0</td>
</tr>
</tbody>
</table>

**Important:** There is also an Under Analysis severity. This severity displays when the National Vulnerability Database (NVD) has not assigned a CVSS base score to the vulnerability. OTX queries NVD and MITRE every hour looking for the latest vulnerabilities. Every time you run a vulnerability scan, USM Anywhere queries OTX to update the vulnerabilities information. If the NVD has updated the CVSS base score for that vulnerability, USM Anywhere will update the status after you run a new vulnerability scan.
To see the CVSS score of a vulnerability

1. Go to Environment > Vulnerabilities.
2. Click the vulnerability to display its details.

About Active and Inactive Vulnerabilities

In USM Anywhere you can find active vulnerabilities and inactive vulnerabilities. When you run a scan on an asset and USM Anywhere finds a vulnerability, this vulnerability is active for that specific asset. If you later run a new scan over the same asset and USM Anywhere finds more vulnerabilities, but the vulnerability found in the previous scan has not been found in this new scan, this vulnerability is inactive and the new vulnerabilities are active. Inactive vulnerabilities are those who are not present in the latest scan but were in a previous one.

A Practical Example

USM Anywhere finds 15 vulnerabilities when you run a scan over an asset, so you will see "active: 15, inactive: 0". Then you fix these vulnerabilities. A week later, you run a scan over the same asset. This new scan finds 3 vulnerabilities, so you will have 3 vulnerabilities active out of 15 vulnerabilities found and USM Anywhere will display "active: 3, inactive: 12".

Searching Active or Inactive Vulnerabilities

When you go to Environment > Vulnerabilities, USM Anywhere displays, by default, all active vulnerabilities. The Active filter is selected.
If you want to see the inactive vulnerabilities, select the filter **Inactive**. USM Anywhere displays the list of your inactive vulnerabilities.

**System Settings for Authenticated Scans**

An authenticated scan is a vulnerability testing measure performed from the vantage of a logged-in user. The quality and depth of an authenticated scan depends on the privileges granted to the authenticated user account. The following table lists the recommended settings for creating a designated account on different operating systems (OSes). See [Creating Credentials](#) for information about creating credentials for authenticated scans in USM Anywhere.
System Settings for Authenticated Scans

Escalation Options for Authenticated Scans by OS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Methods and Credentials</th>
<th>Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>SSH password or public key authentication</td>
<td>sudo, su</td>
</tr>
<tr>
<td>Windows</td>
<td>Microsoft Windows username and password through Microsoft Windows Remote Management (WinRM)</td>
<td>None</td>
</tr>
</tbody>
</table>

Requirements for Linux

You must have the following on the Linux host to perform an authenticated scan:

- The OpenSSH server installed
- Network connectivity between the USM Anywhere Sensor and the SSH port on the Linux host

Installing the OpenSSH Server

Refer to the vendor documentation for your Linux distribution for instructions on how to install and configure the OpenSSH server:

- **Ubuntu**: [https://help.ubuntu.com/community/SSH/OpenSSH/Configuring](https://help.ubuntu.com/community/SSH/OpenSSH/Configuring)
- **Debian**: [https://wiki.debian.org/SSH](https://wiki.debian.org/SSH)
- **FreeBSD**: [https://www.freebsd.org/doc/handbook/openssh.html](https://www.freebsd.org/doc/handbook/openssh.html)

Requirements for Windows

For Microsoft Windows hosts, USM Anywhere uses Windows Remote Management (WinRM) to perform authenticated scans. Therefore, you need to have the following items on the Windows machine:

- WinRM version 2.0 or later.
- PowerShell version 5.1 or later. USM Anywhere performs some tests prior to running the authenticated scans to make sure that the scans can succeed. These tests require PowerShell 5.1 or later to be installed on your machine.
- Port 5985 open on your firewall. WinRM listens for HTTP traffic at port 5985 by default. Make sure that your firewall allows incoming connections through this port.

- The Windows Management Instrumentation (WMI) service enabled. WinRM supports WMI classes and operations. It also leverages WMI to collect data about disks, network adapters, services, or processes in your environment.

In addition, using the Group Policy Editor, go to Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell, and make these changes:

- Enable Allow Remote Shell Access.
- Set the MaxConcurrentOperationsPerUser parameter to at least 3, ideally 10 or 15.
- Set the MaxMemoryPerShellMB parameter to 1024.

See Microsoft Documentation for more information on WinRM parameters.

**Important:** For a Windows server that is hardened according to the Center for Internet Security (CIS) benchmarks, such as the CIS Amazon Machine Image (AMI) for Windows Server 2016 available in the Amazon Web Services (AWS) Marketplace, there are local group policies that block these connectivity requirements. For these servers, you must open the port and re-enable WinRM and remote access on each boot of the server.

### Creating a Windows Admin Account

AT&T Cybersecurity recommends that you create a designated admin account solely for the authenticated scans rather than using an established admin account or a guest account. The most important aspect about Windows credentials is that the account used to perform the scans should have privileges to access all required files and registry entries, which in many cases means administrative privileges.

When creating such an account, you must keep in mind the following:

- This account needs to be able to create temporary files and temporary registry values.
- This account must have remote and local log-on rights. See Setting Log-on Locally and the Security Policy for more information.
- If using Active Directory (AD), assign user rights to either the Remote Management Users group or the Administrators group, because only these two groups can log in through WinRM. This authentication uses sAMAccountName, which is limited to 20 characters.
- When configuring network access policy for this account, select Classic: local users authenticate as themselves.
- If your machine is joined to a domain, a local account won't be able to log in. In this case, you must add a new registry named LocalAccountTokenFilterPolicy:

  Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
  Value Name: LocalAccountTokenFilterPolicy
  Type: DWORD
  Value: 1
See Microsoft Documentation for a better understanding of Windows authentication for remote connections.

**Setting Log-on Locally and the Security Policy**

USM Anywhere enables you to add a WinRM credential. The account you use to log on to the target system must have remote and local logon rights.

**Note:** Set the local logon rights to avoid large numbers of processes and large amounts of memory usage.

**Important:** The vulnerability scan needs to be able to perform a local logon on the target device because it needs to create a "delegatable" identity token to access domain resources from its session on the target device. Although it is possible to run a scan without having the local logon privileges and without the correct token, the attempts to collect certain information can fail with errors, for example "Access Denied", which might impact the rule results.

**To set the local logon rights¹**

1. Select **Start > All Programs > Accessories > Run** and enter **gpedit.msc** to open the Local Group Policy Editor.

![](image)

2. In the console tree, select **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.**

¹These instructions may vary depending on your Windows version.
3. Click **Allow log on locally** to open its properties.
4. Assign the rights to your user.
5. Click OK.
6. Repeat the steps for Allow log on through Remote Desktop Services.

Managing Credentials in USM Anywhere

When running a scan in USM Anywhere, you have the option to run it with or without authentication, a process used to verify the identity of a user, user device, or other entity, usually through a username and password. A credential is an identification that proves you are who you claim to be, and you are therefore a reliable source.

When running a scan without authentication, USM Anywhere probes the network services available on the target machine. Using known protocol behaviors, it attempts to identify the software that is running as well as its configuration and version. With this information, USM Anywhere then attempts to match the identified software with the known vulnerabilities to produce a report. The benefit of this approach is that the detection can be very specific in identifying known vulnerable behaviors.

When you choose to run a scan with authentication, your credentials allow USM Anywhere to query the running machine to gain detailed and accurate information about the running software and its configuration. This prevents false positives from misidentified services that can sometimes occur in the unauthenticated approach. In addition, an authenticated scan ensures that all services and software are analyzed — regardless of whether the service is running or accessible from the network.

**Important:** A vulnerability scan requires credentials to perform an authenticated scan on a host.

Keep in mind these points:

- USM Anywhere uses the credentials available for a given asset, no matter what the privileges are for those credentials.
- When you run a scan for an asset, USM Anywhere uses the asset credential if the asset has one; if the credential does not work or the asset does not have an assigned credential, USM Anywhere will use the credential of the group which the asset is a member of, if it is part of an asset group.

**Important:** Credentials assigned directly to an asset have higher priority than those assigned to an asset group.
• When the asset does not have an assigned credential and the asset is a member of several asset groups with different assigned credentials, USM Anywhere tests every credential and will use the first one that works.

• When you assign a credential to an asset group, USM Anywhere will assign the credential to the group instead of assigning it to all of its members. If you want to assign a credential to all members of a group, see Assign Credentials to Group Members.

• USM Anywhere supports these cipher types:
  • aes128-ctr
  • 3des-ctr
  • blowfish-cbc
  • aes256-cbc
  • aes192-cbc
  • aes128-cbc
  • 3des-cbc
  • aes256-ctr

This topic discusses the following subtopics:

• Creating Credentials
• Assigning Credentials to Assets
• Removing Credentials from Assets

Scan Target Platform Support

USM Anywhere supports running vulnerability scans on the following platforms and devices:

**Microsoft Windows:**

• Windows 7, 8.1, and 10

**Linux:**

• Amazon Linux and Linux 2
• CentOS 6, 7, and 8
• Debian 10
• Fedora 32 and 33
• Linux Mint 18, 19, 20, and Debian Edition 4
• Oracle Linux 6, 7, and 8
• Redhat Enterprise Linux 6, 7, and 8
• Ubuntu 16.04, 18.04, 20.04, and 20.10
Apple macOS:
- macOS 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, and 11

Creating Credentials

USM Anywhere enables you to assign credentials to your assets. If the required credential set is not yet defined in USM Anywhere, you must add it before you can associate it with one or more assets. The Credentials page displays a list of all credential sets that are defined and available to be associated with an asset or asset group.

To add a new credential

1. Go to Settings > Credentials.

2. Click New Credentials.

   The Add New Credential dialog box opens.
3. Enter a name for the credential in the Name field and, if desired, a description to clarify its use in the Description field.

4. In Credential Type, select SSH or Windows RM based on the operating system of the asset.

Windows RM

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

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

- **Username:** Enter the username for the account with the required privileges.
  
  **Important:** The username must have 20 characters or less.

- **Password:** Enter the password for the user account.

- **Domain:** (Optional.) Enter the domain name registered in the Domain Name System (DNS).
Note: Use a fully qualified domain name (FQDN) instead of a Network Basic Input/Output System (NetBIOS) name. If you use a NetBIOS name, you will get an invalid SSH gateway error.

- **Port**: If an alternative port number is required, enter the port number. The default port, 5985, is standard.

  - **Username**: Enter the username for the account with the required privileges.
  - **New Password**: Enter the password.
  - **Domain**: Enter the domain.
  - **Port**: Enter the port number, default is 5985.

**SSH**

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

- **Username**: Enter the username for the account with the required privileges.
- **Authentication method**: Set the SSH authentication mode and enter the password, private key, or both.
  - **Password**: Select this option to use a simple password to authenticate the user account. It is mandatory if you do not use a private key.
  - **Private key (no passphrase)**: Select this option to use a private key to authenticate the user account.
  - **Private key with passphrase**: Select this option to use a private key and password combination to authenticate the user account.
**Important:** A private key must start with an appropriate header, such as "-----
BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----". Always copy the certificate in the form with the header.

- **Password**: This field only appears if you select Password as authentication method. Enter the password that authenticates the user.

- **Privilege elevation**: Select the elevated privilege to use for the credentials.
  - **sudo**: Use this option to run single commands with root privileges. For example:
    ```
    sudo 'command1'; sudo 'command2'; sudo 'command3' ...
    ```
  - **su**: Use this option to run single commands with superuser privileges. This requires you to enter the username and password for the superuser account. For example:
    ```
    su username -c 'command1'; su username -c 'command2'; su username -c 'command3' ...
    ```

- **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. See Scan Target Platform Support for more information.

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

**SSH Key Manual Generation**

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

**To create an SSH key manually**

1. Open the command line for Linux or Terminal for macOS.
2. Enter `ssh-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 /users/<username>/.ssh/id_rsa for macOS), or designate another location for the file.

   The command line prompts you to specify a passphrase and enter it again to confirm it.

4. Specify a passphrase or, if you don’t want to use a passphrase, leave the line blank, and then press **Enter**.

5. The SSH key is saved to either the default location or the location you specified.

Assigning Credentials to Assets

USM Anywhere enables you to assign credentials to an asset, to an asset group, or to members of an asset group.

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

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

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 **edit** icon.

### Credentials

Credentials are used to perform authenticated Asset Scans to search for vulnerabilities, configuration issues, and collect software inventory information.

The system can scan Linux, Solaris, AIX, HP-UX, MacOS, VMware ESXi, Cisco IOS/XE, Cisco ASA, and JunOS.

Changes to credentials in this section will update the credential assigned to any Asset(s) or Asset Group(s).

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>AUTHENTICATION METHOD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>credentials-name-2-cobb-1882</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-2-cobb-1881</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-1-3500-2001</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>vsos</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-1-cobb-1881</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-1-cobb-1882</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
<tr>
<td>credentials-name-2-3500-2001</td>
<td>SSH</td>
<td>Password</td>
<td>Description</td>
</tr>
</tbody>
</table>
A dialog box opens.

3. Enter part of the asset name in the field at the bottom of the dialog box
This displays the matching items below the field. You can enter more text to filter the list further.

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

The credentials overwrite dialog box opens.
Warning: If the asset has already assigned credentials, these credentials are going to be overwritten.

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

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

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

**To assign a credential on the Assets page**

1. Go to Environment > Assets and locate the asset.
2. Next to the asset name, click the ✰ icon and select Assign Credentials.
   
   The assign credentials dialog box opens.
3. In the Available Credentials drop-down list, select the credential to use.

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.

---

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

**Assigning Credentials to an Asset Group**

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. If you want to assign a credential to all members of a group, see **Assign Credentials to Group 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 **key** icon.

A dialog box opens.
3. Click the **Asset Groups** tab.

4. At the bottom of the dialog box, enter part of the asset group name in the field.
   
   This displays the matching items below the field. You can enter more text to filter the list further.

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

6. Click the **X** icon to close the dialog box.

**To assign a credential on the Asset Groups page**

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

The assign credentials dialog box opens.
3. In the Available Credentials drop-down list, select the credential to use.

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

4. Click **Save**.

**Assigning Credentials to Group Members**

1. Go to **Environment > Asset Groups**.
2. Click the icon next to the asset group name and select **Full Details**.
3. Click **Actions > Assign Credentials to Group Members**.
   
   The Configure Asset Group Members dialog box opens.
4. Select the credentials to use or create a new one, see Creating Credentials
5. Click **Save**.

### Removing Credentials from Assets

USM Anywhere enables you to remove credentials from your environment.
Removing a credential from the Credentials page

1. Go to Settings > Credentials to open the credentials main page.
2. Click the ▼ icon in the line of the credential you want to remove the association from.

   ![Credentials Delete](image)

   Note: You can use the ▼ icon from the main credentials page to check the assets assigned to the credential. Once you delete the credential, the association between the asset and the credential finishes.

3. Click Accept to confirm the process or click Cancel to exit.

Removing a credential associated with an asset from the Assets page

1. Go to Environment > Assets.
2. Select the asset. See Selecting Assets in Asset List View for more information.
3. Click the ▼ icon you want to remove the credential from and select Assign Credentials.
4. Click Remove Current Credentials From Asset.
5. Click Save.

Remove a Credential Associated with an Asset Group from the Asset Groups Page

1. Go to Environment > Asset Groups.
2. Locate the asset group that you want to remove the credential from and click the icon and select Full Details.
3. Click Modify Credentials to open the Assign Credentials to Asset Group dialog box.
4. Click **Remove Current Credentials From Asset Group**.

5. Click **Save**

**Performing Vulnerability Scans**

In USM Anywhere you can run:

**Authenticated scans**

An authenticated scan verifies scanned IPs and detects vulnerabilities, configuration issues, and software. The USM Anywhere Sensor initiates a credentialed SSH (Linux), WinRM (Windows), or MacOS connection to the asset and remotely runs a series of commands for host-based assessment. See [Managing Credentials in USM Anywhere](#). You can run authenticated asset scans from these pages:

- **Environment > Assets** for running an authenticated scan in that precise moment. See [Running Authenticated Asset Scans](#) for more information.

- **Environment > Asset Groups** for running an authenticated asset groups scan in that precise moment. See [Running Authenticated Asset Groups Scans](#) for more information.
• **Settings > Scheduler** for scheduling an authenticated scan job during a specific period of time. See [Scheduling Asset Scans from the Job Scheduler Page](#) and [Scheduling Asset Groups Scans from the Job Scheduler Page](#) for more information.

• **Environment > Vulnerabilities** for running an asset scan. You can scan a single asset, an asset group, or enter a network range. See [Running an Asset Scan from Vulnerabilities](#) for more information.

**Warning:** An authenticated scan may fail if the local mail exchanger, which applies to Linux hosts, is enabled in the target asset.

You cannot scan USM Anywhere sensors.

### Unauthenticated scans

Use an asset scan to discover services, operating systems, hostnames, IP and MAC addresses, and vulnerabilities of known hosts in the deployed network. You can run non-authenticated asset scans from these pages:

• **Environment > Assets** for running an asset scan in that precise moment. See [Running Asset Scans](#) for more information.

• **Environment > Asset Groups** for running an asset group scan in that precise moment. See [Running Asset Groups Scans](#) for more information.

• **Settings > Scheduler** for scheduling an asset scan job during a specific period of time. See [Scheduling Asset Scans from the Job Scheduler Page](#) and [Scheduling Asset Groups Scans from the Job Scheduler Page](#) for more information.

**Note:** See [USM Anywhere Scans Best Practices](#) for more information.

### Commands Used in Authenticated Scans

When you run an authenticated scan in USM Anywhere, there are multiple commands executing at the same time. These commands change constantly and there are new definitions released every day. You can also verify which commands have been executing at any given moment.

**Linux**

Linux-authenticated scans use privilege escalation over ssh. Commands are logged in the audit log:

- `/var/log/secure`
- `/var/log/auth`

**Windows**

Windows-authenticated scans perform file and registry checks to determine the version of the installed patch.
Running an Asset Scan from Vulnerabilities

1. Go to **Environment > Vulnerabilities**.
2. Click **New Scan**.

   The Authenticated Asset Scan dialog box opens.

3. Select the assets you want to scan:
   - Single Asset. You need to enter the name of the target you want to scan or select it from a list of your targets.
   - Asset Group Name. You need to enter the name of the asset group you want to scan or click **Select from List** for selecting it from a list of your asset groups.
   - Network ranged. You need to enter the network range you want to scan.

4. Click **Next**.

   A new Authenticated Asset Scan dialog box opens.
5. Click **Assign Credentials** for assigning credentials to the assets and devices you want to scan. Click **Create New Credentials** for creating a credential. See Managing Credentials in USM Anywhere for more information.

6. Click **Select Another Target** if you want to come back.

7. You can select the targets to scan if you have more than one.

8. Click **Start Scan**.

   The scan starts. Depending on the selected asset, the scan can last several minutes. When the scan finishes, you can see the status and if the scan found vulnerabilities. If you want to view the results of your scan, you need to go to the asset details page. See Viewing Assets Details for more information.

9. Click **Continue Scanning And Close**.

   While the scan is running, a Scanning button shows. When the scan finishes, the message Scan finished. Refresh to view scan results displays.

10. Click **Refresh Scan Results** to update the list.

### Viewing Vulnerabilities Scan Results

A vulnerability is a weakness in your system, which reduces your system's information assurance. USM Anywhere helps you to define, identify, classify, and prioritize the vulnerabilities in your system.

USM Anywhere provides a centralized view of your vulnerabilities. Go to Environment > Vulnerabilities to see this centralized view.
The Vulnerabilities page displays information on vulnerabilities. These are the different parts of the page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the vulnerabilities.
- The main part of the page is the list of vulnerabilities, where each row describes an individual vulnerability. Click a vulnerability to open its details. See Viewing Vulnerabilities Details for more information. Each vulnerability includes a check box that you can use to select it. You can select all vulnerabilities in the same page by clicking the check box in the first column of the header row.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the icon to hide the filter pane. Click the icon to expand the filter pane.

**Refreshing the page**

USM Anywhere gives you the option of refreshing the page manually by clicking the icon.
Vulnerabilities from Assets Main Page

To explore vulnerabilities from assets

1. Go to Environment > Assets.
2. Click the filter Has Vulnerabilities.

3. Next to the asset name that you want to explore, Click the ✓ icon and select Vulnerabilities.

The asset details page opens with the list of vulnerabilities.
4. Click the vulnerability you want to explore.

5. (Optional.) Click the star symbol to the left of the vulnerability name to mark it for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and a link to it.

Vulnerabilities List Columns

For each vulnerability in the vulnerabilities columns list, USM Anywhere displays useful information to help you manage that vulnerability.

The following table lists the fields you see on the page.

List of the Default Columns in Vulnerabilities

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Seen</td>
<td>Last date on which the vulnerability was seen in the asset. The displayed date depends on your computer's time zone.</td>
</tr>
<tr>
<td>Vulnerability ID</td>
<td>Displays the associated Common Vulnerabilities and Exposures (CVE) ID, in case of having it.</td>
</tr>
<tr>
<td>Vulnerability Description</td>
<td>Displays the description of the vulnerability.</td>
</tr>
<tr>
<td>Column Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Labels</td>
<td>Label applied to the vulnerability. See Labeling the Vulnerabilities for more information.</td>
</tr>
<tr>
<td>Source</td>
<td>Source that found the vulnerability.</td>
</tr>
<tr>
<td>Asset</td>
<td>This is the asset that is vulnerable.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates the severity of the vulnerability. Values are High, Medium, Low, and Under Analysis. See About Vulnerability Severity.</td>
</tr>
<tr>
<td>Score</td>
<td>Displays the score in the Common Vulnerability Scoring System (CVSS). See Common Vulnerability Scoring System SIG for more information.</td>
</tr>
<tr>
<td>First Seen</td>
<td>Detection date of the vulnerability in the asset. The displayed date depends on your computer's time zone.</td>
</tr>
</tbody>
</table>

From the list of vulnerabilities, you can click any individual vulnerability row to display more information on the selected vulnerability. See Viewing Vulnerabilities Details for more information.

To select a vulnerability, select the check-box to the left of the vulnerability. You can select all vulnerabilities at the same time by selecting the first checkbox in the column. These buttons display when you select a vulnerability:

- **Apply Labels**: You can add a label to a vulnerability, which enables you to have classified vulnerabilities. See Labeling the Vulnerabilities for more information.

- **New Scan**: This button runs a new authenticated asset scan. See Running an Asset Scan from Vulnerabilities for more information.

You can choose the number of items to display by selecting 20, 50, or 100 below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Click the ★ icon to bookmark an item for quick access. Clicking the ★ icon on the secondary menu shows the bookmarked items and provides links to them.

Click **Generate Report** button to open the Configure Report dialog box. See Create a Vulnerabilities Report for more information.

Click the ⬇️ icon displayed next to the asset name below the asset column to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.

- **Find in events**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.
- **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See [Using OTX in USM Anywhere](#) for more information.
- **Full Details**: See [Viewing Assets Details](#) for more information.
- **Configure Asset**: See [Editing the Assets](#) for more information.
- **Delete Asset**: See [Deleting the Assets](#) for more information.
- **Assign Credentials**: See [Managing Credentials in USM Anywhere](#) for more information.
- **Authenticated Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See [Running Authenticated Asset Scans](#) for more information.
- **Scan with AlienApp**: This option enables you to run an asset scan through an AlienApp. See [Running Asset Scans Using an AlienApp](#) for more information.
- **Configuration Issues**: This option opens the Assets Details page. The Configuration Issues tab is selected in the page. See [Viewing Assets Details](#) for more information.
- **Vulnerabilities**: This option opens the Assets Details page. The Vulnerabilities tab is selected in the page. See [Viewing Assets Details](#) for more information.
- **Alarms**: This option opens the Assets Details page. The Alarms tab is selected in the page. See [Viewing Assets Details](#) for more information.
- **Events**: This option opens the Assets Details page. The Events tab is selected in the page. See [Viewing Assets Details](#) for more information.

**Vulnerability Assessment**

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

USM Anywhere delivers vulnerability assessment as part of a complete package of security monitoring and management capabilities for efficient threat detection. USM Anywhere does this to improve security in your network, you first need to know what is vulnerable.

This topic discusses these subtopics:
Report Templates in Vulnerabilities

USM Anywhere includes a wide range of report templates classified according to the compliance templates for alarms, vulnerabilities, and events collected in the system. The templates are combined into these two groups:

- **PCI**: Payment Card Industry Data Security Standards (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These reports are identified and based on specific PCI DSS requirements to provide the auditor with the specific information requested. For example, PCI DSS requirement 10.7.a: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.

- **NIST CSF**: The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

- **ISO 27001**: ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).

**To apply a report template**

1. Go to **Environment > Vulnerabilities**.
2. From the Vulnerabilities list view, click **View** above the filters and select **Report templates**.
3. Select a report.
   - You can use the search field or scroll down the list.
4. Click **Apply**.

   The result displays with the filters applied.

**Searching Vulnerabilities**

USM Anywhere includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure filters** link located in the upper-left corner of the page. The management of filters is similar to that for assets. See **Managing Filters** for more information.

The following table lists the filters you see on the page.
### Filters Displayed by Default in the Main Vulnerabilities Page

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 Hours</td>
<td>Filter vulnerabilities triggered in the last hour, last 24 hours, last 7 days, last 30 days or last 90 days. You can also configure your own period of time by clicking the <strong>Custom Range</strong> option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select <strong>AM</strong> or <strong>PM</strong>.</td>
</tr>
<tr>
<td>Active/Inactive</td>
<td>Filter vulnerabilities by the active or inactive vulnerabilities. See <a href="#">About Active and Inactive Vulnerabilities</a>.</td>
</tr>
<tr>
<td>Labels</td>
<td>Filter vulnerabilities by the labels applied to the vulnerability. See <a href="#">Labeling the Vulnerabilities</a> for more information.</td>
</tr>
<tr>
<td>Vulnerability Name</td>
<td>Filter vulnerabilities by name of the vulnerability.</td>
</tr>
<tr>
<td>Severity</td>
<td>Filter vulnerabilities by severity of the vulnerability. Values are High, Medium, and Low, see <a href="#">About Vulnerability Severity</a>.</td>
</tr>
<tr>
<td>Source</td>
<td>Filter vulnerabilities by the source that found the vulnerability.</td>
</tr>
<tr>
<td>Asset</td>
<td>Filter vulnerabilities of the asset that is vulnerable.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>This is the asset group that has vulnerable asset. The number between parentheses indicates the number of assets in the asset group.</td>
</tr>
</tbody>
</table>

The number between brackets displayed by each filter indicates the number of items that match the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

#### Icons Next to the Filter Title

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>📅</td>
<td>Sort the filters alphabetically.</td>
</tr>
<tr>
<td>📜</td>
<td>Sort the filters by the number of items that match them.</td>
</tr>
</tbody>
</table>

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the ✗ icon next to the filter. Or clear all filters by clicking **Reset**.
Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.
Standard Mode

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

To activate the standard mode when the advanced mode is on

1. Go to Environment > Vulnerabilities.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray, .

USM Anywhere™ User Guide 553
Note: If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

Advanced Mode

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

To activate the advanced mode

1. Go to Environment > Vulnerabilities.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green, .

To perform a search in the advanced mode

1. Go to Environment > Vulnerabilities.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
   This turns the icon green, .
3. Click the filters that you want to select.
   The selected filters display inside a dashed rectangle.
4. In the lower-left corner of the page, click Apply Filters. Or in the upper side of the page, click Apply.

The result of your search displays.

To search using the NOT operator

1. Go to Environment > Vulnerabilities.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Click the filter that you want to exclude.
4. In the filter group, click Not.
### Important: You have to select a filter to see this operator.

### Note: The selected filter displays the ❌ icon and the filter chiclet is labeled in red.

<table>
<thead>
<tr>
<th>Vulnerabilities View: Default</th>
<th>Status: Active</th>
<th>Asset Groups is not: Assets with Alarms ❌</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun 03/28/2021 - Fri 02/04/2022</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Search & Filters

- **Configure Filters**
  - Enter search phrase
  - **Active**
    - Asset Groups
    - Assets with Alarms (209)
    - Database Servers (51)
    - Linux Assets (25)
    - vmware-sensor-network (20)
    - Windows Assets (9)
    - Web Servers (5)
    - Assets with Agents (3)
  - **Inactive**

#### Displayed Filters:

- **LAST SEEN**
  - Mon, Oct 04 2021, 05:20 PM

#### Vulnerabilities Table

<table>
<thead>
<tr>
<th>LAST SEEN</th>
<th>VULNERABILITY ID</th>
<th>VULNER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2017-12448</td>
<td>CVE-20</td>
</tr>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2017-12454</td>
<td>CVE-20</td>
</tr>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2017-13734</td>
<td>CVE-20</td>
</tr>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2017-12455</td>
<td>CVE-20</td>
</tr>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2016-4074</td>
<td>CVE-20</td>
</tr>
<tr>
<td>Mon, Oct 04 2021, 05:20 PM</td>
<td>CVE-2017-11333</td>
<td>CVE-20</td>
</tr>
</tbody>
</table>

### Important: Some filters don't include the NOT operator (for example, Services or Software).

5. Click **Apply**.

To search all values of a filter

1. Go to **Environment > Vulnerabilities**.
2. In the upper-left corner of the page, click the 🔍 icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

To search Vulnerabilities using the search field

1. Go to **Environment > Vulnerabilities**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example,
"bob@mycompany.com").

Note: Keep in mind that wildcard characters are considered as literals.

3. Click the icon.

The result of your search displays with the items identified.

Viewing Vulnerabilities Details

The vulnerabilities details page provides in-depth information on vulnerabilities.
To view the details of a vulnerability
1. Go to **Environment > Vulnerabilities**.
2. Click the vulnerability to display its details.
**DSA-4208-1 procps -- procps**

**Select Action**

### Vulnerabilities Details

<table>
<thead>
<tr>
<th>REFERENCE ID</th>
<th>CVE-2018-1122</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVERITY</td>
<td>High</td>
</tr>
<tr>
<td>CVSS SCORE V2</td>
<td>4.4</td>
</tr>
<tr>
<td>CVSS SCORE V3</td>
<td>7</td>
</tr>
<tr>
<td>FIRST SEEN</td>
<td>Wed, Jul 28 2021, 8:44 AM</td>
</tr>
<tr>
<td>LAST SEEN</td>
<td>Mon, Feb 7 2022, 11:23 AM</td>
</tr>
<tr>
<td>RULE</td>
<td>ovat.org.secpod.oval:def:603404</td>
</tr>
<tr>
<td>SOURCE</td>
<td>jovel</td>
</tr>
<tr>
<td>LABELS</td>
<td></td>
</tr>
</tbody>
</table>

### Description

The Qualys Research Labs discovered multiple vulnerabilities in procps, a set of command line and full screen utilities for browsing procs. The Common Vulnerabilities and Exposures project identifies the following problems: CVE-2018-1122 top read its configuration from the current working directory if no $HOME was configured. If top were started from a directory writable by the attacker this could result in local privilege escalation. CVE-2018-1123 Denial of service against the ps invocation of another user. CVE-2018-1124 An integer overflow in the file2strvec function of libprocps could result in local privilege escalation. CVE-2018-1125 A stack-based buffer overflow in pgrep could result in denial of service for a user using pgrep for inspecting a specially crafted process. CVE-2018-1126 Incorrect integer size parameters used in wrappers for standard C allocators could cause integer truncation and lead to integer overflow issues.

### Affected Software

- Procp-Ng_PROJECT: Procp-Ng
- Canonical Ubuntu Linux (Show Affected Versions)
- Debian Debian Linux (Show Affected Versions)

### Asset

- IP ADDRESS: [View All..]
- OPERATING SYSTEM: Debian 8x

**Vulnerabilities**: 345  **Configuration Issues**: 0  **Alarms**: 0  **Events**: 3.36k  **Running**: [Running]
Click the ✭ icon to bookmark an item for quick access. Clicking the ✭ icon on the secondary menu shows the bookmarked items and provides links to them.

The Vulnerabilities Details page includes the Select Action button that is supported for your assigned user role. Use this button to launch an authenticated asset scan. See Applying Actions to Vulnerabilities for more information.

You can see the vulnerabilities details, then a description, the affected software, and the associated asset. If you want more information, click the ✅ icon. See Viewing Assets Details for more information.

The labels field indicates if the vulnerability has been classified by using a label. You can click the ⚰️ icon to manage the labels of the vulnerability. See Labeling the Vulnerabilities for more information.

3. In the upper right corner, click the previous and next buttons to navigate between items.
4. Click the ❌ icon to close the dialog box.
5. Click the vulnerability title to expand its details.

Applying Actions to Vulnerabilities

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

USM Anywhere enables you to respond to the vulnerability. Use this button to launch an authenticated scan of an asset. You need to select the sensor, if you have more than one installed in your environment, and then indicate the asset to scan.

To apply an action to a vulnerability

1. Go to Environment > Vulnerabilities.
2. Search for the vulnerability for which you want to launch an authenticated scan.
3. Click the vulnerability.
4. The vulnerability details dialog box opens with the information about the specific vulnerability.
**Viewing Vulnerabilities Details**

**DSA-4208-1 procps -- procps**

Select Action

<table>
<thead>
<tr>
<th><strong>Vulnerabilities Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REFERENCE ID</strong></td>
</tr>
<tr>
<td><strong>SEVERITY</strong></td>
</tr>
<tr>
<td><strong>CVSS SCORE V2</strong></td>
</tr>
<tr>
<td><strong>CVSS SCORE V3</strong></td>
</tr>
<tr>
<td><strong>FIRST SEEN</strong></td>
</tr>
<tr>
<td><strong>LAST SEEN</strong></td>
</tr>
<tr>
<td><strong>RULE</strong></td>
</tr>
<tr>
<td><strong>SOURCE</strong></td>
</tr>
<tr>
<td><strong>LABELS</strong></td>
</tr>
</tbody>
</table>

**Description**
The Qualys Research Labs discovered multiple vulnerabilities in procps, a set of command line and full screen utilities for browsing process. The Common Vulnerabilities and Exposures project identifies the following problems: CVE-2018-1122 top read its configuration from the current working directory if no $HOME was configured. If top were started from a directory writable by the attacker this could result in local privilege escalation. CVE-2018-1123 Denial of service against the ps invocation of another user. CVE-2018-1124 An integer overflow in the file2strvec function of libprocps could result in local privilege escalation. CVE-2018-1125 A stack-based buffer overflow in pgrep could result in denial of service for a user using pgrep for inspecting a specially crafted process. CVE-2018-1126 Incorrect integer size parameters used in wrappers for standard C allocators could cause integer truncation and lead to integer overflow issues.

**Affected Software**

*Procs-Ng_project Procs-Ng*  
*Canonical Ubuntu Linux (Show Affected Versions)*  
*Debian Debian Linux (Show Affected Versions)*

**Asset**

<table>
<thead>
<tr>
<th><strong>IP ADDRESS</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPERATING SYSTEM</strong></td>
<td>Debian 8x</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Vulnerabilities</strong></th>
<th><strong>Configuration Issues</strong></th>
<th><strong>Alarms</strong></th>
<th><strong>Events</strong></th>
<th><strong>Running</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>345</td>
<td>0</td>
<td>0</td>
<td>3.36k</td>
<td></td>
</tr>
</tbody>
</table>
5. Click **Select Action**.

A dialog box opens, but depending on the sensor installed in your environment and the advanced AlienApps available for that or those sensors, you can see a different dialog box with different options. See *Advanced AlienApps* for more information.
6. Depending on the selected option, you should fill in different fields.

7. Click Run.

Available Remediation Patches for Vulnerabilities

USM Anywhere enables you to display the available remediation patches for a vulnerability. In case of an existing remediation patch for a vulnerability, USM Anywhere displays the patch name, a description, the source, and the reference identification (ID).

To display the available remediation patches on a vulnerability

1. Go to Environment > Vulnerabilities.

2. Search for the vulnerability where you want to see the available remediation patches. See Searching Vulnerabilities for more information.

3. Click the vulnerability to open a dialog box with the vulnerability.
4. Click the vulnerability title to open the full details of the vulnerability.

5. Click the Available Patches tab.

Labeling the Vulnerabilities

USM Anywhere includes a set of labels that you can use to classify your vulnerabilities, to track the status of the vulnerabilities, and to search vulnerabilities using them as a filter. See Searching Vulnerabilities for more information on how to search vulnerabilities.

You can't edit or delete the set of default labels:

- In Progress
- Closed
- Open
- False Positive

USM Anywhere enables you to create, edit, and delete your own labels. You can apply a label to one or more vulnerabilities. You can also apply multiple labels to the same vulnerability.
To label a vulnerability from the vulnerabilities main page

1. Go to Environment > Vulnerabilities.
2. Search for the vulnerability or vulnerabilities to which you want to apply a label. See Searching Vulnerabilities for more information.
3. Do one of these options:
   - Click the icon in the labels column of the vulnerability you want to label, select the label, and click **Apply**.
• Select the checkbox to the left of a vulnerability, click **Apply Labels**, select the label, and click **Apply**.

---

**To label a vulnerability from the vulnerabilities details page**

1. Go to **Environment > Vulnerabilities**.
2. Search for the vulnerability to which you want to apply a label. See **Searching Vulnerabilities** for more information.
3. Click the vulnerability.
4. In the **Labels** field, click the 🖊 icon to select a label.

5. Click **Save**.

**To create a new label**

1. Go to **Environment > Vulnerabilities**.
2. Select the checkbox to the left of the vulnerability.
3. Click **Apply Labels**.
4. Click **Manage Custom Labels**.
5. Click **Create New Label**.
6. Enter a name for the label.
7. Click Save.

**To edit a label**
1. Go to Environment > Vulnerabilities.
2. Select the checkbox to the left of the vulnerability.
3. Click Apply Labels.
4. Click Manage Custom Labels.
5. Click the icon next to the label you want to edit.
6. Modify the name of the label.
7. Click the icon to apply the changes.

**To remove a label from a vulnerability**
1. Go to Environment > Vulnerabilities.
2. Select the checkbox to the left of a vulnerability. You can also select several vulnerabilities or select all vulnerabilities at the same time by selecting the first checkbox in the column.
3. Click Remove Vulnerabilities Labels.
4. Select the label or labels you want to remove.
5. Click Remove.

**To remove a label from a vulnerability**
1. Go to Environment > Vulnerabilities.
2. Do one of these options:
   - Select the checkbox to the left of a vulnerability. You can also select several vulnerabilities or select all vulnerabilities at the same time by selecting the first checkbox in the column. Then click Remove Vulnerabilities Labels, click the label, and click Remove.
   - In the labels column of the vulnerability from which you want to remove the label, click the icon next to the label.

**Create a Vulnerabilities Report**

You can create a PDF or CSV report of the vulnerabilities directly from the vulnerabilities page.

**Important:** AT&T Cybersecurity recommends Google Chrome as the preferred browser for generating reports.
To create a vulnerabilities report

1. Go to Environment > Vulnerabilities.
2. You can use filters to define the vulnerabilities content you want to display in your report. Or select the vulnerabilities you want to include in your report.

3. Click the Generate Report button to open the Configure Report dialog box.
   The filters selected and displayed for the page view are the ones that are populated in the report.

4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

5. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

**Note:** This option is not available when generating reports for assets or asset groups.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, or Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the *Number of records* section, choose the maximum number of records to include on the report. For CSV the options are 20, 50, 100, 500, 1000, or 50 K. For PDF the options are 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the 
   and the 
   icons.

15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.

**USM Anywhere Scans Best Practices**

USM Anywhere provides several kinds of scans that can be done in different ways. This page gives you clearer information about scans, types of scans, the specific ways of doing a scan, the right order for doing scans and avoid asset duplicity, and so on. See USM Anywhere Scheduler Best Practices for more information.

**Discovery Methods**

The following table shows the types of scans that you can run using USM Anywhere.

<table>
<thead>
<tr>
<th>Types of Scans</th>
<th>Information Collected</th>
<th>From Where You Can Do It</th>
<th>Sensors</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active directory (AD)</td>
<td>Inventory Information</td>
<td>• Setup Wizard during your sensor's deployment</td>
<td>Microsoft Azure, Microsoft Hyper-V, and VMware</td>
<td>Completing the Azure Sensor Setup, Completing the Hyper-V Sensor Setup, and Completing the VMware Sensor Setup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At any time from the sensor details page</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Job Scheduler page</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset discovery</td>
<td>Discovers assets in your environment, detects changes in assets, and discovers malicious assets in the network</td>
<td>• Setup Wizard</td>
<td>All</td>
<td>Completing the Hyper-V Sensor Setup, Completing the VMware Sensor Setup, Adding Assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Adding new assets both in a quick and in an advanced way</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Job Scheduler page</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Types of Scans in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Types of Scans</th>
<th>Information Collected</th>
<th>From Where You Can Do It</th>
<th>Sensors</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset group scans</td>
<td>Assets</td>
<td>• Asset groups&lt;br&gt;• Job Scheduler page</td>
<td>All</td>
<td>Running Asset Groups Scans</td>
</tr>
<tr>
<td>Asset scans</td>
<td>Assets</td>
<td>• Assets&lt;br&gt;• Job Scheduler page</td>
<td>All</td>
<td>Running Asset Scans</td>
</tr>
<tr>
<td>Authenticated asset group scans</td>
<td>Assets</td>
<td>• Asset Groups&lt;br&gt;• Job Scheduler page</td>
<td>All</td>
<td>Running Authenticated Asset Groups Scans</td>
</tr>
<tr>
<td>Authenticated asset scans</td>
<td>Assets</td>
<td>• Assets&lt;br&gt;• Job Scheduler page</td>
<td>All</td>
<td>Running Authenticated Asset Scans</td>
</tr>
<tr>
<td>Log collection scans</td>
<td>Log files from an external data source</td>
<td>Job Scheduler page: log collection jobs are initially preset at installation and can't be modified by a user</td>
<td>All</td>
<td>USM Anywhere Scheduler</td>
</tr>
<tr>
<td>Scheduled AD scan jobs</td>
<td>Inventory Information</td>
<td>Job Scheduler page</td>
<td>Microsoft Azure, Microsoft Hyper-V, and VMware</td>
<td>Scheduling Active Directory Scans from the Job Scheduler Page</td>
</tr>
<tr>
<td>Scheduled API scans</td>
<td>Assets</td>
<td>Job Scheduler page</td>
<td>GCP, Microsoft Azure, Microsoft Hyper-V, and VMware</td>
<td>USM Anywhere Scheduler</td>
</tr>
<tr>
<td>Scheduled asset scans</td>
<td>Assets</td>
<td>Job Scheduler page</td>
<td>All</td>
<td>Scheduling Asset Scans from the Job Scheduler Page</td>
</tr>
<tr>
<td>Scheduled asset group scans</td>
<td>Assets</td>
<td>Job Scheduler page</td>
<td>All</td>
<td>Scheduling Asset Groups Scans from the Job Scheduler Page</td>
</tr>
</tbody>
</table>
Types of Scans in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Types of Scans</th>
<th>Information Collected</th>
<th>From Where You Can Do It</th>
<th>Sensors</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Authenticated Asset Scans</td>
<td>Assets</td>
<td>Job Scheduler page</td>
<td>All</td>
<td>Scheduling Asset Scans from the Job Scheduler Page</td>
</tr>
<tr>
<td>Scheduled authenticated asset group scans</td>
<td>Assets</td>
<td>Job Scheduler page</td>
<td>All</td>
<td>Scheduling Asset Groups Scans from the Job Scheduler Page</td>
</tr>
<tr>
<td>User scans</td>
<td>Scheduled user behavior monitoring scan jobs</td>
<td>Job Scheduler Page</td>
<td>All</td>
<td>Scheduling User Discovery Jobs from the Job Scheduler Page</td>
</tr>
</tbody>
</table>

Performance Issues Associated with Scans

When running a scan, keep the following in mind:

- Run API scans first to avoid duplicates and discover the most assets in your environment, and then run asset discovery/asset (group) scans with the Asset Scanner to update the asset. When an asset is discovered through a network scan, and then that asset is discovered through an APIs method, the asset will be duplicated.
- After deploying an agent, link it to existing assets.
- When an AD scan discovers an asset, any asset discovery/asset (group) scan updates the existing asset created by the AD scan.
- Assets discovered by API methods contain far more information than assets discovered by network scans and greatly reduce the risk of having duplicate assets. For example, assets discovered by API methods can include information such as the asset state (powered on, powered off, terminated, and so on), the resources allocated to the asset, or the asset operating system.
- If multiple API methods return the same assets, then use only the method that provides the most assets to prevent duplicate assets. The other API methods can be disabled in the Job Scheduler page. See USM Anywhere Scheduler for more information.
- The following table gives you information about the use of some scan types over other:
## Scans Differences

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>AD Scan</th>
<th>VMware Scan</th>
<th>AWS Scan</th>
<th>Azure Scan</th>
<th>GCP Scan</th>
<th>Agent</th>
<th>Network Scan</th>
<th>Manually Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Asset OS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Depends on information gathered</td>
<td>No</td>
</tr>
<tr>
<td>Host resources</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Asset info updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Depends on information gathered</td>
<td>Depends on information gathered</td>
</tr>
<tr>
<td>Asset state</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No only agent state</td>
<td>No</td>
</tr>
</tbody>
</table>
Open Threat Exchange® and USM Anywhere

AT&T Alien Labs™ Open Threat Exchange® (OTX™) is an open information-sharing and analysis network that provides access to real-time information about issues and threats that may impact your organization, allowing you to learn from and work with others who have already experienced such attacks.

Information in OTX derives from both public and private entities. Alien Labs and other security researchers constantly monitor, analyze, reverse engineer, and report on sophisticated threats including malware, botnets, phishing campaigns, and more. An OTX pulse consists of one or more Indicators of Compromise (IOCs) that constitute a threat or define a sequence of actions that could be used to carry out an attack.

Topics covered in this section include:

- About OTX
- Using OTX in USM Anywhere
- Entering Your OTX Key

USM Anywhere™

User Guide
About OTX

AT&T Alien Labs™ Open Threat Exchange® (OTX™) is a threat data platform that provides open access for all, allowing you to collaborate with a worldwide community of threat researchers and security professionals.

On the OTX page, you can connect the deployed USM Anywhere Sensor to your OTX account. Once connected, the sensor starts to receive raw pulse data from OTX and USM Anywhere correlates that data.

When it detects Indicators of Compromise (IOCs) interacting with assets in your environment, USM Anywhere generates related OTX pulse and IP Reputation-related security events and alarms. The platform consists of these two chief components:

- **Pulses**: Collections of indicators of compromise (IOCs), reported by the OTX community, which other community members review and comment on. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IOCs, reported by the OTX community worldwide. See About OTX Pulses and IOCs.

- **IP Reputation**: Provides notification of communication between known malicious hosts and your assets. See About OTX IP Reputation.

About OTX Pulses and IOCs

The OTX community reports on and receives threat data in the form of pulses. A pulse consists of at least one, but more often multiple, Indicators of Compromise (IOCs).

An IOC is an artifact observed on a network or in an end point, judged with a high degree of confidence to be a threat vector. Examples of threat vectors include campaigns or infrastructures used by an attacker. This table provides a list of IOC types:

<table>
<thead>
<tr>
<th>Indicator of compromise (IOC) types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR Rules</td>
<td>Classless inter-domain routing. Specifies a range of IP addresses on a network that is suspected of malicious activity or attack.</td>
</tr>
<tr>
<td>CVE number</td>
<td>Standards group identification of Common Vulnerabilities and Exposures (CVEs).</td>
</tr>
<tr>
<td>Domains</td>
<td>A domain name for a website or server suspected of hosting or engaging in malicious activity. Domains may also encompass a series of hostnames.</td>
</tr>
<tr>
<td>Email</td>
<td>An email address associated with malicious activity.</td>
</tr>
<tr>
<td>File Hashes (MD5, SHA1, SHA256, PEHP1S4 IMPHASH)</td>
<td>A hash computation for a file that can be used to determine whether contents of a file may have been altered or corrupted.</td>
</tr>
<tr>
<td>File Paths</td>
<td>Unique location in a file system of a resource suspected of malicious activity.</td>
</tr>
<tr>
<td>Hostnames (subdomains)</td>
<td>The hostname for a server located within a domain, suspected of malicious activity.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>An IP address used as the source/destination for an online server or other device suspected of malicious activity.</td>
</tr>
<tr>
<td>MUTEX Name</td>
<td>Mutual exclusion object allowing multiple program threads to share the same resource. Mutexes are often used by malware as a mechanism to detect whether a system has already been infected.</td>
</tr>
<tr>
<td>URI</td>
<td>A uniform resource identifier (URI) that describes the explicit path to a file hosted online, which is suspected of malicious activity.</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform resource locations (URLs) that summarizes the online location of a file or resource associated with suspected malicious activity.</td>
</tr>
</tbody>
</table>
About OTX IP Reputation

OTX IP Reputation identifies IP addresses and domains worldwide that are submitted by the OTX community. IP Reputation verifies them as either malicious or, at least, suspicious until more data comes in to increase their threat ranking. Through its incoming IP data from all of these sources, IP Reputation supplements OTX data with valuable data about actively or potentially malicious activity appearing worldwide that can affect your systems.

IP Reputation Data Sources

IP Reputation receives data from a variety of sources:

- **Open-source intelligence**: Public and private security research organizations.
- **USM Anywhere deployments**: Consists of users who have voluntarily agreed to anonymously share information about external traffic into their network with AT&T Cybersecurity.

**Note**: AT&T Cybersecurity ensures that none of the data shared with OTX can be traced to the contributor or their USM Anywhere deployment.

Who Has Access to IP Reputation?

All USM Anywhere users receive the benefit of IP Reputation data whether or not they sign up for an OTX account.

When you open an OTX account, you may elect to share IP Reputation data with other OTX users. Any data you contribute are anonymous and secure.

**Note**: You can configure USM Anywhere to stop sharing IP Reputation data with OTX at any time by visiting the Open Threat Exchange Configuration page.

IP Reputation Ranking Criteria

IP Reputation uses ranking criteria based on IP Reliability and IP Priority that OTX updates on an ongoing basis to calculate changing assessments to risk level. This helps prevent false positives.

**IP Reliability**

IP Reputation data derives from many data sources of differing reliability. Ranking in this case is based on the relative number of reports regarding a malicious IP in relation to others reported. If, for example, OTX receives 10 reports on a given IP address versus 20 on another, it gives the IP with 10 reports a lower reliability ranking than the IP with 20 reports.

**IP Priority**

OTX ranks IP address priority, based on the behavior associated with each IP address listed. For example, an IP address used as a scanning host receives a lower priority than an IP address known to have been used as a Botnet server.

**Ongoing Ranking Reassessment**

OTX constantly updates its IP Reputation data as new information emerges, affecting IP reliability or priority criteria. Each update re-prioritizes IP reliability and priority values and the threat level of an IP accordingly.

Using OTX in USM Anywhere
When you sign up for and connect your Open Threat Exchange® (OTX) account to your USM Anywhere deployment, it configures USM Anywhere to receive raw pulse data and other IP reputation information. (Reputation data is updated separately from OTX pulse information.)

USM Anywhere then correlates that data with incoming events, alerting you to OTX pulse and IP Reputation-related security events and alarms when it detects IOCs interacting with assets in your environment. Such interactions might consist of malicious IPs communicating with systems, malware detected in your network, or outbound communication with command-and-control (C&C) servers.

Connecting OTX to USM Anywhere helps manage risks and threats in these ways:

- USM Anywhere receives threat updates every 15 minutes in the form of raw data for all pulses to which you subscribe, either directly or through subscriptions to other OTX users.
- You receive updates on your subscribed pulses by email, either individually as they occur or in digest mode.
- You can review an OTX pulse activity feed containing detailed analytics about related threat vectors reported by OTX.
- As soon as you log into USM Anywhere, you can see which pulses are most active in your environment by looking at Open Threat Exchange Dashboard.
- USM Anywhere evaluates IOCs against all events as long as they are generated and generates an alarm when a malicious IP address communicates with any of your assets, or when any other IOCs become active in your network.

OTX Account and OTX Key

USM Anywhere enables you to display OTX information if you have a valid OTX key. Go to Settings > OTX to see the AlienVault Open Threat Exchange (OTX) page.

See Entering Your OTX Key for more information about how to enter your OTX key.

OTX IP Reputation Data Correlated with Events

USM Anywhere maintains an IP reputation list that stores data it receives from OTX about public IP addresses involved in malicious or other suspect activities. Whenever an event has its source or destination IP addresses listed in the IP Reputation list, reputation data will be added to the data stored for the event. This enables USM Anywhere to support some additional features like re-prioritization of events and alarms depending on the IP of the hosts involved.

The IP reputation list maintained by USM Anywhere is stored on the USM Anywhere Cloud. Activity, Reliability, and Priority values provided by OTX are saved with event information for those events having reputation data for either source or destination IP addresses.

The main purpose of the IP reputation list is to provide a list of known or potentially dangerous IP addresses. If any alarm or event is generated by the action of a listed dangerous IP address, then this event will have a smaller probability of being a false positive. This also enables for the recalculation of event/alarm risk depending on its “IP Reliability” and “IP Priority” values.

Note: Reputation events are anonymized and submitted to the AT&T Cybersecurity OTX service for those customers who enable that capability in USM Anywhere. With the feedback received from customer systems and all the other sources AT&T Cybersecurity uses, the IP Reputation values are updated before being redistributed to customers.

Displaying Alarms and Events Based on OTX Pulse and IP Reputation

The USM Anywhere Alarm and Events web UI provides methods of searching for and filtering alarm and security events based on OTX pulse and IP Reputation information. For each event, the database stores associated information on the source and destination IP address provided by OTX, in addition to the activity reported in the event, for example, spamming, phishing, scanning, malware distribution, and so on.
Searching, Filtering, and Viewing Alarms

Different from the way other alarms are processed, USM Anywhere generates an alarm whenever it detects even *one event* associated with an OTX pulse. Alarm correlation begins at that point and proceeds for a period of 24 hours. During this time, USM Anywhere adds any new events related to that pulse to the same alarm.

If any new events related to the pulse occur after that 24-hour period, USM Anywhere generates a second alarm and a new correlation period begins. As an exception to this rule, should an event contain data on record with OTX IP Reputation information, USM Anywhere correlates the alarm, using its standard directive taxonomy.

**Note:** If an OTX pulse is creating too much noise and generating too many false positive alarms, you can always just unsubscribe from the pulse.

USM Anywhere does not offer a filter for IP Reputation-based alarms. However, you can view these within the Alarms list, where they occur. See [Alarms List View](#) for more information.

You can configure the columns/fields related to OTX information to be displayed in the list and save your columns configuration to get back to it whenever you need it. See [Configuring Columns on Alarms](#) for more information.

**Important:** The "Suspicious Behavior - OTX Indicators of Compromise" correlation rule generates alarms if the pulse comes from the AlienVault OTX account.

Searching, Filtering, and Viewing Events

From the USM Anywhere Events main page, you can search for and filter events based on whether OTX pulses exist for source or destination IP addresses, as well as the severity of different IP Reputation scores. See [Events List View](#) for more information.

This screenshot displays the search and filter OTX options:

**Filters Configuration**

**Available Filters**

- otx
- Alarm Destination OTX Activity
- Alarm Source OTX Activity
- Destination OTX Activity
- Destination OTX Priority
- Destination OTX Reliability
- OTX Activities
- OTX Indicators
- OTX Pulses
- Source OTX Activity
- Source OTX Priority

**Selected Filters**

- Suppressed
- Account Name
- Data Source Plugin
- Event Name
- Source Asset
- Sensor
- Asset Groups
- Username
You can configure the columns and fields related to OTX information to be displayed in the list and save your columns configuration to get back to it whenever you need it. See Configuring Columns for more information.

Once you have made your selection, the Event list display will be updated to show only those events matching the IP Reputation criteria you specified, plus OTX pulse information, if you selected that option.

In the Events main page, you can click the icon to display the OTX IP Reputation information available for an event. This icon opens the AlienVault OTX page.

Creating rules using OTX and Threat Intelligence IOC fields

USM Anywhere enables you to create orchestration rules using OTX and threat intelligence Indicator of Compromise (IOC) fields and functions. You can select the OTX and threat intelligence fields as conditions to create an orchestration rule. See Orchestration Rules for more information and this example of how to create an alarm rule using threat intelligence IOC fields.

To create an alarm rule using threat intelligence IOC fields
1. Go to Settings > Rules > Orchestration Rule.
2. Select Create Orchestration Rule > Alarm Rules.
3. Click Add Condition and select the property values you want to include in the rule to create a matching condition.
   - **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.
   - **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.
   - **Important:** Instead of using the equals and equals, case insensitive operators for array fields, AT&T Cybersecurity recommends the use of the in or contains operators.
   - **Note:** If you need to add a property value that maps with a property key, you need to know the mapping of the field. See Determining the Mapping of a Field for more information.
4. (Optional.) Click Add Group to group your conditions.
   - **Note:** See Operators in the Orchestration Rules for more information.
5. Click Next.
6. Enter a name for the rule.
7. Select an intent.
   - The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See intent for more information about the available threat categories.
8. Enter a method.
   - If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.
   - **Note:** This is a required field; if you do not complete this field, the Save button remains inactive.
9. Select a strategy.
   - The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.
10. Enter a priority.
11. Configure a mute value.

Once an alarm is created, you can set the time that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

12. Modify these two options:

- **Occurrences**: Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length**: Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

   ![Occurrences and Length](image)

   In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

13. Select the fields that you want to display in the generated alarm.

   You can select or remove the fields you want to include in the details of the alarm by clicking the ➔ and the ◀ icons.

14. Click **Save**

   The created rule displays in the list of rules. See [Alarm Rules from the Orchestration Rules Page](#) for more information.

---

**Entering Your OTX Key**

You need to **sign up for an AT&T Alien Labs™ Open Threat Exchange® (OTX™) account** and have an **OTX key** if you want USM Anywhere to receive alerts based on any threat in OTX.
To enter your OTX key in USM Anywhere

1. Go to **Settings > OTX**.

2. Enter the OTX key you obtained from the OTX API page.

3. Select the look-back period. See **The Look-Back Period** for more information.

4. Click **Validate OTX Subscription Key**.

A message displays at the top of the page to inform you about the success of the subscription and the Valid OTX Key is green.

To delete the OTX Subscription

1. Go to **Settings > OTX**.

2. Click **Delete OTX Subscription**.

A message displays at the top of the page to inform you about that the subscription has been deleted.

---

**Note:** USM Anywhere displays if the subscription is enabled and if the OTX pulses are up-to-date. If the OTX pulses are not up-to-date, USM Anywhere displays when they have been updated.
The Look-Back Period

USM Anywhere enables you to configure a period of time, called a look-back period, for receiving raw pulse data from OTX. The look-back period helps your environment to be more effective and agile. Threats are continuously changing, and it is important to have this data updated. In addition, Indicators of Compromise (IOCs) get old quickly and an IP address that was a threat three months ago may not be now.

**Note:** The configuration of a look-back period helps you to avoid alarms generated by old pulses and without a current value.

You can define a look-back period, which uses pulses from the current date back for a certain range of time that you choose. These are the look-back period options from which you can choose:

- **1 month:** Select this option to use pulses from the current day to the previous month.
- **3 months:** Select this option to use pulses from the current day to the previous 3 months.
- **6 months:** Select this option to use pulses from the current day to the previous 6 months.
- **1 year:** Select this option to use pulses from the current day to the previous year.
- **Unlimited:** Select this option to use pulses without a restriction of time.

**Important:** The longer the selected period is, the longer time it takes to receive the pulses.

**Note:** Keep in mind that the range of the look-back period that you choose adjusts according to what is the current day of the month. This means that, for example, if you have chosen the **1 month** option and it is the first day of the month, you will receive pulses from the previous month, and when it is the fifth day of the month, you will receive pulses from that fifth day of the month to the fifth day of the previous month.

To update the look-back period:

1. Go to **Settings > Threat Intelligence**.
2. Change the look-back period.
3. Click **Update**.

A message displays at the top of the page to inform you that the OTX Subscription has been updated.

**Important:** Keep in mind that it takes some time if you update the look-back period, depending on your selection.
USM Anywhere Sensor Management

USM Anywhere Sensors deploy into each environment and help you gain visibility into all of your on-premises and cloud environments. USM Anywhere Sensors collect and normalize logs, monitor networks, and collect information about the assets deployed in your environments.

After you install and set up the USM Anywhere Sensor, it communicates with USM Anywhere in the cloud about the assets in your network. The USM Anywhere Sensor then transfers any available raw log data to USM Anywhere in the cloud for correlation and event generation, among other things.

**Note:** The number of sensors that you can add to your environment depends on your USM Anywhere license. You can go to **Settings > My Subscription** to view the number of licensed sensors. See **Subscription Management** for more information.

This topic discusses these subtopics:

- Sensors Page Overview ................................................................. 585
- Adding a New Sensor ................................................................. 587
- Configuring a Sensor ................................................................. 590
- Editing a Sensor ........................................................................... 591
- Assigning a Sensor .................................................................... 591
- Redeploying a Sensor ............................................................... 593
- Deleting a Sensor ....................................................................... 595
- Sensor Disconnected from the USM Anywhere Service .............. 596
The Sensors page enables you to add new sensors, configure the deployed sensors, delete and redeploy sensors, and edit a sensor for modifying the name or description. Go to Data Sources > Sensors to open the Sensors main page. The page displays the list of sensors you have deployed in your environment.

The following table lists the default columns in the Sensors page.

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
<td>Name of the deployed sensor. The type of sensor is displayed below the name.</td>
</tr>
<tr>
<td>Description</td>
<td>Text identifying the sensor.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address assigned to the sensor.</td>
</tr>
<tr>
<td>Version</td>
<td>Installed version of the sensor.</td>
</tr>
</tbody>
</table>
List of the Default Columns in the Sensors Page (Continued)

<table>
<thead>
<tr>
<th>Column Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Status</td>
<td>Status of the sensor, which can be the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Waiting for connection</strong>: The sensor has been added to the system, but it is not connected.</td>
</tr>
<tr>
<td></td>
<td><strong>Connected</strong>: The sensor is connected, but it is still initializing and performing configurations.</td>
</tr>
<tr>
<td></td>
<td><strong>Connection lost</strong>: The sensor has lost the connection. (Logs, including NXLog messages, are cached locally and will be forwarded to USM Anywhere when the connection resumes.)</td>
</tr>
<tr>
<td></td>
<td><strong>Ready</strong>: The sensor is connected and configured.</td>
</tr>
<tr>
<td>Configured</td>
<td>Icon to indicate if the sensor is configured (✔) or not (❌).</td>
</tr>
</tbody>
</table>

The ✍ icon only displays when the sensor is not configured. Use this icon to go back to the wizard and finish the sensor configuration.

Use the ✍ icon to modify the sensor name or the sensor description. See Editing a Sensor for more information.

Use the 🗑 icon to delete the sensor and deploy a new one. See Redeploying a Sensor for more information. You can also use this button to delete the sensor permanently. See Deleting a Sensor for more information.

You can also click a sensor to display the specific information about that sensor. See Configuring a Sensor for more information.

Sensors Running on an Outdated Version of USM Anywhere

USM Anywhere doesn't support sensors running on an outdated version of USM Anywhere. When USM Anywhere identifies a configured sensor running on an outdated version, a yellow announcement displays to warn you about it. See Configure Network Interfaces for On-Premises Sensors to confirm that the sensor on an outdated version meets the proper requirements and contact AT&T Cybersecurity Technical Support for assistance.
Adding a New Sensor

Role Availability

After your USM Anywhere service is provisioned and running, you can add and deploy new sensors as needed. For these sensors, instead of receiving an authentication code from AT&T Cybersecurity, you must generate the license key for any new sensor you intend to add from within the USM Anywhere web user interface (UI). The rest of the sensor deployment process is the same as the first one.

Note: The number of sensors that you can add to your environment depends on your USM Anywhere license. You can go to Settings > My Subscription to view the number of licensed sensors. See Subscription Management for more information.

To check your allowed USM Anywhere Sensors

1. Go to Settings > My Subscription to open the page.
2. Check the allowed sensors you have and the license end date. The displayed date depends on your computer's time zone.

My Subscription

<table>
<thead>
<tr>
<th>License Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LICENSE TYPE</td>
<td>Standard 30-Days</td>
</tr>
<tr>
<td>LICENSE END DATE</td>
<td>Fri. January 01 21:00</td>
</tr>
<tr>
<td>SERVICE TIER</td>
<td>500 GB per month</td>
</tr>
<tr>
<td>LICENSED SENSORS</td>
<td>5</td>
</tr>
<tr>
<td>ACTIVE SENSORS</td>
<td>5</td>
</tr>
<tr>
<td>MONTHS OF COLD STORAGE FOR RAW LOGS</td>
<td>12</td>
</tr>
</tbody>
</table>
To add a new sensor

1. Deploy your sensor.

   Follow the instructions based on your sensor type:
   - **AWS Sensor:** See [Deploy the AWS Sensor](#) for more information.
   - **Azure Sensor:** See [Deploy the USM Anywhere Sensor from the Azure Marketplace](#) for more information.
   - **GCP Sensor:** See [Deploy the GCP Sensor](#) for more information.
   - **Hyper-V Sensor:** See [Create the Hyper-V Virtual Machine](#) for more information.
   - **VMware Sensor:** See [Create the VMware Virtual Machine](#) for more information.

2. Obtain an authentication code for the new sensor.
   a. In USM Anywhere, go to **Data Sources > Sensors**.
   b. Click **New Sensor**.

   ![Note: If your USM Anywhere License does not allow you to create more sensors, this button will remain inactive.](#)

   The dialog box displays an authentication code for the new sensor. This code starts with an "S".

   ![New Sensor](#)
Important: This code will expire in 24 hours.

Note: While the authentication code used for the very first sensor you create begins with a "C", any additional sensors are authenticated with codes beginning with "S".

c. Click the icon to copy the code to your clipboard.

3. Register your sensor.

Click or enter the URL of your sensor to get to the setup page. It prompts you to provide the following information:

a. Enter a name and description for the sensor.

b. In the field with the key icon ( ), paste the sensor authentication code you copied.

c. In the field with the computer icon ( ), copy and paste the URL of your existing instance.

For example, if the subdomain with which you registered with AT&T Cybersecurity was "mycompany", the URL would be mycompany.alienvault.cloud for USM Anywhere, or mycompany.gov.alienvault.us for AT&T TDR for Gov.

d. Click Start Setup.
A progress dialog box displays a status message.

Connecting USM Anywhere Sensor

When the connection is complete, a confirmation message opens.

**WELCOME TO USM ANYWHERE SENSOR SETUP**

USM Anywhere Sensor has been successfully configured.
To access USM Anywhere Click Here

---
e. Click the link to open the USM Anywhere web UI.

Upon login, this displays the USM Anywhere Sensor Configuration page with the connected sensor listed in the page.

4. Configure your sensor.

Follow the instructions based on your sensor type:

- **AWS Sensor**: See Complete the AWS Sensor Setup for more information.
- **Azure Sensor**: See Complete the Azure Sensor Setup for more information.
- **GCP Sensor**: See Complete the GCP Sensor Setup for more information.
- **Hyper-V Sensor**: See Complete the Hyper-V Sensor Setup for more information.
- **VMware Sensor**: See Complete the VMware Sensor Setup for more information.

**Note:** If you do not want to complete the sensor setup immediately, you can click Start Using USM Anywhere at the bottom of the page. However, AT&T Cybersecurity strongly recommends that you do so now, because you must complete the sensor setup before you can use it.

5. Go to **Data Sources > Sensors** to open the page.

6. Check in the list of sensors that your new sensor is on the list, ready, and well-configured.

### Configuring a Sensor

**Role Availability**  

- Read-Only
- Analyst
- Manager

USM Anywhere enables you to modify the configuration data of your sensor.
To configure a sensor

1. Go to **Data Sources > Sensors** to open the page.
2. Click the sensor you want to configure.
   
   The specific information about the sensor displays. The tabs are similar to the Setup Wizard. See the **Setup Wizard** documentation for more information.
3. Click the available tabs to modify the data of the items that need to be modified.

**Editing a Sensor**

This option enables you to change the sensor name and the description of a sensor.

To edit a sensor

1. Go to **Data Sources > Sensors** to open the page.
2. Click the icon of the sensor you want to edit.
3. Modify the sensor name or the sensor description.

4. Click **Save**.

**Assigning a Sensor**
All assets that are detected by a sensor in the scan of your network are assigned automatically to that sensor. If you have several sensors, the asset will be assigned to the sensor that has detected the asset. An asset cannot be assigned to more than one sensor.

It is best practice to identify, prioritize and organize assets. By doing so, you can limit the scope of network security audits to subsections of your network, making scan results more manageable. You can also more easily distribute assets to multiple users to facilitate the delegation of responsibilities. USM Anywhere provides a way of organizing your assets. If you have more than one sensor configured and you want to organize your assets in your network, you may want to assign a different sensor from the one that was assigned automatically.

For this reason, you may need to edit shared properties of some assets to assign a sensor. Luckily you do not have to edit these assets one by one. Instead, you can select all the relevant assets and modify their shared properties in one go. USM Anywhere enables you to perform the following tasks for your own asset organization, which saves time and resources:

- set a sensor to an asset if you want to change the one that was assigned automatically.
- set multiple assets at the same time. You can do this by performing a bulk operation. You can set a sensor to several assets at the same time if you want to have certain assets assigned to a particular sensor.
- set a sensor to an asset group if you want to have a group of assets assigned to a particular sensor.

To assign a sensor to an asset or a set of assets

1. Go to Environment > Assets.
2. Select the assets you want to assign. See Selecting Assets in Asset List View.

USM Anywhere™ User Guide
592
4. Select the sensor you want to assign the selected assets.

Choose Sensor
This sensor will be assigned to all selected assets

5. Click Save.

To assign a sensor to an asset group

1. Go to Environment > Asset Groups.
2. Click the icon close to the asset group name and select Full Details.
4. Select the sensor you want to assign the selected asset group.
5. Click Save.
USM Anywhere enables you to redeploy a sensor when needed. If you redeploy a sensor, all the assets, AlienVault Agents, events, alarms, rules, and scheduler jobs are kept and linked to the new sensor. If you delete the sensor instead, you will lose all the information related to that sensor.

However, when a sensor is redeployed, the disk and memory states of the old sensor are discarded. Customer-specific configurations, stored on the sensor due to compliance constraints, are lost. Therefore, you must redo the following configurations after redeploying a sensor:

- All the settings you have modified for the old sensor.

  You can find these settings under Data Sources > Sensors, and then select your sensor. This includes the credentials to access your virtual environment and your Active Directory (AD) settings.

- All the certificates you have uploaded for log forwarding, which can be Graylog, syslog, or NXLog.

  You can find these settings under Data Sources > Sensors, on the Sensor Apps tab.

- All the AlienApp configurations you have entered.

To redeploy a sensor

1. Go to Data Sources > Sensors to open the page.
2. Click the icon of the sensor you want to redeploy.
3. Click Delete this sensor and deploy a new one.

   A dialog box opens showing the authentication code that you need for activating the new sensor. Copy the code for later usage.

4. Deploy the sensor following the instructions in the Deployment Guide. Depending on the type of sensor, you must follow different instructions.

   ![Note: AT&T Cybersecurity recommends that you keep the same IP address as the old sensor to minimize reconfiguration efforts.]

5. Connect the new sensor using the authentication code you have copied.

   This code instructs USM Anywhere to link the assets, AlienVault Agents, events, alarms, rules, and scheduler jobs on the old sensor to the new sensor.

6. Configure your USM Anywhere Sensor following the steps in the Setup Wizard. See the Setup Wizard documentation for more information.
7. Redo the relevant configurations discussed at the beginning of this section.
8. Verify that the redeployed sensor can receive data from your network.
Deleting a Sensor

USM Anywhere enables you to delete completely a sensor from your environment. Keep in mind that if you delete a sensor, you will delete all assets and jobs related to that sensor.

To delete a sensor

1. Go to **Data Sources > Sensors** to open the page.
2. Click the icon of the sensor you want to delete.
3. Click **Delete this sensor permanently**.

The deleted sensor is not displayed in the list of sensors.

**Important:** Keep in mind that if you terminate an AWS instance, an Azure virtual machine, GCP virtual machine, or a VMware virtual machine, any assets that have vulnerabilities associated with them will not be automatically deleted when the discovery scan finds them terminated in AWS, Azure, or VMware vCenter/vSphere.
Sensor Disconnected from the USM Anywhere Service

USM Anywhere Sensors sometimes disconnect from the USM Anywhere service (for example, during an update process). There is a process every hour to verify if the sensor has been disconnected for 30 minutes or longer. When this happens, USM Anywhere informs users in a Manager role by email and generates an event. A new event is generated every 30 minutes until the sensor reconnects.

**Warning:** Currently, the Sensor Appears Offline and Sensor Reconnected events are generated at the same time as the regular events and system events. Soon, these events will be generated only as system events. See Regular Events and System Events, Orchestration Rule for the "Sensor Appears Offline" System Event, and Orchestration Rule for the "Sensor Reconnected" System Event for more information.

**Note:** Logs, including NXLog messages, are cached locally and will be forwarded to USM Anywhere when the connection resumes.

When a sensor disconnects from the USM Anywhere service, it sends an email notice within two hours to the email address you used to sign into USM Anywhere (as long as you are in a Manager role).
role). This notice informs you that your sensor is not connected. You can immediately take action to restore your service either by working with AT&T Cybersecurity Technical Support or by making an environmental, network connectivity change.

The notification will be generated daily until the sensor is reconnected. After seven days, the notifications will no longer be issued.

USM Anywhere checks every hour to verify whether the sensor has been reconnected. After your sensor reconnects, you receive an email notification informing you that your service has been restored. Because of this automated notification, you do not have to log in to the product to check the sensor connection status. USM Anywhere generates an event when a sensor reconnects.

Important: If you are not receiving notifications of a disconnection, or your notifications are being sent outside of the expected window, that could indicate issues in your control node. See View Network Testing Information for instructions on how to verify your control node’s connection.

Creating an Alarm Rule from These Events

Although USM Anywhere informs users in a Manager role by email when a sensor has been disconnected from the service and when the sensor has been reconnected, you can create an alarm rule to have more control when these events occur. The following activity is an example of how to create an alarm rule from the sensor offline event. You can do the same for the sensor reconnected event by entering reconnected in step 2.
To create an alarm rule from the Sensor Appears Offline event

1. Go to **Activity > Events**.

2. Enter **offline** in the Enter search phrase field.

3. Click one of the events.

4. Select **Create Rule > Create Alarm Rule**.

   ![Create Alarm Rule dialog box](image)

   The Create Alarm Rule dialog box opens.

5. Select a packet type in the Match drop-down list.
The first match criteria for all rules must be the packet_type detail field:

- **Logs**: Use this packet type for event-based rules.
- **Warnings**: Use this packet type for configuration issues-based rules.
- **Vulnerabilities**: Use this packet type for vulnerabilities-based rules.

6. Click **Add Conditions** and select these properties values:

7. Click **Next**.
8. Enter a name for the rule.
9. (Optional.) Enter a description for identifying this rule.
10. Select an intent.

---

1This packet type refers to configuration issues that are used to identify incorrect uses of certain features. For example, the app for AWS assesses your configuration of AWS to identify insecure use of the AWS security features.
The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See Intent for more information about the available threat categories.

11. Enter a method.

If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.

**Note:** This is a required field; if you do not complete this field, the Save button remains inactive.

12. Select a strategy.

The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the strategy the malicious user is using to achieve their goal.

13. Enter a priority.

See Priority Field for Alarms for more information.

14. Configure a mute value.

Once an alarm is created, you can set the time that USM Anywhere will not create a new alarm based on the same conditions. This configured time is the mute value, and you can specify it in seconds, minutes, and hours.

15. Modify these two options:

- **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.

- **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.
16. (Optional.) Select the fields that you want to display in the generated alarm.

You can select or remove the fields you want to include in the details of the alarm. A field passes from one column to the other by clicking it.

17. Click **Save**.

The created rule displays in the list of rules. You can see it from **Settings > Rules > Orchestration Rules**. See **Orchestration Rules** for more information.

### The AWS Cloud Connector in USM Anywhere

The Amazon Web Services (AWS) Cloud Connector provides operational visibility into the security of your AWS environment. Based on the collected log information, USM Anywhere receives the data stored in your Amazon Simple Storage Service (S3) buckets, generates the related events for that data within USM Anywhere, and provides real-time alerting to identify malicious activity.

After you install and enable the AWS Cloud Connector, it communicates with USM Anywhere in the cloud about the data stored in your Amazon S3 buckets. See **AWS Cloud Connector** for more information.

This topic discusses these subtopics:

- **Cloud Connector List View** ................................................................. 602
- **Adding an AWS Cloud Connector** .................................................... 603
- **Viewing AWS Cloud Connector Details** ......................................... 607
- **Editing an AWS Cloud Connector** ................................................... 612
- **Downloading an Existing AWS Cloud Connector Template** ............... 613
- **Cloud Connectors System Events** ..................................................... 618
- **Deleting an AWS Cloud Connector** .................................................. 621
Cloud Connector List View

Through USM Anywhere you can manage your Amazon Web Services (AWS) Cloud Connector according to your needs. The AWS Cloud Connector page enables you to add new Cloud Connectors, edit deployed Cloud Connectors, delete and redeploy Cloud Connectors, and edit a Cloud Connector to modify its name or description. Go to Data Sources > Cloud Connectors to open the Cloud Connectors main page.

The page displays the list of AWS Cloud Connectors you have deployed in your environment.

The following table lists the default columns that appear in the AWS Cloud Connector list view, and their descriptions.

List of the Default Columns in the AWS Cloud Connectors Page

<table>
<thead>
<tr>
<th>Columns Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>Name of the deployed Cloud Connector.</td>
</tr>
<tr>
<td>Account ID</td>
<td>Identifier (ID) of the AWS account.</td>
</tr>
<tr>
<td>Type</td>
<td>The Cloud Connector type. This value is always AWS S3.</td>
</tr>
</tbody>
</table>
| Status             | Status of the Cloud Connectors, which can be the following:
|                    | **Awaiting configuration**: The Cloud Connector has been added to the USM Anywhere environment, but it hasn't been configured in your cloud account. |
|                    | **Active**: The Cloud Connector is connected and configured. |
|                    | **Disabled**: The Cloud Connector isn't enabled. |
|                    | **Idle**: The Cloud Connector hasn't received data in the last hour. |
|                    | **Not receiving data**: The Cloud Connector hasn't received data in the latest 24 hours. |
|                    | **Offline**: The Cloud Connector is offline. |
### List of the Default Columns in the AWS Cloud Connectors Page (Continued)

<table>
<thead>
<tr>
<th>Columns Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error (24 HRS)</td>
<td>Errors in the latest 24 hours. You can click the number of a row to open the errors tab. See Viewing AWS Cloud Connector Details for more information.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Icon to indicate and change the Cloud Connector from enabled (✔) to (✘) or vice versa.</td>
</tr>
</tbody>
</table>

Use the icon ☰ to expand the specific information about an AWS Cloud Connector. There is a graph to see the bucket events by the latest 24 hours or past seven days, and a button to download the associated AWS CloudFormation template. You can click the number below the errors columns to open and see the detected errors. See Viewing AWS Cloud Connector Details for more information.

#### Adding an AWS Cloud Connector

**Role Availability**

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

It is necessary to add an Amazon Web Service (AWS) Cloud Connector into USM Anywhere to enable it to receive the data stored in your Amazon Simple Storage Service (S3) buckets, generate the related events in USM Anywhere with that data, and provide real-time alerting to identify malicious activity.
To add an AWS Cloud Connector

1. Go to Data Sources > Cloud Connectors.

2. Click Add Connector.
The Add New Connector dialog box opens.

3. The AWS Cloud Connector type is already selected.

4. Enter your AWS account identifier (ID).

5. Select the region where you want to deploy the Amazon Web Services (AWS) CloudFormation template.

6. (Optional.) Enter a name for your AWS Cloud Connector.

7. Click **Next**.
Add New Connector

Connector Type
AWS S3

AWS Account ID
[ redacted ]

Region
us-west-1

Connector Name
AWS_West_Connector

Download AWS Configuration Template

Download your template then log into your AWS environment and go to CloudFormations to create your stack. Once you’ve configured your connector in AWS, return to USM Anywhere to enable your connector and begin logging data. Learn more about configuring your connector in AWS.

[Download Template]
8. (Optional.) Click **Download Template**.

   See [Downloading an Existing AWS Cloud Connector Template](#) for more information.

9. Click **Done**.

   **Note:** USM Anywhere generates a console user event when an AWS Cloud Connector is created, modified, enabled, disabled, or deleted. See [USM Anywhere Console User Events List View](#) for more information.

### Viewing AWS Cloud Connector Details

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

The Amazon Web Services (AWS) Cloud Connector details page provides in-depth information on an AWS Cloud Connector. There is a graph to see the bucket events in the latest 24 hours, and seven days, and a button to download the AWS CloudFormation template. You can also find the details of the buckets related to that Cloud Connector and see any detected errors.

**To view the details of an AWS Cloud Connector**

1. Go to **Data Sources > Cloud Connectors** to open the page.
2. Click the . . . icon of the sensor for which you want to view its details, and then select **View Connector**.

    **Cloud Connectors**

    ![Cloud Connector Details](Image)

    Use the ☑ icon to disable the AWS Cloud Connector.
Click the Errors tab to see the detected errors.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Source</th>
<th>Detected On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error getting the S3 Object</td>
<td></td>
<td>Thu, Jan 10, 2022, 06:23 PM CET</td>
</tr>
<tr>
<td>Error getting the S3 Object</td>
<td></td>
<td>Mon, Jan 10, 2022, 05:43 PM CET</td>
</tr>
<tr>
<td>Error getting the S3 Object</td>
<td></td>
<td>Wed, Jan 12, 2022, 07:15 AM CET</td>
</tr>
</tbody>
</table>

**Data Source Rules**

USM Anywhere enables you to add and apply rules to files stored in your Amazon Simple Storage Service (S3) bucket. Using a rule, USM Anywhere can match a file with a specific data source and generate the related events. If the file doesn't match with a data source, then USM Anywhere will create an event as an AlienVault Generic Data Source. See AlienVault Generic Data Source for more information.

**To open the Data Source Rules tab**

1. Go to Data Sources > Cloud Connectors to open the Cloud Connectors main page.
2. Click the icon of the cloud connector for which you want to open the data source rules tab, and then select View Connector.
3. Click the Data Source Rules tab.
To add a rule

1. Go to **Data Sources > Cloud Connectors** to open the Cloud Connectors main page.
2. Click the **...** icon of the cloud connector for which you want to add a rule, and then select **View Connector**.
3. Click the **Data Source Rules** tab.
4. Click **Add Rule**.

The Add New Data Source Rule dialog box opens.

5. In the **Connector Source** field, choose the Amazon S3 bucket.

   You can choose one of them or all.

6. (Optional.) In the **Filenames Matching With [optional]** field, use regular expressions (regex) to specify a pattern that must be followed by the files.

   If you don't specify anything, USM Anywhere will match all files in the Amazon S3 bucket with the specified data source. See **Using Regular Expressions in USM Anywhere** for more information.

   For example:

   ```
   /**AWSLogs\595129146488\CloudTrail
   ```
This expression pattern means that all files inside the CloudTrail folder will match with the rule.

Important: If the file-name is not matching any rule, USM Anywhere tries to identify the data source based on the file-name and the event format. The events are parsed as generic if the data source can't be identified.

7. In the Data Sources field, enter the data source you want to match with the files.

If you enter more than one data source, USM Anywhere will try to match with the first data source. If USM Anywhere can't generate an event, then it will try to match with the following data source, and so on. If the file doesn't match with any data source, then USM Anywhere will create an event as an AlienVault Generic Data Source. See AlienVault Generic Data Source for more information.

8. Click Save.

To edit a rule

1. Go to Data Sources > Cloud Connectors to open the Cloud Connectors main page.
2. Click the icon of the cloud connector for which you want to edit the rule, and then select View Connector.
3. Click the Data Source Rules tab.
4. Click the icon of the connector source you want to edit the rule.

The Edit Data Source Rule dialog box opens.
5. Modify the data of the items that need to be modified.
6. Click **Save**.

**To delete a rule**

1. Go to **Data Sources > Cloud Connectors** to open the Cloud Connectors main page.
2. Click the icon of the sensor for which you want to open the data source rules tab, and then select **View Connector**.
3. Click the **Data Source Rules** tab.
4. Click the icon of the connector source to which you want to delete the rule.
The data source rule delete dialog box opens.

5. Click **Delete**.

**Editing an AWS Cloud Connector**

USM Anywhere enables you to edit an Amazon Web Service (AWS) Cloud Connector. This option enables you to change the region where you want to deploy the AWS CloudFormation template and the name of your AWS Cloud Connector.

**To edit an AWS Cloud Connector**

1. Go to **Data Sources > Cloud Connectors** to open the page.
2. Click the *** icon of the sensor for which you want to edit, and then select **Edit Connector**.

   The Edit Connector dialog box opens.
3. Modify the region or the name of your AWS Cloud Connector.

4. Click **Save**.

**Note**: USM Anywhere generates a console user event when an AWS Cloud Connector is created, modified, enabled, disabled, or deleted. See [USM Anywhere Console User Events List View](#) for more information.

## Downloading an Existing AWS Cloud Connector Template

USM Anywhere helps you in generating an Amazon Web Service (AWS) CloudFormation template that you need for gathering data from your Amazon Simple Storage Service (S3) buckets.
To download an Amazon Web Services (AWS) Cloud Connector template from the Cloud Connectors main page

1. Go to **Data Sources > Cloud Connectors**.

2. Click the icon to expand the specific information about the AWS Cloud Connector whose template you want to download.

3. Click **Download Template**.
   
   The `s3connector-template.json` file downloads. This is the default name of the file, but you can change it.

4. Open your AWS Management Console page and upload the template.
   
   See [Uploading AWS CloudFormation Templates](#) for more information.

To download an AWS Cloud Connector template from the details page of a Cloud Connector

1. Go to **Data Sources > Cloud Connectors**.

2. Click the icon of the sensor for which you want to download the template, and then select **View Connector**.
3. Click **Download Template**.

   The `s3connector-template.json` file downloads. This is the default name of the file, but you can change it.

4. Open you AWS Management Console page and upload the template.

   See [Uploading AWS CloudFormation Templates](#) for more information.

**To download an AWS Cloud Connector template when you add a Cloud Connector**

1. Go to **Data Sources > Cloud Connectors**.
2. Click **Add Connector**.

   The Add New Connector dialog box opens.

3. Select the AWS Cloud Connector type in case you have more than one.
4. Enter your AWS account identifier (ID).
5. Select the region where you want to deploy the AWS CloudFormation template.
6. (Optional.) Enter a name for your AWS Cloud Connector.
7. Click Next.
Add New Connector

Connector Type
AWS S3

AWS Account ID
US-APR0000W

Region
us-west-1

Connector Name
AWS_West_Connector

Download AWS Configuration Template

Download your template then log into your AWS environment and go to CloudFormations to create your stack. Once you’ve configured your connector in AWS, return to USM Anywhere to enable your connector and begin logging data. Learn more about configuring your connector in AWS.

Download Template
8. Click Download Template.

The `s3connector-template.json` file downloads. This is the default name of the file, but you can change it.

9. Open your AWS Management Console page and upload the template.

See Uploading AWS CloudFormation Templates for more information

Cloud Connectors System Events

USM Anywhere generates system events when your Amazon Web Services (AWS) Cloud Connector fails and there is an error in an Amazon simple Storage Service (S3) file. Through these events, you have the option of retrying to process the Amazon S3 file.

To retry an Amazon S3 collector error

1. Go to Settings > System Events to open the System Events main page.
2. Use the Event Name filter to search the AWS S3 collector errors.

See Searching System Events for more information.
3. Click the **Error processing S3 bucket notification** filter.

The result of your search displays with the errors identified.
4. Click the error you want to retry.
   
   The specific error dialog box opens.

5. Click **Retry**.
Deleting an AWS Cloud Connector

Note: After clicking **Retry**, USM Anywhere tries to process the file again. If the file can't be read, a new system event is generated.
USM Anywhere enables you to completely delete an Amazon Web Services (AWS) Cloud Connector from your environment.

**To delete an AWS Cloud Connector**

1. Go to **Data Sources > Cloud Connectors** to open the page.
2. Click the **...** icon of the sensor for which you want to delete, and then select **Delete**.

   The Delete Cloud Connector dialog box opens.

   ![Delete Cloud Connector dialog box]

3. Click **Delete**.

**Note:** USM Anywhere generates a console user event when an AWS Cloud Connector is created, modified, enabled, disabled, or deleted. See **USM Anywhere Console User Events List View** for more information.
Subscription Management

With a USM Anywhere license, you can always view your subscription data in one place. Use the My Subscription page to access your license information, event data, and raw log data, and to connect to a USM Central instance.

Subscription Data

Go to Settings > My Subscription to open the page.

The following table lists the fields you see on the page.
## Information on the My Subscription Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Usage</td>
<td></td>
</tr>
<tr>
<td>Total Searchable Data</td>
<td>The total remaining data available in the hot storage.</td>
</tr>
<tr>
<td>Consumed Data</td>
<td>The amount of data USM Anywhere has processed every month.</td>
</tr>
<tr>
<td>Projected Data Consumption</td>
<td>The amount of data already stored for the month plus calculated data storage needs for the rest of the month. See <a href="#">Projected Data Consumption</a> for more information.</td>
</tr>
<tr>
<td>Sensors</td>
<td>The number of licensed sensors and pending deployment sensors. Click <strong>Manage Sensors</strong> to open the Sensors page. See <a href="#">Sensors Page Overview</a> for more information.</td>
</tr>
<tr>
<td>Purge Event Data</td>
<td>The ability to purge data will soon be deprecated.</td>
</tr>
<tr>
<td>EPS</td>
<td>Events per second (EPS) in the last 24 hours.</td>
</tr>
<tr>
<td>Filtered EPS</td>
<td>Percentage of filtered EPS in the last 24 hours.</td>
</tr>
<tr>
<td>Filtering Rules</td>
<td>Number of filtering rules in your environment. Click <strong>Manage Rules</strong> to open the Filtering Rules page. See <a href="#">Filtering Rules from the Orchestration Rules Page</a> for more information.</td>
</tr>
</tbody>
</table>

### License Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Type</td>
<td>Either the trial or subscription license.</td>
</tr>
<tr>
<td>Service Tier</td>
<td>The monthly storage limit. See <a href="#">AT&amp;T Cybersecurity pricing page</a> for details or to request a quote.</td>
</tr>
</tbody>
</table>

**Important:** Tier options do not have unlimited processing power, memory allotment, or disk input/output (I/O) speeds. In addition to storage per month, your deployment size’s impact on any of these factors will influence which tier option is right for your environment. AT&T Cybersecurity recommends pre-deployment sizing discussions with your sales representative to help select the right tier for you.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License End Date</td>
<td>Either the trial expiration date (for trial licenses) or support end date (for subscription licenses). The displayed date depends on your computer’s time zone.</td>
</tr>
</tbody>
</table>
### Information on the My Subscription Page (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cold Storage        | Click **Export Raw Logs** to download the raw log files in ZIP format. See **Raw Log Data** for more information. By default, cold storage is unlimited for USM Anywhere customers within their service terms, but unlimited for AT&T Threat Detection and Response for Government (AT&T TDR for Gov) customers for three years. Keep in mind these points:  
  - You can export raw logs for a 31-day month, but you are limited to a 30-day span if the range exceeds a single month.  
  - The start time is 00:00:00 on the start date selected, and the end time is 23:59:59 on the end date selected. So if you select from 1/1/2020 to 2/1/2020, the logs start at 00:00:00 1/1/2020 and end at 23:59:59 2/1/2020. |
| Email               | Email address associated with your license.                                                                                                                                                        |
| MSSP Status         | Indicates whether the USM Anywhere deployment has been successfully connected to a USM Central or not. See **Connecting a USM Anywhere to a USM Central** for more information.                                    |
| MSSP Service        | Name of the connected USM Central deployment.                                                                                                                                                    |
| Historical Data Consumption | A list of data consumption by month. Click **Download CSV** for downloading a file with this information.                                                                                  |
| Top Data Sources    | Displays a list of the top data sources. Click **Download CSV** for downloading a file with this information.                                                                                     |
| Top Event Names     | List of the top event names related to their data source. Click **Download CSV** for downloading a file with this information.                                                                  |
| Top Reporting Devices | List of top reporting devices. Click **Download CSV** for downloading a file with this information.                                                                                          |

### Raw Log Data

Raw log data is data that has been forwarded through your sensors. USM Anywhere stores this data and enables you to extract raw log data for audit purposes or further forensic analysis.

**Important:** AT&T Cybersecurity recommends that you download the raw log data on a monthly basis.

When requesting raw log files, the date range cannot exceed 30 days. To download more than 30 days' worth of data, you must make multiple requests. Refrain from making all requests at the same time, which may tie up your USM Anywhere instance. You can make 2 or 3 requests, wait for the emails to arrive, and then make your next requests.
To extract raw log data

1. Go to **Settings > My Subscription**.
2. Click **Export Raw Logs** inside License Information.

   ![License Information Table]

<table>
<thead>
<tr>
<th>License Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LICENSE TYPE</strong></td>
</tr>
<tr>
<td><strong>SERVICE TIER</strong></td>
</tr>
<tr>
<td><strong>LICENSE END DATE</strong></td>
</tr>
<tr>
<td><strong>MSSP STATUS</strong></td>
</tr>
<tr>
<td><strong>MSSP SERVICE</strong></td>
</tr>
</tbody>
</table>

The Export Raw Log Files dialog box opens.

![Export Raw Log Files Dialog]

3. Select a date range to download the raw log files in ZIP format.

   ![Date Range Selection]

   **Note:** The date range cannot exceed 30 days.

4. Click **Request Download**.

   The Log Files Requested dialog box opens to inform you that your request is being processed. This process can take up to 24 hours.
**Important:** The beginning date can't be earlier than your first day of storage.

5. Click **OK**.
   
   You will receive an email with a link to your file.

6. Click the link in the email to download the ZIP file.

7. Extract the zipped bundle, and you see the files listed as `forensics-YYYY-MM-DD.hh.log.gz`, where `YYYY-MM-DD.hh` refers to the date and hour.

### Email Notifications Concerning Your License

USM Anywhere sends the following notification emails to the email address associated with your license. Typically, this is the email address used to register the trial or your subscription:

- A license is changed from trial to subscription.
- A license tier is upgraded.
- A license expiration date is updated.
- The number of sensors allowed is updated.
- An activated license has expired.
- An activated license is deleted.

### Projected Data Consumption

| Role Availability | Read-Only | Analyst | Manager |
On the My Subscription page, USM Anywhere displays the total data you have consumed for the month, the remaining data to be consumed, and the projected data you will consume based on your current usage. The service tier specified on your license determines the amount of data you’re allowed to consume each month.

### License Usage

<table>
<thead>
<tr>
<th>TOTAL SEARCHABLE DATA</th>
<th>249.9 GB LEFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONSUMED DATA</td>
<td>780.0 MB of 250 GB</td>
</tr>
<tr>
<td>PROJECTED DATA CONSUMPTION</td>
<td>1.4 GB of 250 GB</td>
</tr>
<tr>
<td>PURGED DATA</td>
<td>0 kB</td>
</tr>
</tbody>
</table>

#### Sensors

- 2 Deployed
- 2 Sensors pending deployment

#### Purge Event Data

⚠️ The ability to purge data will soon be deprecated. Over-tier capabilities will then be handled differently.

For now, purging is restricted to reflect the allotted frequency of twice per month. Please create **filtered event rules**. Filtered Events do not count against your monthly tier.

The Projected Data Consumption field is calculated using the following formula:

\[
\text{projectedMonthlyConsumption} = \left( \frac{\text{currentMonthDataConsumption}}{\text{totalDaysOfDataConsumption}} \right) \times \text{DaysInMonth}
\]

Where:

- \( \text{currentMonthDataConsumption} \) = the total data consumed in the current month.
- \( \text{totalDaysOfDataConsumption} \) = the number of days passed in the current month (includes days with no recorded data).
- \( \text{DaysInMonth} \) = the total number of days in the month.

For example, in a 30-day month, if at the end of the 15th day the instance has received 10 TB of data, the projected data consumption will be \((10 \text{ TB} / 15) \times 30 = 20 \text{ TB}\).

The Projected Data Consumption field is crucial because it provides an estimate on how much data you will consume by the end of the month. This number should never exceed your allocated monthly usage. Exceeding the monthly limit turns USM Anywhere into **transient mode**, where incoming events are no longer searchable. More importantly, USM Anywhere's performance deteriorates. System process time increases, causing the sensor cache to fill up and the sensor to disconnect.
AT&T Cybersecurity recommends that you monitor your projected data consumption early and constantly, so that you can perform countermeasures when you’re to exceed your monthly limit. You can reduce consumption by monitoring fewer networks, cutting down the number of data sources, or creating filtering rules to restrict data collection.

On the same My Subscription page, there is a chart that displays the data collected during the current period.

---

### License Usage

<table>
<thead>
<tr>
<th>TOTAL SEARCHABLE DATA</th>
<th>PROJECTED DATA CONSUMPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>250.0 GB LEFT</strong></td>
<td><strong>60.0 MB of 250 GB</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONSUMED DATA</th>
<th>PURGED DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>19.3 MB of 250 GB</strong></td>
<td><strong>0 KB</strong></td>
</tr>
</tbody>
</table>

**SENSORS**

- 2 Deployed
- 18 Sensors pending deployment

**Manage Sensors**

---

### Purge Event Data

⚠️ The ability to Purge data will soon be deprecated. Over-tier capabilities will then be handled differently.

For now, Purging will be restricted to reflect the allotted frequency stated in the documentation of twice per month. Please create Filter Event Rules. Filtered Events do not count against your monthly tier.

---

On the lower side of the page, there are three tables that show the breakdown of how much data is being processed by each data source, event names, and reporting device. You can use the Last 24 Hours filter for identifying data during the last hour, last 24 hours, last 7 days, last 30 days, or last 90 days. You can also configure your own period of time by clicking the Custom Range option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select AM or PM.

---

Click **Download CSV** to create a comma-separated value (CSV) file detailing the specific information of each table in a spreadsheet.
Connecting a USM Anywhere to a USM Central

The My Subscription page displays if your deployment has been connected to a USM Central or if there are no connections.

Deployment Status

USM Central is a unified console that gives you a single place to monitor and manage multiple USM deployments. USM Anywhere displays if you have your deployment connected to a USM Central, the status of that connection, the domain, and when it was connected.

Deployment Status Types

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>The deployment is connected to the USM Central environment.</td>
</tr>
<tr>
<td>Not Connected</td>
<td>The deployment is not currently connected to USM Central.</td>
</tr>
<tr>
<td>Connection Denied</td>
<td>A connection request was initiated from the deployment and the request was denied from the USM Central console.</td>
</tr>
<tr>
<td>Connection Request Sent</td>
<td>A connection request was initiated from the deployment and is awaiting an acceptance or denial. You can accept or decline the request in the USM Central console.</td>
</tr>
<tr>
<td>Connecting</td>
<td>The USM Central is waiting for a USM Anywhere connection.</td>
</tr>
</tbody>
</table>

To connect a USM Anywhere to USM Central

1. Go to Settings > My Subscription.
2. Go to the License Information section and click Configure MSSP Service.
The Connect deployment to USM Central dialog box displays.

3. Click **Connect**.

4. Enter the domain for the USM Central instance.

5. Click **Connect**.

   The system sends a request to USM Central.

   The connection is not complete until the user accepts the connection request. See **USM Central Connections** for more information.
Once the request has been accepted, the deployment has been connected.

![Connection to USM Central](image)

### Disconnecting a USM Anywhere from a USM Central

To disconnect a USM Anywhere from a USM Central

1. Go to **Settings > My Subscription**.
2. Go to the License Information section and click **Configure MSSP Service**.
   
   The Connection to USM Central dialog box opens.
3. Click **Disconnect**.

   The disconnect deployment dialog box opens.

   ![Disconnect deployment dialog box](image)

4. Click **Yes, Disconnect**.
Your environment has a limited data consumption tier depending on your subscription tier.

**Important:** Tier options do not have unlimited processing power, memory allotment, or disk input/output (I/O) speeds. In addition to storage per month, your deployment size's impact on any of these factors will influence which tier option is right for your environment. AT&T Cybersecurity recommends pre-deployment sizing discussions with your sales representative to help select the right tier for you.

**Note:** If the events per second (EPS) threatens to impact your sensor's capacity. USM Anywhere may engage EPS Adaptive Response. EPS Adaptive Response enables your system to take more time to process events coming in by throttling your EPS, which keeps your system running without risking event loss. See [Protecting Your Sensor's Performance with EPS Adaptive Response](#) to read more about EPS Adaptive Response.

If your environment is going to exceed your data consumption tier, a yellow announcement displays in your USM Anywhere to warn you about it. All users can see this yellow announcement in your environment, and you can close it by clicking the icon in the upper-right side of the page.

USM Anywhere sends three emails four days apart to warn you that you are going to reach your data consumption tier. USM Anywhere sends these emails to the address assigned to the license.

**Important:** By closing the announcement, you acknowledge that a manager user is aware that the license is reaching its threshold for the current month.

Besides the yellow announcement, a dialog box opens if your environment is going to exceed your data consumption tier each time you log in to USM Anywhere.
If your environment has exceeded your data consumption tier, your USM Anywhere starts operating in transient mode. When running in transient mode, USM Anywhere no longer stores events in the hot storage or searchable data store, but will still generate alarms, run authenticated asset scans, and store raw logs associated with events in cold storage. This transient mode ends when you start a new month (based on your anniversary start date) or if you upgrade your subscription tier. If your environment has exceeded your data consumption tier, a red announcement displays in your USM Anywhere to warn you about it. All users can see this red announcement in your environment, and you can't close it.

USM Anywhere sends an email to warn you that it has reached your data consumption tier. The account receiving this kind of email is the one associated with your license.
Besides the red announcement, a dialog box opens if your environment has exceeded your data consumption tier each time you log in to USM Anywhere.
Note: Please contact the AT&T Cybersecurity Sales department if you need to upgrade your subscription tier or modify your license.

To refrain from reaching your monthly limit, AT&T Cybersecurity recommends that you create filtering rules to restrict data collection. If you've reached the monthly limit, you can purge your earliest seven days of data from the current month through the My Subscription page. This can be done twice a month. The button to purge data will only be active after you have reached your limit and your system is operating in transient mode. If you purge data to go back under your data limit, the transient mode will end as of the date that you enacted the purge. The purge won't retroactively remove transient mode for the days that the limit had been exceeded.
To purge seven days of event data

1. Go to **Settings > My Subscription**.
2. Click **Purge 7 Days of Event Data**.

The purge event data dialog box opens.
3. Click **Purge**.

**Note:** The 7 days of event data refer to the first 7 days of the current month. If you choose to purge again in the same month, then the second 7 days will be purged (the 8th of the month through the 14th).
USM Anywhere has a robust reporting function that enables you to create detailed reports on a broad range of specifics in your environment.

**Note:** The report feature in AT&T TDR for Gov works differently compared to USM Anywhere. See [Reports in AT&T TDR for Gov](#) for more information.

The Reports section of USM Anywhere contains three main sections:

- **Saved Reports** – This page contains all of the reports that have been saved in USM Anywhere. You can filter the reports by category and whether they are scheduled to run at set intervals (see [Scheduled Reports](#) for more information). You can edit, copy, or delete the reports from this page, or review previously run reports. See [Saved Reports on USM Anywhere](#) for more information.

- **Compliance Templates**. Report templates related to Payment Card Industry (PCI), National Institute of Standards Technology Cybersecurity Framework (NIST CSF), Health Insurance Portability and Accountability Act (HIPAA), and ISO 27001 compliance protocols are accessible from this page. See [USM Anywhere Compliance Templates](#) for more information.

- **Event Type Templates**. Report templates based on event data sources or types of event data sources are contained on this page. See [USM Anywhere Event Type Templates](#) for more information.

You can also create custom reports from the [Create Alarms Report](#), [Create an Assets Report](#), and [Create an Events Report](#) pages.
The Saved Reports page contains a list of all the reports that have been saved in USM Anywhere. From this page, you can edit, copy, delete, or run any of the reports you've saved. The reports listed on the page can be filtered by category or scheduled status. You can also click the icon next to any of the saved reports to view their export history or download a previously run report.

**Note:** The report feature in AT&T TDR for Gov works differently compared to USM Anywhere. See Reports in AT&T TDR for Gov for more information.

### Saved Reports

<table>
<thead>
<tr>
<th>Category</th>
<th>Saved Reports</th>
<th>Scheduled:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Events Report</td>
<td>Events</td>
<td>application/pdf</td>
</tr>
<tr>
<td>Compliances</td>
<td>Alarms</td>
<td>application/pdf</td>
</tr>
<tr>
<td>Monthly Overview</td>
<td>Alarms</td>
<td>application/pdf</td>
</tr>
<tr>
<td>Alarms Report</td>
<td>Alarms</td>
<td>application/pdf</td>
</tr>
</tbody>
</table>

### Export History

<table>
<thead>
<tr>
<th>FORMAT</th>
<th>RECORD LIMIT</th>
<th>RUN BY</th>
<th>Run Date</th>
<th>SENT TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF</td>
<td>50</td>
<td><a href="mailto:admin@test.net">admin@test.net</a></td>
<td>Jul 23 2019, 12:51 AM</td>
<td><a href="mailto:admin@test.net">admin@test.net</a></td>
</tr>
<tr>
<td>PDF</td>
<td>50</td>
<td><a href="mailto:admin@test.net">admin@test.net</a></td>
<td>Aug 23 2019, 07:00 AM</td>
<td><a href="mailto:admin@test.net">admin@test.net</a></td>
</tr>
</tbody>
</table>

**To edit a saved report**

1. Click the **icon to edit the report.**
2. **Click Edit Filters** to add any additional filters you want to include in the report.
3. Under the Format section, select either **CSV** or **PDF** for the format of the report.
4. Under Repeat, click the drop-down list to select how often you want the scheduled report to be generated. If you don't want the report to be recurring, leave the selection as **Never**.
   - If you have selected the option to schedule recurring reports to be generated, the First Run Date, Repeat On, and Time sections show up below the Repeat section:
     - **First Run Date field:** Select the day you want the first report to be generated.
     - **Repeat On section:** Click the days of the week you want the report to run on if you've selected the Weekly or Bi-weekly option, or select the day of the month if you selected Monthly.
     - **Time section:** Select the UTC time you want the reports to be run on the days they're generated.
5. In the Email Addresses section, enter the email addresses of the people to whom you want the report to be sent when it is generated. Select **Enable link expiration** if you want the link to the report to expire after 14 days.
6. Click **Next** to go to the Format Output section of the report.
10. In the Name field, enter a name for the report. This name displays in the Saved Reports page. You also have the option to add description that will be included in the generated emails when it is run.

8. For the Number of Records, choose the maximum number of records to be included on the report.

9. If you have chosen the PDF format, you will see the Graphs section, and you can use this section to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ➙ icons.

10. Select Save & Run to save your report and run it, or select Run if you don’t wish to keep the report in your Saved Reports page.

USM Anywhere Compliance Templates

**Role Availability**

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

AllenVault USM Anywhere provides out-of-the-box, pre-built compliance reporting templates based on alarms, vulnerabilities, and events collected in the system. These reports make it fast and simple to navigate the requirements and demonstrate compliance during an audit. You can easily customize, save, and export any report as needed.

You can find these templates on **Reports > Compliance Templates**.

USM Anywhere supports several compliance templates including the following:

- **PCI**: Payment Card Industry Data Security Standards (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These reports are identified and based on specific PCI DSS requirements to provide the auditor with the specific information requested. For example, PCI DSS requirement 10.7.a: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis. See **PCI DSS Compliance Templates** for more information.

- **NIST CSF**: The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. See **NIST CSF Compliance Templates** for more information.

- **HIPAA**: The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. This includes covered entities, anyone who provides treatment, payment and operations in healthcare, and business associates, anyone with access to patient information and provides support in treatment, payment, or operations. Subcontractors, or business associates of business associates, must also be in compliance. See **HIPAA Compliance Templates** for more information.

- **ISO 27001**: ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The ISO and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an Information Security Management System (ISMS). See **ISO 27001 Compliance Templates** for more information.

PCI DSS Compliance Templates

**Role Availability**

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

The Payment Card Industry Data Security Standards (PCI DSS) are a set of technical and operational requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. Administered by the PCI Security Standards Council, the PCI standard requires validation of compliance on an annual basis.

This section includes the descriptions for PCI DSS compliance templates on USM Anywhere:
USM Anywhere™

User Guide
The report generated from this template provides a list of all Login Failure events that USM Anywhere records. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Event Name</td>
<td>&quot;PAM authentication failure&quot;, &quot;Failed password&quot;, &quot;SSH connection: Failed password&quot;, &quot;PAM X more authentication failures&quot;, &quot;Authentication failure&quot;, &quot;FAILED su&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 10.2.4 - Linux report

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.

Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

Click Run to run the report.

**PCI DSS 10.2.4 - Windows**

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

This report provides a list of all Login Failure events that USM Anywhere records. The following table shows the event filters used by this template:

**Filters Used by PCI DSS 10.2.4 - Windows**

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>&quot;Security&quot;</td>
</tr>
<tr>
<td>Data Source</td>
<td>&quot;Windows NxLog&quot;, &quot;AlienVault Agent - Windows EventLog&quot;</td>
</tr>
<tr>
<td>Reporting Device Rule ID</td>
<td>&quot;4625&quot;, &quot;529&quot;, &quot;530&quot;, &quot;531&quot;, &quot;532&quot;, &quot;533&quot;, &quot;534&quot;, &quot;53&quot;, &quot;536&quot;, &quot;537&quot;, &quot;539&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 10.2.4 - Windows report

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

PCI DSS 10.2.5.b - Linux

The report generated from this template provides a list of all privilege escalations and the performed action. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Data Source</td>
<td>&quot;Linux SUDO&quot;</td>
</tr>
<tr>
<td>Event Name</td>
<td>&quot;Successful su&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 10.2.5.b - Linux report

1. Go to Reports > Compliance Templates.

2. Click Generate Report on the specific line for this report.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.
Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.
6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and icons.
14. Select **Save & Run** if you wish to keep the report in your **Saved Reports on USM Anywhere** page and receive the report in the indicated email.
15. Click **Run** to run the report.

**PCI DSS 10.2.5.b - Windows**

The report generated from this template provides a list of any changes, additions, or deletions to any account that a root or administrator user has made. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>&quot;Security&quot;</td>
</tr>
<tr>
<td>Data Source</td>
<td>&quot;Windows NxLog&quot;, &quot;AlienVault Agent - Windows EventLog&quot;</td>
</tr>
<tr>
<td>Reporting Device Rule ID</td>
<td>&quot;576&quot;, &quot;4672&quot;, &quot;577&quot;, &quot;4673&quot;, &quot;578&quot;, &quot;4674&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate the PCI DSS 10.2.5.b - Windows report

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ▶️ and the ◀️ icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.

PCI DSS 10.2.5.c - Linux

The report generated from this template provides a list of any changes, additions, or deletions to any account that a root or administrator user has made. The following table shows the event filters used by this template:
To generate the PCI DSS 10.2.5.c - Linux report

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ◀ icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.
The report generated from this template provides a list of any changes, additions, or deletions to any account that a root or administrator user has made. The following table shows the event filters used by this template:

### Filters Used by PCI DSS 10.2.5.c - Windows

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>&quot;Security&quot;</td>
</tr>
<tr>
<td>Data Source</td>
<td>&quot;Windows NxLog&quot;, &quot;AlienVault Agent - Windows EventLog&quot;</td>
</tr>
<tr>
<td>Reporting Device Rule ID</td>
<td>&quot;624&quot;, &quot;4720&quot;, &quot;4722&quot;, &quot;4725&quot;, &quot;4726&quot;, &quot;4738&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 10.2.5.c - Windows report

1. Go to **Reports > Compliance Templates**.
2. Click **Generate Report** on the specific line for this report. The Configure Report dialog box displays.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.
5. Under the Format section, select either **CSV** or **PDF** for the format of the report.
6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ⇐ icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.

**PCI DSS 10.7.a**

This view provides a summary of USM Anywhere hot and cold storage, satisfying the requirements for PCI DSS 10.7.a. The View link goes to the My Subscription page (Settings > My Subscription). See Subscription Management for more information.

**PCI DSS 10.7.c**

The report generated from this template provides a view of the last 90 days of events that is available for analysis, and satisfies the requirements for PCI DSS 10.7.c. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 10.7.c report
1. Go to Reports > Compliance > Templates.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the **Format** section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the **Report Name** field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the **Number of records** section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.
14. Select **Save & Run** if you wish to keep the report in your **Saved Reports on USM Anywhere** page and receive the report in the indicated email.
15. Click **Run** to run the report.

**PCI DSS 11.5.a - Linux**

The report generated from this template provides a view of the file integrity monitoring (FIM) events that the use of change-detection mechanism satisfies in PCI DSS 11.5.a - Linux. The following table shows the event filters used by this template:

### Filters Used by PCI DSS 11.5.a - Linux

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Data Source Device</td>
<td>&quot;Osquery&quot;, &quot;AlienVault Agent&quot;</td>
</tr>
<tr>
<td>Event type</td>
<td>&quot;file_events&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate the PCI DSS 11.5.a - Linux report
1. Go to Reports > Compliance Templates.

2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

PCI DSS 11.5.a - Windows

The report generated from this template provides a view of the FIM events that the use of change-detection mechanism satisfies in PCI DSS 11.5.a - Windows. The following table shows the event filters used by this template:
<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the PCI DSS 11.5.a - Windows report

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF in the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ++ and the -- icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.
The report generated from this template provides proof that threat assessments are being performed on all systems set up for a vulnerability scan. This report may not be run if vulnerability scans are not set up on all systems mentioned in PCI DSS 5.1.2. The following table shows the event filters used by this template:

### Filters Used by PCI DSS 5.1.2

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### To generate the PCI DSS 5.1.2 report

1. Go to **Reports > Compliance Templates**.
2. Click **Generate Report** on the specific line for this report. The Configure Report dialog box displays.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.

Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.
6. Select if you want to generate the report again, and choose **Never, Daily, Weekly, Bi-weekly, and Monthly**.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

**PCI DSS 6.1**

The report generated from this template provides a proof that vulnerabilities are being assigned with a risk ranking in the severity field. The following table shows the event filters used by this template:

### Filters Used by PCI DSS 6.1

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**To generate the PCI DSS 6.1 report**

1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the 🔂 and the 🔁 icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

---

**PCI DSS 8.1.6.a - Windows**

The report generated from this template proves that account lockouts are taking place on monitored devices. Note that this report is predefined for Microsoft Windows but can be modified to include other devices as well. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>&quot;Security&quot;</td>
</tr>
<tr>
<td>Data Source</td>
<td>&quot;Windows NxLog&quot;, &quot;AlienVault Agent - Windows EventLog&quot;</td>
</tr>
<tr>
<td>Reporting Device Rule ID</td>
<td>4740</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

---

**To generate the PCI DSS 8.1.6.a - Windows report**

1. Go to Reports > Compliance Templates.
2. Click **Generate Report** on the specific line for this report.
   
   The Configure Report dialog box displays.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.
Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.

6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.

7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

**PCI DSS 8.2.1.c**

The report generated from this template provides instances of plain text passwords on the network. The absence of these events satisfies the requirements. The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;PCI DSS&quot;</td>
</tr>
<tr>
<td>Category</td>
<td>&quot;Suspicious Activity&quot;</td>
</tr>
<tr>
<td>Event Activity</td>
<td>&quot;Password leak&quot;</td>
</tr>
<tr>
<td>Subcategory</td>
<td>&quot;Suspicious Traffic&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate the PCI DSS 8.2.1.c report
1. Go to Reports > Compliance Templates.
2. Click Generate Report on the specific line for this report.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the → and the ← icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.

NIST CSF Compliance Templates

Role Availability

Read-Only  Analyst  Manager

The National Institute of Standards Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.
This section includes the descriptions for NIST CSF compliance templates on USM Anywhere:

- NIST CSC Control PR.IP-12: A Vulnerability Management Plan is Developed and Implemented
- NIST CSC Control PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and Reviewed in Accordance with Policy
- NIST CSF Control DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods
- NIST CSF Control DE.AE-3: Event Data Are Aggregated and Correlated from Multiple Sources and Sensors
- NIST CSF Control DE.AE-5: Incident Alert Thresholds Are Established
- NIST CSF Control DE.CM-3: Personnel Activity Is Monitored to Detect Potential Cybersecurity Events
- NIST CSF Control DE.CM-4: Malicious Code Is Detected
- NIST CSF Control DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software Is Performed
- NIST CSF Control DE.CM-8: Vulnerability Scans Are Performed
- NIST CSF Control DE.DP-4: Event Detection Information Is Communicated to Appropriate Parties
- NIST CSF Control ID.AM-1: Physical Devices and Systems within the Organization Are Inventoried
- NIST CSF Control ID.AM-5: Resources (E.G., Hardware, Devices, Data, and Software) Are Prioritized Based on their Classification, Criticality, and Business Value
- NIST CSF Control ID.RA-1: Asset Vulnerabilities Are Identified and Documented
- NIST CSF Control ID.RA-2: Threat and Vulnerability Information is Received from Information Sharing Forums and Sources
- NIST CSF Control PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users
- NIST CSF Control RS.AN-3: Forensics Are Performed
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. Note on Control: This report shows that vulnerabilities are being identified, partially satisfying the control. An update policy would need to be in place for this to be fully satisfied.


The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To generate the NIST CSC Control PR.IP-12 report
1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range. Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.
6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.

13. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.

15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.

**NIST CSC Control PR.PT-1: Audit/Log Records Are Determined, Documented, Implemented, and Reviewed in Accordance with Policy**

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Note on Control: This Control can be partially satisfied by having logs available in USM Anywhere for log review. The user is responsible for their own log review process for the rest of the control. Associated Frameworks: CCS CSC 14, COBIT 5 APO 11.04, ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4, ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, NIST SP 800-53 Rev. 4 AU Family.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the NIST CSC Control PR.PT-1 report

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.
   
   The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.

USM Anywhere™ User Guide
Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days**, or **Custom Range** to set a particular date range.

6. Under the Format section, select either **CSV** or **PDF** for the format of the report.

7. Select if you want to generate the report again, and choose **Never, Daily, Weekly, Bi-weekly**, and **Monthly**.

8. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

9. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

10. Click **Next**.

11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

12. (Optional.) Add a description that will be included.

13. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

15. Select **Save & Run** if you wish to keep the report in your **Saved Reports on USM Anywhere** page and receive the report in the indicated email.

16. Click **Run** to run the report.

---

**NIST CSF Control DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods**

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. **Note on Control:** This control is partially satisfied by alarms being available for investigation and response, but requires the user to have a clear investigation and response policy utilizing the available logs. Associated Frameworks: ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2, ISO/IEC 27001:2013 A.16.1.1, A.16.1.4, NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate the NIST CSF Control DE.AE-2 report

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.

The Configure Report dialog box displays.

4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the Number of records section, select the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ◀ icons.
15. Select Save if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
16. Click Run to run the report.

NIST CSF Control DE.AE-3: Event Data Are Aggregated and Correlated from Multiple Sources and Sensors
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. The Default Fields satisfy this control by showing different sensors and hosts send events to USM Anywhere.

Associated Frameworks: ISA 62443-3-3:2013 SR 6.1, NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

The following table shows the event filters used by this template:

### Filters Used by NIST CSF Control DE.AE-3: Event Data Are Aggregated and Correlated from Multiple Sources and Sensors

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

**To generate the NIST CSF Control DE.AE-3 report**

1. Go to **Reports > Compliance Templates**.
2. On the left navigation pane, click **NIST CSF**.
3. Click **Generate Report** on the specific line for this report.
   
   The Configure Report dialog box displays.
4. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
5. Click the date field if you want to choose a different date range.

Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days,** or **Custom Range** to set a particular date range.

6. Under the Format section, select **CSV** or **PDF** for the format of the report.
7. Select if you want to generate the report again, and choose **Never, Daily, Weekly, Bi-weekly,** and **Monthly**.
8. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
9. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
10. Click **Next**.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.

NIST CSF Control DE.AE-5: Incident Alert Thresholds Are Established

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. Associated Frameworks: COBIT 5 APO12.06, ISA 62443-2-1:2009 4.2.3.10, NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8.

The View link goes to the orchestration rules page (Settings > Rules). See Rules Management for more information.

NIST CSF Control DE.CM-3: Personnel Activity Is Monitored to Detect Potential Cybersecurity Events

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Since all events could be attributed to user events, and all events are run through the correlation engine, this control is satisfied by the default view. Associated Frameworks: ISA 62443-3-3:2013 SR 6.2, ISO/IEC 27001:2013 A.12.4.1, NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the NIST CSF Control DE.CM-3 report

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.
15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
16. Click Run to run the report.

NIST CSF Control DE.CM-4: Malicious Code Is Detected

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Since all events could be attributed to user events, and all events are run through the correlation engine, this control is satisfied by the default view. Associated Frameworks: ISA 62443-3-3:2013 SR 6.2, ISO/IEC 27001:2013 A.12.4.1, NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Family</td>
<td>All</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate NIST CSF Control DE.CM-4 report

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.

The Configure Report dialog box displays.

4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

5. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

6. Under the Format section, select either CSV or PDF for the format of the report.

7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

10. Click Next.

11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

12. (Optional.) Add a description that will be included.

13. Under the Number of records section, select the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ➜ icons.

15. Select Save if you wish to save the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click Run to run the report.

NIST CSF Control DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software Is Performed
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Unauthorized access to accounts will partially satisfy the control. Associated Frameworks: NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the NIST CSF Control DE.CM-7 report

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.
   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.
6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click **Next**.

11. In the **Report Name** field, enter a name for the report. This name will be displayed in the Saved Reports page.

12. (Optional.) Add a description that will be included.

13. Under the **Number of records** section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.

14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➡️ and the ⬅️ icons.

15. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

16. Click **Run** to run the report.

**NIST CSF Control DE.CM-8: Vulnerability Scans Are Performed**

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

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. The Authenticated vulnerability scan log in the linked view shows that vulnerability scans are run, and will satisfy this control. Associated Frameworks: COBIT 5 BAI03.10, ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7, ISO/IEC 27001:2013 A.12.6.1, NIST SP 800-53 Rev. 4 RA-5.

The View link goes to the job scheduler of asset scans page (**Settings > Scheduler > Asset Scans**). See **Scheduling Asset Scans from the Job Scheduler Page** for more information.

**NIST CSF Control DE.DP-4: Event Detection Information Is Communicated to Appropriate Parties**

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

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. Within the user settings view, the receive alarms notification checkbox satisfies this control. Associated Frameworks: COBIT 5 APO12.06, ISA 62443-2-1:2009 4.3.4.5.9, ISA 62443-3-3:2013 SR 6.1, ISO/IEC 27001:2013 A.16.1.2, NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4.

The View link goes to the users list page (**Settings > Users**). See **USM Anywhere User Management** for more information.

**NIST CSF Control ID.AM-1: Physical Devices and Systems within the Organization Are Inventoried**

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

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. This can partially satisfy the control by providing a list of network assets, or fully satisfy the control in some cases. Associated Frameworks: CCS CSC 1, COBIT 5 BAI09.01, BAI09.02, ISA 62443-2-1:2009 4.2.3.4, ISA 62443-3-3:2013 SR 7.8, ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, NIST SP 800-53 Rev. 4 CM-8.

This report shows the assets list by using the "NIST CSF Control ID.AM-1: Physical Devices and Systems within the Organization are Inventoried" view.
To generate the NIST CSF Control ID.AM-1 report:

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.

**Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description. It will be numbered.
13. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove a graph by clicking the + or - icons.
15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
16. Click Run to run the report.

NIST CSF Control ID.AM-5: Resources (E.G., Hardware, Devices, Data, and Software) Are Prioritized Based on their Classification, Criticality, and Business Value
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. Hardware and devices can be prioritized into asset groups, satisfying part of the control. Associated Frameworks: COBIT 5 AP003.03, AP003.04, BAI09.02, ISA 62443-2-1:2009 4.2.3.6, ISO/IEC 27001:2013 A.8.2.1, NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14.

This report shows the asset groups list by using the "NIST CSF Control ID.AM-5: Resources (e.g., Hardware, Devices, Data, and Software) are Prioritized Based on their Classification, Criticality, and Business Value" view.

To generate the NIST CSF Control ID.AM-5 report
1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
4. **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.
5. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
6. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

7. Under the Format section, select either CSV or PDF for the format of the report.
8. Select if you want to generate the report daily, weekly, bi-weekly, and monthly.
9. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
10. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
11. Click Next.
12. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
13. (Optional.) Add a description that will be included.
14. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
15. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ➔ icons.

16. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

17. Click Run to run the report.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. This report satisfies both identification and documentation since vulnerabilities are tracked and described in the vulnerabilities tab. Associated Frameworks: CCS CSC 4, COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12, ISO/IEC 27001:2013 A.12.6.1, A.18.2.3, NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To generate the NIST CSF Control ID.RA-1 report
1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range.
6. Under the Format section, select either CSV or PDF for the format of the report.
The NIST Frameworks: Authorized Access

ISO/IEC Control and NIST 800-100, 800-500, 1000, or 2500.

If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

Click Run to run the report.

NIST CSF Control ID.RA-2: Threat and Vulnerability Information is Received from Information Sharing Forums and Sources

Role Availability

Control Description Access Control (ID.RA): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. Associated Frameworks: ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12, ISO/IEC 27001:2013 A.6.1.4, NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5.

The View link goes to the OTX dashboard page (Dashboard > Open Threat Exchange). See Open Threat Exchange Dashboard for more information.

NIST CSF Control PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users

Role Availability


The following table shows the event filters used by this template:

### USM Anywhere™ User Guide
### Filters Used by NIST CSF Control PR.AC-1: Identities and Credentials Are Managed for Authorized Devices and Users

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

**To generate the NIST CSF Control PR.AC-1 report**

1. Go to Reports > Compliance Templates.
2. On the left navigation pane, click NIST CSF.
3. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
4. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
5. Click the date field if you want to choose a different date range. Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.
6. Under the Format section, select either CSV or PDF for the format of the report.
7. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
8. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
9. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
10. Click Next.
11. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
12. (Optional.) Add a description that will be included.
13. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
14. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and icons.
15. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
16. Click Run to run the report.

NIST CSF Control RS.AN-3: Forensics Are Performed

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities. Note on Control: Orchestration rules are available to automatically run forensics on alarms and events. Having the output of these forensic scans available for reporting would satisfy this control. Associated Frameworks: ISA 62443-3-2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, ISO/IEC 27001:2013 A.16.1.7, NIST SP 800-53 Rev. 4 AU-7, IR-4.

The View link goes to the orchestration rules page (Settings > Rules). See Rules Management for more information.

HIPAA Compliance Templates

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. This includes covered entities, anyone who provides treatment, payment and operations in healthcare, and business associates, anyone with access to patient information and provides support in treatment, payment, or operations. Subcontractors, or business associates of business associates, must also be in compliance.

This section includes the descriptions for HIPAA compliance templates on USM Anywhere:

- HIPAA A03 §164.308(a)(1)(ii)(A)
- HIPAA Control T23 §164.312(a)(1)
- HIPAA Control T23 §164.312(a)(5)
- HIPAA Control T33 §164.312(c)(1) - Linux
- HIPAA Control T33 §164.312(c)(1) - Windows
The "HIPAA A03 §164.308(a)(1)(ii)(A) – Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?" report generated from this template provides a risk analysis that is the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. Consider whether your practice categorizes its information systems as high, moderate or low impact systems. Consider that information system categorization helps your practice to scope audits and prioritize investments for security mitigation. Consider whether your practice’s risk analysis is designed to protect its information systems and ePHI that it processes, stores, and transmits from unauthorized access, use, disclosure, disruption, change, or damage. Consider whether your practice’s risk analysis: Identifies threats. Identifies vulnerabilities inherent in its technology, processes, workforce, and vendors. Contemplates the likelihood of occurrence. Estimates the potential magnitude of harm.

This report shows the asset groups list by using the "HIPAA A03 §164.308(a)(1)(ii)(A) - Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?" view.

**To generate the HIPAA A03 §164.308(a)(1)(ii)(A) report**

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click HIPAA.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays,
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

---

**HIPAA Control T03 §164.312 (a)(1)**

The "HIPAA Control T03 §164.312 (a)(1) Does your practice analyze the activities performed by all of its workforce and service providers to identify the extent to which each needs access to ePHI?" report generated from this template considers that a "user" can be any entity that accesses your practice’s ePHI, whether it is a person or a device. Consider whether your practice:

- Defines roles and responsibilities in sufficient detail to demonstrate whether access to ePHI is necessary.
- Determines whether remote access is necessary from physical environments that are not under your practice’s control. If so, determine by whom, how (e.g., electronic device), and when.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;HIPAA&quot;</td>
</tr>
<tr>
<td>Suppressed</td>
<td>True</td>
</tr>
</tbody>
</table>

To generate the HIPAA Control T03 §164.312 (a)(1) report

1. Go to Reports > Compliance Templates.
   - On the left navigation pane, click HIPAA.

2. Click Generate Report on the specific line for this report.
   - The Configure Report dialog box displays.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.
Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.

6. Select if you want to generate the report again, and choose **Never, Daily, Weekly, Bi-weekly, and Monthly**.

7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

**HIPAA Control T30 §164.312(b)**

The "HIPAA Control T30 §164.312(b)" report generation from this template considers that written policies and procedures can drive the development of processes and implementation of standards and controls, which reduce risk to ePHI. Can provide essential information for privacy and security awareness and role-based training.

The View link goes to the My Subscription page (**Settings > My Subscription**). See **Subscription Management** for more information.
To generate the HIPAA Control T30 §164.312(b) report

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click HIPAA.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, select a maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.
The "HIPAA Control T33 §164.312(c)(1) Does your practice have mechanisms to corroborate that ePHI has not been altered, modified or destroyed in an unauthorized manner? - Linux" report generated from this template considers whether your practice has data authentication mechanisms and tools, such as checksum. Checksum is a computation that is introduced when ePHI is transmitted or stored. The computation is checked at a later time (such as when ePHI recalled or when it is received at the intended destination) to ascertain whether the computations match. If the checksum matches, then it is less likely that the ePHI was altered or modified. Also consider whether your practice relies on encryption validation to authenticate ePHI.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;HIPAA&quot;</td>
</tr>
<tr>
<td>Data Source Device</td>
<td>Osquery</td>
</tr>
<tr>
<td>Event Type</td>
<td>file_events</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the HIPAA Control T33 §164.312(c)(1) - Linux report:

1. Go to Reports > Compliance Templates. On the left navigation pane, click HIPAA.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
   - Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.
5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ➠ icons.
14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click **Run** to run the report.

**HIPAA Control T33 §164.312(c)(1) - Windows**

The "HIPAA Control T33 §164.312(c)(1) Does your practice have mechanisms to corroborate that ePHI has not been altered, modified or destroyed in an unauthorized manner? - Windows" report generated from this template considers whether your practice has data authentication mechanisms and tools, such as checksum. Checksum is a computation that is introduced when ePHI is transmitted or stored. The computation is checked at a later time (such as when ePHI recalled or when it is received at the intended destination) to ascertain whether the computations match. If the checksum matches, then it is less likely that the ePHI was altered or modified. Also consider whether your practice relies on encryption validation to authenticate ePHI.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Groups</td>
<td>&quot;HIPAA&quot;</td>
</tr>
<tr>
<td>Data Source Device</td>
<td>Windows NxLog</td>
</tr>
<tr>
<td>Event Type</td>
<td>File System</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the HIPAA Control T33 §164.312(c)(1) - Windows report

1. Go to **Reports > Compliance Templates**.
   - On the left navigation pane, click **HIPAA**.
2. Click **Generate Report** on the specific line for this report.
   - The Configure Report dialog box displays.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

ISO 27001 Compliance Templates

ISO/IEC 27001 provides guidance for implementing information security controls to achieve a consistent and reliable security program. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) developed 27001 to provide requirements for an information security management system (ISMS).

This section includes the descriptions for ISO 27001 compliance templates on USM Anywhere:

- ISO 27001 A.6.1.4: Contact with Special Interest Groups
- ISO 27001 A.8.1.1: Inventory of Assets
- ISO 27001 A.8.1.2: Ownership of Assets
- ISO 27001 A.8.2.1: Classification of Information
- ISO 27001 A.8.2.2: Labeling of Information
- ISO 27001 A.11.2.6: Security of Equipment and Assets Off-Premises
ISO 27001 A.12.2.1: Controls Against Malware
- ISO 27001 A.12.4.1: Event Logging
- ISO 27001 A.12.4.2 - Linux: Protection of Log Information
- ISO 27001 A.12.4.2 - Windows: Protection of Log Information
- ISO 27001 A.12.7.1: Information Systems Audit Controls
- ISO 27001 A.16.1.2: Reporting Information Security Events
- ISO 27001 A.16.1.4: Assessment of and decision on information security events
- ISO 27001 A.18.2.2: Compliance with Security Policies and Standards
- ISO 27001 A.18.2.3: Technical Compliance Review

USM Anywhere™
User Guide
ISO 27001 A.6.1.4: Contact with Special Interest Groups

The "ISO 27001 A.6.1.4: Contact with Special Interest Groups" standard provides appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

The View link goes to the OTX dashboard page ([Dashboard > Open Threat Exchange](Dashboard)). See [Open Threat Exchange Dashboard](Dashboard) for more information.

ISO 27001 A.8.1.1: Inventory of Assets

The "ISO 27001 A.8.1.1: Inventory of Assets" report is related to the assets associated with information and information processing facilities that shall be identified and an inventory of these assets shall be drawn up and maintained.

This report shows the assets list by using the "ISO 27001 A.8.1.1: Inventory of Assets" view.

To generate the ISO 27001 A.8.1.1: Inventory of Assets report

1. Go to Reports > Compliance Templates. On the left navigation pane, click ISO 27001.
2. Click Generate Report on the specific line for this report. The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

---

**ISO 27001 A.8.1.2: Ownership of Assets**

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

The "ISO 27001 A.8.1.2: Ownership of Assets" report is related to the assets maintained in the inventory that shall be owned. This report shows the assets list by using the "ISO 27001 A.8.1.2: Ownership of Assets" view.

To generate the ISO 27001 A.8.1.2: Ownership of Assets report:

1. Go to Reports > Compliance Templates.
   - On the left navigation pane, click ISO 27001.

2. Click **Generate Report** on the specific line for this report.
   - The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.

4. Click the date field if you want to choose a different date range.

   Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.
1. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

2. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

3. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

4. Click Next.

5. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

6. (Optional.) Add a description that will be included.

7. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

8. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the + and the - icons.

9. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

10. Click Run to run the report.

ISO 27001 A.8.2.1: Classification of Information

The "ISO 27001 A.8.2.1: Classification of Information" report is related to the information that shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

This report shows the assets list by using the "ISO 27001 A.8.2.1: Classification of Information" view.

To generate the ISO 27001 A.8.2.1: Classification of Information report

1. Go to Reports > Compliance Templates.

2. Click Generate Report on the specific line for this report.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to include a parameter date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.
14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click Run to run the report.

ISO 27001 A.8.2.2: Labeling of Information

The "ISO 27001 A.8.2.2: Labeling of Information" report is related to an appropriate set of procedures for information labeling that shall be developed and implemented in accordance with the information classification scheme adopted by the organization. This report shows the assets list by using the "ISO 27001 A.8.2.2: Labeling of Information" view.

To generate the ISO 27001 A.8.2.2: Labeling of Information report

1. Go to Reports > Compliance Templates.
   - On the left navigation pane, click ISO 27001.
2. Click Generate Report on the specific line for this report.
   - The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the + and the - icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

ISO 27001 A.11.2.6: Security of Equipment and Assets Off-Premises

The "ISO 27001 A.11.2.6: Security of Equipment and Assets Off-Premises" report is related to security that shall be applied to off-site assets, taking into account the different risks of working outside the organization's premises.

This report shows the assets list by using the "ISO 27001 A.11.2.6: Security of Equipment and Assets Off-Premises" view.

To generate the ISO 27001 A.11.2.6: Security of Equipment and Assets Off-Premises report

1. Go to Reports > Compliance Templates.

   On the left navigation pane, click ISO 27001.

2. Click Generate Report on the specific line for this report.

   The Configure Report dialog box displays.

Note: This report doesn't have selected filters because it goes directly to an asset inventory.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.

4. Click the date field if you want to choose a different date range.

Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.

6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.

7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select **Save & Run** if you wish to keep the report in your **Saved Reports on USM Anywhere** page and receive the report in the indicated email.

15. Click **Run** to run the report.

---

**ISO 27001 A.12.2.1: Controls Against Malware**

The "ISO 27001 A.12.2.1: Controls Against Malware" report is related to detection, prevention and recovery controls to protect against malware that shall be implemented, combined with appropriate user awareness. This report shows the assets list by using the "ISO 27001 A.12.2.1: Controls Against Malware" view.

The following table shows the event filters used by this template:
To generate the ISO 27001 A.12.2.1: Controls Against Malware report

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ▶️ and the ◀️ icons.
14. Select **Save & Run** if you wish to keep the report in your **Saved Reports on USM Anywhere** page and receive the report in the indicated email.

15. Click **Run** to run the report.

**ISO 27001 A.12.4.1: Event Logging**

The "ISO 27001 A.12.4.1: Event Logging" report is related to event logs recording user activities, exceptions, faults and information security events that shall be produced, kept and regularly reviewed. This report shows the assets list by using the "ISO 27001 A.12.4.1: Event Logging" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

**To generate the ISO 27001 A.12.4.1: Event Logging report**

1. Go to **Reports > Compliance Templates**. On the left navigation pane, click **ISO 27001**.
2. Click **Generate Report** on the specific line for this report. The Configure Report dialog box displays.
3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.

Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.
6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.
7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.
14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.
15. Click **Run** to run the report.

**ISO 27001 A.12.4.2 - Linux: Protection of Log Information**

The "ISO 27001 A.12.4.2 - Linux: Protection of Log Information" report is related to logging facilities and log information that shall be protected against tampering and unauthorized access. This report shows the assets list by using the "ISO 27001 A.12.4.2 - Linux: Protection of Log Information" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>file_events</td>
</tr>
<tr>
<td>Data Source Device</td>
<td>Osquery</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the ISO 27001 A.12.4.2 - Linux: Protection of Log Information report

1. Go to **Reports > Compliance Templates**.
   On the left navigation pane, click **ISO 27001**.
2. Click **Generate a report on the specific file for this report**.
   The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
4. Click the date field if you want to choose a different date range.
Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.

6. Select if you want to generate the report again, and choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**.

7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

ISO 27001 A.12.4.2 - Windows: Protection of Log Information

The "ISO 27001 A.12.4.2 - Windows: Protection of Log Information" report is related to logging facilities and log information that shall be protected against tampering and unauthorized access. This report shows the assets list by using the "ISO 27001 A.12.4.2 - Windows: Protection of Log Information" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>File System</td>
</tr>
<tr>
<td>Data Source Device</td>
<td>Windows NxLog</td>
</tr>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>
To generate the ISO 27001 A.12.4.2 - Windows: Protection of Log Information report:

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.

2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.

   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ⇐ icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

ISO 27001 A.12.7.1: Information Systems Audit Controls
The "ISO 27001 A.12.7.1: Information Systems Audit Controls" report is related to the audit requirements and activities involving verification of operational systems that shall be carefully planned and agreed to minimize disruptions to business processes.

This report shows the assets list by using the "ISO 27001 A.12.7.1: Information Systems Audit Controls" view.

To generate the ISO 27001 A.12.7.1: Information Systems Audit Controls report

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.

Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. A link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ⟵ icons.
To generate the ISO 27001 A.16.1.2: Reporting Information Security Events report:

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.

2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.
9. Click **Next**.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: **20, 50, 100, 500, 1000, or 2500**.
13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➡️ and the ⬅️ icons.
14. Select **Save & Run** if you wish to keep the report in your Saved Reports page and receive the report in the indicated email.
15. Click **Run** to run the report.

**ISO 27001 A.16.1.4: Assessment of and decision on information security events**

The "ISO 27001 A.16.1.4: Assessment of and decision on information security events" report is related to the information security events shall be assessed and it that shall be decided if they are to be classified as information security incidents. This report shows the assets list by using the ISO 27001 A.16.1.4: Assessment of and decision on information security events" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppressed</td>
<td>False</td>
</tr>
</tbody>
</table>

To generate the ISO 27001 A.16.1.4: Assessment of and decision on information security events report

1. Go to **Reports > Compliance Templates**.  
   On the left navigation pane, click **ISO 27001**.

2. Click **Generate Report** on the specific line for this report.

   The Configure Report dialog box displays.

   **Note:** This report doesn't have selected filters because it goes directly to an asset inventory.

3. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.

4. Click the date field if you want to change a different date range.
Choose **Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range** to set a particular date range.

5. Under the Format section, select either **CSV** or **PDF** for the format of the report.

6. Select if you want to generate the report again, and choose **Never, Daily, Weekly, Bi-weekly, and Monthly**.

7. Enter an email address to send the report. Select the **Send to my Email Address** option to add your email automatically.

8. Select the **Enable link expiration** option. This link is delivered by email and expires in 14 days.

9. Click **Next**.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and icons.

14. Select **Save & Run** if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click **Run** to run the report.

**ISO 27001 A.18.2.2: Compliance with Security Policies and Standards**

The "ISO 27001 A.18.2.2: Compliance with Security Policies and Standards" report is related to the managers that shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, rules, and other cybersecurity requirements. This report shows the assets list by using the "ISO 27001 A.18.2.2: Compliance with Security Policies and Standards" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**USM Anywhere™ User Guide**
To generate the ISO 27001 A.18.2.2: Compliance with Security Policies and Standards report:

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.

2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.

3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.

4. Click the date field if you want to choose a different date range.

   Choose Last Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Last 90 Days, or Custom Range to set a particular date range.

5. Under the Format section, select either CSV or PDF for the format of the report.

6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.

7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.

8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.

9. Click Next.

10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.

11. (Optional.) Add a description that will be included.

12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen a PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the ➔ and the ← icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

ISO 27001 A.18.2.3: Technical Compliance Review
The "ISO 27001 A.18.2.3: Technical Compliance Review" report is related to the information systems that shall be regularly reviewed for compliance with the organization’s information security policies and standards. This report shows the assets list by using the "ISO 27001 A.18.2.3: Technical Compliance Review" view.

The following table shows the event filters used by this template:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Vulnerability</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To generate the ISO 27001 A.18.2.3: Technical Compliance Review report

1. Go to Reports > Compliance Templates.
   On the left navigation pane, click ISO 27001.
2. Click Generate Report on the specific line for this report.
   The Configure Report dialog box displays.
3. Click Edit Filters if you want to modify the selected filters, and then Continue to Filters. Do the modifications you need, and then click Edit Report.
4. Click the date field if you want to choose a different date range.
5. Under the Format section, select either CSV or PDF for the format of the report.
6. Select if you want to generate the report again, and choose Never, Daily, Weekly, Bi-weekly, and Monthly.
7. Enter an email address to send the report. Select the Send to my Email Address option to add your email automatically.
8. Select the Enable link expiration option. This link is delivered by email and expires in 14 days.
9. Click Next.
10. In the Report Name field, enter a name for the report. This name will be displayed in the Saved Reports page.
11. (Optional.) Add a description that will be included.
12. Under the Number of records section, choose the maximum number of records to include on the report: 20, 50, 100, 500, 1000, or 2500.

13. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views. You can add or remove graphs included in the report by clicking the and the icons.

14. Select Save & Run if you wish to keep the report in your Saved Reports on USM Anywhere page and receive the report in the indicated email.

15. Click Run to run the report.

USM Anywhere Event Type Templates

USM Anywhere includes a set of predefined templates based on the classification of event data source types and based on data sources.

You can find these templates on Reports > Event Type Templates.

There are these types of templates:


- **Data Sources.** You can find templates based on the most commonly used data sources including NIDS, AWS, Amazon DynamoDB, Amazon S3, AWS VPC Flow Logs, AWS Load Balancers, Azure, Cisco Umbrella, Cylance, FireEye, Fortigate, G Suite, McAfee ePO, Office 365, Okta, Palo Alto, SonicWall, Sophos UTM, Watchguard, VMware, Windows, AlienVault Agent. There is also a template for the AlienVault Generic Data Source.
USM Anywhere User Management

Because USM Anywhere manages important security functions for your organization, the system requires that all users log in with a user-name and a password. See Role-Based Access Control (RBAC) in USM Anywhere for more information about the roles in USM Anywhere.

When the first user links to a newly-provisioned USM Anywhere environment, they configure the password for the initial user account. This is the default administrator as defined in your subscription and this user account cannot be deleted. The Settings > Users page provides tools to add, edit, and remove other user accounts in the system.

If you want to protect your account, enable multifactor authentication (MFA) for your user account. When this feature is activated, USM Anywhere displays the multifactor authentication page for you to complete your MFA configuration. The displayed page provides a unique QR code for your Authenticator app to retrieve a verification code. See Using Multifactor Authentication for more information about this security configuration.

**Note:** AT&T Cybersecurity recommends that users enable MFA for their account. MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account.

Users can access settings for their own account and log out of the system by clicking the  icon in the upper right corner of the page.

USM Anywhere collects information about when a user logs into the system and what the user does. This information is available in USM Anywhere when you go to Settings > System Events. You may notice that there are logins from an admin@<your-subdomain>.alienvault.cloud user on a regular basis. The login has been created by an automated health check system, which checks for system configuration and performance issues on your instance. USM Anywhere creates these events for transparency.

USM Anywhere offers remote technical support for troubleshooting and diagnosis, where the AT&T Cybersecurity Technical Support Engineers access your instance from their computers. On such occasions, USM Anywhere provides an audit trail by creating a temporary user with the username of <user>@alienvault.com. These users are disabled after the remote session ends, and you can view them under Settings > Users.

This topic discusses these subtopics:

- Creating Users .............................................................................................................................................. 705
- Role-Based Access Control (RBAC) in USM Anywhere .................................................................................. 707
- Editing Users .................................................................................................................................................... 718
Managing Your Profile Settings ................................................................. 721
Deleting Users ..................................................................................... 729
Configuring Web UI Session Timeout ................................................... 730
Creating Users

Add a user account in your USM Anywhere environment for each member of your team that needs access. USM Anywhere implements role-based access control (RBAC). See Role-Based Access Control (RBAC) in USM Anywhere for more information.

To create a user

1. Go to Settings > Users to open the page.

2. Click New User.

The Create User dialog box opens.
3. Enter the user's **Email** address and **Full Name**.
   This is the email address used to verify the account and set the initial password.

4. Select the role you want to assign to the user. See Role-Based Access Control (RBAC) in USM Anywhere for more information.

5. Select the **Status** you want for the user.
   Typically, you should keep the default **Enabled** status for a new user account.

6. Click **Save**.
   USM Anywhere sends an email to the email address that includes a link to set a password and login.

   The password reset link will be valid for the next 24 hours. If you do not click the reset link within that period of time, USM Anywhere will display a message:
You need to click **Send Link** to receive a new email with a new password reset link.

**Role-Based Access Control (RBAC) in USM Anywhere**

USM Anywhere implements the role-based access control (RBAC), which provides users with the following:

- The ability to restrict certain users from accessing administrative capabilities like adding new users and sensors
- Predefined roles that range from read-only access to full administrative capabilities so users can easily select the appropriate role for a new user

There are three roles in USM Anywhere:

- **Read-Only**: You can access views and search the system, but cannot make system changes that impact other users.
- **Analyst**: You can view and search the system, schedule jobs, launch actions, configure rules, and configure asset credentials. But you cannot add or modify sensor configurations; configure credentials for AlienApp, notification apps, and threat intelligence integrations; or add users.
- **Manager**: This role enables analyst permissions, and enables you to add or modify sensor configurations; configure credentials for AlienApps, notification apps, and threat intelligence integrations; and add users.

**Important**: There is a maximum number of sessions per user. Users whose role is Manager can log in to USM Anywhere from up to three different browsers at the same time. Users whose role is Analyst or Read-Only can log in to USM Anywhere from up to two different browsers at the same time.

You can view a user’s role under the User List by going to **Settings > Users**.
When the status of a user changes to Disabled, the role column of that user in the User List will include Suspended.

### Users List

Users can log into USM Anywhere, with access based on their assigned roles. All users can edit their credentials by clicking the icon in the upper right hand corner.

<table>
<thead>
<tr>
<th>EMAIL</th>
<th>FULL NAME</th>
<th>ROLE</th>
<th>STATUS</th>
<th>Multi-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:U1@at.com">U1@at.com</a></td>
<td>User1</td>
<td>Analyst, Suspended</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td><a href="mailto:U2@at.com">U2@at.com</a></td>
<td>User2</td>
<td>Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

All AT&T Cybersecurity documentation will tell you which roles can perform a specific set of steps, using a table like the one below.

#### Role Availability

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

You can see the predefined roles in USM Anywhere in the following table:

### Predefined Roles in USM Anywhere

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Dashboard and dashboard views</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Create custom dashboard</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Upper Navigation</td>
<td>Access: documentation, support, and forum links</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Profile Settings</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity &gt; Alarms</strong></td>
<td>View: alarms page and alarm details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Configure filters</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down menu items: add to current filter, find in events, look up in AT&amp;T Alien Labs Open Threat Exchange OTX™</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: full details, configuration issues, vulnerabilities, alarms, events</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Manage columns</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Save views</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Alarm details: alarm action, create rule, suppress alarm, apply label, set a status, add to investigation</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Alarm labels: apply, create, manage</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Alarm Status: update</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
### Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity &gt; Events</strong></td>
<td>View: events page and event details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Configure filters</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: add to current filter, look up in OTX</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: add to current filter, full details, configuration issues, vulnerabilities, alarms, events</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Save views</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Events details: event action, create rule, add to investigation</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
## Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment &gt; Assets</td>
<td>View: assets page and assets details</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure filters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: find in events, look up in OTX, full details, configuration issues, vulnerabilities, alarms, events</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: configure asset, delete asset, asset scan, authenticated scan</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Manage columns</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Save views</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Actions menu: create asset (quick, advanced), import assets, delete selected, edit fields, assign credentials, set sensor, set compliance scope, add to asset group</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset details: deploy an agent, assign credentials, schedule a job</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset details, actions menu: configure asset, delete asset, add to asset group, agent query, asset scan, authenticated scan, assign credentials, schedule scan job</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create event if asset stops sending data</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
## Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment &gt; Asset Groups</td>
<td>View: asset groups page and asset groups details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Configure filters</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset Group drop-down list: full details, configuration issues, vulnerabilities, alarms, events</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset Group drop-down list: configure asset group, delete asset group, asset group scan, assign credentials, authenticated scan</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Save views</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Actions menu: create asset group (static and dynamic)</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset group details, actions menu: configure asset group, delete asset group, edit fields, assign credentials to group members, assign agent profile, set sensor, set compliance scope, asset group scan, assign credentials, authenticated scan, schedule scan job</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
## Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environment &gt; Vulnerabilities</strong></td>
<td>View: vulnerabilities page and vulnerabilities details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Save views</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Vulnerability labels: apply, create, manage</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: add to current filter, find in events, look up in OTX, full details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: configure asset, delete asset, asset scan, assign credentials, authenticated scan</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>New scan</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Vulnerabilities details: select action, apply label</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
## Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environment &gt; Configuration Issues</strong></td>
<td>View: configuration issues page and configuration issues details</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configure filters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Save view</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: add to current filter, look up in OTX, full details, configuration issues, vulnerabilities, alarms, events</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: configure asset, delete asset, assign credentials, authenticated scan</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Asset drop-down list: configure asset, delete asset, asset scan, assign credentials, authenticated scan</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configuration issues details, actions menu: configure asset, delete asset, add to asset group, agent query, asset scan, authenticated scan, assign credentials, schedule scan job</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Configuration issues details: deploy an agent, assign credentials, schedule a scan job</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment &gt; Users</td>
<td>View users page and user details</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>User drop-down list: find in events, full details, configuration issues, alarms, events</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>User drop-down list: configure user, delete user, user scan</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Manage columns</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate report</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>User menu: import users, delete selected, edit fields, configure user, user scan</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Schedule user scan job</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Reports &gt; Saved Reports</td>
<td>View the saved reports page</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Edit, copy, and delete reports</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Reports &gt; Compliance templates</td>
<td>View the compliance templates reports page</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate reports</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Reports &gt; Event type templates</td>
<td>View the event type templates reports page</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Generate reports</td>
<td>❌</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
### Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data sources &gt; Sensors</strong></td>
<td>View the sensor page</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Add a new sensor</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Configure a sensor</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Edit a sensor</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Assign a sensor</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Delete, redeploy a sensor</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Data sources &gt; AlienApps</strong></td>
<td>Available Apps</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Data sources &gt; Agents</strong></td>
<td>Run an agent query</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Delete an agent</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Assign an agent configuration profile</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Data sources &gt; Cloud Connector</strong></td>
<td>View Connector</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Edit Connector</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Add a connector</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Delete Connector</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Add New Data Source Rule</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Enable and Disable a cloud connector</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
### Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Investigations</strong></td>
<td>View investigations page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Edit an investigation</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create a new investigation</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>View investigations details</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Delete an investigation</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Notification rule for investigations</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Add a note</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; Scheduler</strong></td>
<td>View the job scheduler page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create, edit, enable, disable a job</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; Rules</strong></td>
<td>View the rules page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create an orchestration rule</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create a correlation list</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; Notifications</strong></td>
<td>Modify credentials</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; System</strong></td>
<td>View the system monitor page</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>View the network settings page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create asset field</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Modify the session timeout</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; System events</strong></td>
<td>View the system events page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Settings &gt; Console User Events</strong></td>
<td>View the console user events page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
## Predefined Roles in USM Anywhere (Continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Read-Only User</th>
<th>Analyst User</th>
<th>Manager User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings &gt; OTX</td>
<td>Validate an OTX subscription key</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Settings &gt; Credentials</td>
<td>View the credentials page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create a new credential</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Edit, delete, and manage credentials</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Settings &gt; Users</td>
<td>View the user page</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Create a user</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Edit a user</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Delete a user</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Settings &gt; My subscription</td>
<td>View the my subscription page</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Purge data</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Connect to USM Central™</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Editing Users
Assuming the Manager role, you can modify a number of items for the account of another user. For example, if users are unable to log in because they forgot their password or no longer have an authentication mobile device, you can perform a reset for their account.

To edit a user account

1. Go to Settings > Users to open the page that displays the list of user accounts in your USM Anywhere environment.

   ![User List]

   Users can log into USM Anywhere with access based on their assigned roles. All users can edit their credentials by clicking the pencil icon in the upper right-hand corner.

<table>
<thead>
<tr>
<th>EMAIL</th>
<th>FULL NAME</th>
<th>ROLE</th>
<th>STATUS</th>
<th>MULTI-FACTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>MSSP Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSSP Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSSP Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analyst, MSSP</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSSP Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MSSP Manager</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

   **Note:** Sometimes a ⚠ displays in the Status column. This icon means that the user account is locked for 30 minutes after 3 failed login attempts within 15 minutes. You can unlock the account by sending the user a password reset email (see Send Password Reset below).

   If your own user account is locked, you can wait 30 minutes and try again or contact AT&T Cybersecurity Technical Support for assistance.

2. In the row for the user account, click the ✍️ icon.
3. Make changes to the account parameters, as needed.

![Edit User interface]

**Personal Info**
- **Email**: [Input field]
- **Full Name**: Anita

**Role**
- **Manager**

**Status**
- **Enabled**

**Security**
- **Password**
  - **Send Password Reset**
  - **Reset Multi-Factor Authentication**

---

**Note:** If you click the 🔐 of your own user, the Profile page displays. See Managing Your Profile Settings for more information.

- Change the email address for the account.
- Change the full name for the account.
- Change the role for the account. See Role-Based Access Control (RBAC) in USM Anywhere for more information.
- Change the status for the account. If you need to temporarily disable a user account, you can set the status to Disabled. This is a best practice for revoking access and usually a better alternative to deleting a user account.
- Click **Send Password Reset** to reset the password for the user. When you do a password reset, the user receives an email with a link to set a new password for the account.
- Click **Reset Multi-Factor Authentication** to reset the code used to pair a mobile device.
with the account. See Using Multifactor Authentication for more information.

- Select **Enable Multi-Factor Authentication** to enable MFA. See Using Multifactor Authentication for more information.

4. Click **Save**.

**Managing Your Profile Settings**

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

You can manage your own user account, which enables you to do the following:

- Change your email address, name, and password
- Enable **multifactor authentication** (MFA) for the account
- Select your default landing page after you have logged in
- Configure an interval for auto-refreshing the dashboards and alarms pages
- Activate notifications for alarms
To manage your profile settings
1. In the upper right corner of the USM Anywhere web user interface (UI), click the ⬆️ icon and select **Profile Settings**.
Profile Settings

Profile Settings

Profile

API Clients

Personal Info

Role

Manager

Email

Full Name

Security

Password

Last changed Feb 04, 2022

Update Password

Enable multi-factor authentication

Homepage

Page Type

Dashboard

Auto Refresh

Alarms

None

Dashboards

None

Notifications

Email is limited to 200 notifications per rolling 24 hour period.

Receive alarm notifications

Save
2. Modify the data of the items that can be modified.

**Change Your Email Address, Name, and Password**

USM Anywhere helps you meet the Payment Card Industry (PCI) standard by enforcing password complexity, password expiration, and forbidding password reuse. See the USM Anywhere Password Policy for details.

**To set a new password**

1. Open the Profile Settings page.
2. You have two options to choose from based on your role:
   - **General user:** In the upper right corner, click the icon and select Profile Settings.
   - **Manager:** Go to Settings > Users and click the icon of your user.

Both actions open the profile page.

3. Click **Update Password** to display the password fields.

   **Note:** The date of the last update displays in front of the Update Password button.

4. Enter your current password and the new password.
5. Click **Save**.

**Enable MFA**

If you want to protect your account, enable MFA for your user account. When this feature is activated, USM Anywhere displays the multifactor authentication page for you to complete your MFA configuration. The displayed page provides a unique QR code that is used by the Authenticator app to retrieve a verification code. See Using Multifactor Authentication for more information about this security configuration.

**Note:** AT&T Cybersecurity recommends that users enable MFA for their account. MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account.

**To enable MFA**

1. Open the Profile Settings page.
2. You have two options to choose from based on whether your role is as the general user or as the manager:
   - **General user:** In the upper right corner, click the icon and select Profile Settings.
   - **Manager:** Go to Settings > Users and click the icon of your user.
Both actions open the Profile Settings page.

4. Click Save.

Select Your Default Landing Page After You Have Logged In

USM Anywhere gives you the option of selecting your default landing page after you have logged in.

Important: You can also load the configured default landing page by clicking the logo of USM Anywhere located in the upper-left corner of the page.

To select your default landing page after you have logged in

1. Open the Profile Settings page.
2. You have two options to choose from based on whether your role is as the general user or as the manager:
   - **General user**: In the upper right corner, click the icon and select Profile Settings.
   - **Manager**: Go to Settings > Users and click the icon of your user.

Both actions open the Profile Settings page.

3. Select the default home page you want to display after you have logged in. You have these options:
   - **Dashboards**: You can select a specific dashboard to use it as a landing page. The list of dashboards is alphabetically ordered and also includes the custom dashboards you can create.
     
     Note: Keep in mind that dashboard names that begin with a lowercase letter are located at the end of the list.
   - **Activity**: Select alarms or events.
   - **Environment**: Select assets, asset groups, vulnerabilities, or configuration issues.
   - **Investigations**: You can select the investigations page to use it as a landing page.

Important: You have the option of selecting the views you have created. If there is a selected view and you delete that view, when you log in, USM Anywhere displays the main page related to that view. For example, if you select a custom dashboard page to be your landing page and then you delete that custom dashboard, USM Anywhere displays the dashboards page when you log in.

4. Click Save.
Select the Time for Auto-Refreshing the Alarms and Dashboard Pages

If you want to configure the time that the alarms and dashboard pages refresh their information, you can set an interval. These are the options:

- **None**: The page works as usual and displays the ⏰ icon for manually updating the page.
- **Every 5 min**: The page is reloaded every 5 minutes.
- **Every 10 min**: The page is reloaded every 10 minutes.
- **Every 15 min**: The page is reloaded every 15 minutes.

Activate Alarm Notifications

If you want notification on alarms generated by USM Anywhere, activate the notification option for your user account. When this feature is activated, USM Anywhere sends an email to provide real-time notification of critical security incidents.

**Note**: These notifications send emails using Simple Mail Transfer Protocol (SMTP). There is a quota of 200 emails per day.

To activate alarm notifications

1. Open the Profile page.
2. You have two options to choose from based on whether your role is as the general user or as the manager:
   - **General user**: In the upper right corner, click the ⚙ icon and select **Profile Settings**.
   - **Manager**: Go to **Settings > Users** and click the ⚙ icon of your user.

Both actions open the Profile Settings page.

**Note**: It can take up to one hour for the notifications to take effect.

**Important**: This option is not available for AT&T Cybersecurity Managed Security Service Provider (MSSP) users who logged in through USM Central.

**Important**: You will not receive email notifications for suppressed alarms.
4. Click **Save**.

To log out of the system

1. Click the ⚙ icon.
2. Select **Logout**.
USM Anywhere offers a REST API framework that enables you to customize elements of data in your environment. The APIs return JSON responses with errors that use HTTP response codes. To access the API, you will need to create a client ID and secret code in the USM Anywhere interface, and use that information to create a token. USM Anywhere uses OAuth 2.0 to authenticate against the REST APIs.

**Edition:** The API 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.

### To open the API Clients page

1. In the upper right corner of the USM Anywhere web UI, click the **️ icon and select Profile Settings.**
2. Select **API Clients** tab.

### To enable an API Client

1. In the upper right corner of the USM Anywhere web UI, click the **️ icon and select Profile Settings.**
2. Select **API Clients.**
3. Locate the API client that you want to enable and click the icon. This turns the icon green. To disable an already enabled API Client, toggle the icon to its original status.

To edit an API Client

1. In the upper right corner of the USM Anywhere web UI, click the icon and select Profile Settings.
2. Select API Clients.
3. Locate the API client that you want to modify and click the icon to open a new window.

4. Make changes to the client ID, as needed.
5. Click Update Client.

Deleting Users
You can delete a user account in your USM Anywhere whenever you need to.

When deleting a user, keep in mind these points:

- All dashboards created by the user are deleted (including any shared dashboards). See Sharing your Custom Dashboard for more information.
- All views created by the user are deleted (including shared views). See Alarms Views, Assets Views, Configuration Issues List View, Event Views, USM Anywhere System Events List View, Viewing Vulnerabilities Details for more information.
- API clients created by the user are deleted. See API Clients for more information.
- All profile information are deleted (homepage, auto refresh, receiving notifications). See Managing Your Profile Settings for more information.

Note: Despite deleting a user, all their saved generated reports, created or modified rules, and created or modified investigations stays in your environment.

To delete a user account

1. Go to Settings > Users to open the page that displays the list of user accounts in your USM Anywhere environment.
2. In the row for the user account, click the icon.
3. Click Accept to confirm the process or click Cancel to exit.

Configuring Web UI Session Timeout
USM Anywhere enables you to configure the length of users’ inactivity before automatically logging out. After the configured slot of time, the user is logged out of USM Anywhere.

**To configure your web user interface (UI) session timeout**

1. Go to **Settings > System**.
2. In the left navigation panel, click **Session Settings**.
3. Set the session timeout. It can be 15 minutes, 30 minutes, 1 hour, or 2 hours.

A notification bar displays to confirm the change.

**Note:** The new configuration applies after you log in.
Using USM Anywhere for PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing payment account data security. These requirements are a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

About PCI DSS

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. This data can include credit cards, debit cards, ATM cards, and point of sale (POS) cards. The goal of the standard is to protect cardholder data and decrease the possibility of cardholder data theft and/or loss. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

The PCI DSS is made up of 12 requirements that businesses are expected to comply with. These requirements consist of security policies, procedures, and guidelines for storage, processing, and transmission of cardholder data.

About USM Anywhere for PCI DSS

USM Anywhere helps organizations meet PCI DSS requirements and provides out-of-the-box searches, reports, assets and asset group management to give you visibility into your system, application, and device activity relevant to PCI compliance.

USM Anywhere can play a crucial role for you by delivering the technologies necessary to achieve PCI compliance. Many businesses do not have the tools, knowledge, or resources to fulfill the requirements for PCI Compliance.

Working with Assets and PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) views in USM Anywhere have pre-defined filters based on the PCI DSS Asset Group. This section provides instructions on assigning assets to the asset group to populate the views with data.

Note: USM Anywhere generates PCI reports from the assets assigned to the PCI DSS Asset Group. See USM Anywhere Compliance Templates for more information.

To assign Assets to the PCI DSS Asset Group:

1. Go to Environment > Assets.
2. Select the assets you want to include into the PCI DSS Asset Group. See Selecting Assets in Asset List View for assistance.
3. Select Actions > Set Compliance Scope.
4. Select PCI.

5. Click Save and the selected assets will join the PCI DSS Asset Group.
To identify PCI Assets
1. Go to Environment > Assets.
2. In the upper-left corner of the page, click the Configure Filters link.
3. Search for PCI Asset in the available filters.
4. Click the icon to select the filter.
5. Click Apply.
6. In the left panel, scroll to the bottom to find the section for the PCI Asset filter.
7. Click Yes (n). The number in parentheses indicates the number of PCI Assets.
USM Anywhere Investigations

Using AlienVault USM Anywhere, you can create investigations and organize the information from your environment. This feature enables you to manage and coordinate incident response activities. Use Investigations for linking alarms, events, notes, and other files to their responses, and you will have a complete view of actions you have taken to address a particular threat.

This topic discusses these subtopics:

- Investigations List View ................................................................. 736
- Creating a New Investigation .......................................................... 737
- Editing Investigations ........................................................................ 739
- Viewing Investigations Details ......................................................... 740
- Deleting Investigations .................................................................... 752
- Notification Rule for Investigations .................................................. 753
Investigations List View

The Investigations page provides a list of all of the investigations created in your environment. Go to **Investigations** to open a centralized view of your investigations. Each row describes an investigation.

### List of the Default Columns in the Investigations Page

<table>
<thead>
<tr>
<th>Column / Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name identifying the investigation.</td>
</tr>
<tr>
<td>ID</td>
<td>This is a sequential and automatic number assigned by the system that identifies the investigation.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity of the investigation. Values are Low, Medium, High, and Critical.</td>
</tr>
<tr>
<td>Status</td>
<td>The status applied to the investigation. It can be Open, In Review, and Closed. See <strong>Viewing Investigations Details</strong> if you want to change the status.</td>
</tr>
<tr>
<td>Intent</td>
<td>Classify your investigation as Delivery &amp; Attack, Environmental Awareness, Exploitation &amp; Installation, Reconnaissance &amp; Probing, or System Compromise. See <strong>Intent</strong> for more information.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time the investigation was created. The date displayed depends on your computer's time zone.</td>
</tr>
<tr>
<td>Assignee</td>
<td>Email of the person to whom the investigation has been assigned.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time that the Investigation page was last updated. The date displayed depends on your computer's time zone.</td>
</tr>
<tr>
<td>Last Updated by</td>
<td>Email of the last person who has updated the investigation.</td>
</tr>
</tbody>
</table>
Use the ⬆️ icon if you want to modify some information. See Editing Investigations for more information.

Use the ⌒️ icon if you want to delete an investigation. See Deleting Investigations for more information.

**Sort and Filter the Displayed Investigations**

To change the sort order of the displayed list, click the column label for the field that you want to use to sort the list. Use the filters in the upper side of the list to change the displayed list so that it includes only the jobs you want to see. These are the filters:

- **Filter by Title or ID**: Enter a search string for the name of the investigation or the investigation ID to display only matching jobs.
- **Severity**: Select a value between Low, Medium, High, or Critical. You also have the option All to display all of the severities that you have in your environment.
- **Intents**: Select a value of Delivery & Attack, Environmental Awareness, Exploitation & Installation, Reconnaissance & Probing, or System Compromise.
- **Assignee**: Select the email of the person of whom you want to display its assigned investigations.
- **Open**: Select this checkbox if you only want to display the investigations that are open.
- **In Review**: Select this checkbox if you only want to display the investigations that are in review.
- **Closed**: Select this checkbox if you only want to display the investigations that are closed.

**Creating a New Investigation**

AlienVault USM Anywhere enables you to create and manage your own investigation.
To create a new investigation

1. Go to **Investigations**.
2. In the upper right area of the page, click **New Investigation** to open a new window.

   ![](New_Investigation.png)

3. Enter the information in each field.

   **Fields in the New Investigation Dialog box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name identifying the investigation.</td>
</tr>
<tr>
<td>Intent</td>
<td>Classify your investigation as Delivery &amp; Attack, Environmental Awareness, Exploitation &amp; Installation, Reconnaissance &amp; Probing, or System Compromise. See <strong>Intent</strong> for more information.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity of the investigation. Values are Low, Medium, High, and Critical.</td>
</tr>
</tbody>
</table>
Fields in the New Investigation Dialog box (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status applied to the investigation. By default, it is Open and can not be changed. You can change it later to In Review or Closed. See Viewing Investigations Details to learn more about changing the default Status setting.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional.) Enter an investigation description.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**Note:** USM Anywhere automatically assigns every new investigation to the user who creates the investigation. See Editing Investigations to learn how to modify the assigned user.

Editing Investigations

You can make changes to the investigations that you have created, such as changing the title, intent, or status. If an investigation is no longer needed, you can delete it.

**To edit an investigation**

1. Go to **Investigations**.
2. Locate the investigation in the Investigations list.
3. In the row for the investigation, click the 🖋 icon or the title of the investigation.
4. In the Edit Investigation dialog box, change the parameters as needed.

![Edit Investigation dialog box]

- **Title**: test
- **Intent**: System Compromise
- **Severity**: Low
- **Status**: Open
- **Assignee**: [user name]
- **Description**: Optional

See [Creating a New Investigation](#) for more information about these options.

**Note**: USM Anywhere automatically assigns every new investigation to the user who creates the investigation.

5. Click **Save**.

**Viewing Investigations Details**
To view the details of an investigation

1. Go to **Investigations**.
2. Click the title of an investigation to display its details.

On the upper left side of the page is the name of the investigation. Click the **edit** icon next to the name if you want to make changes to the item. See **Investigations List View** for more information about the fields.

Below the investigation name displays the ID of the investigation. There is also information regarding the created and the last updated dates.

You can change the values displayed in the Assignee, Severity, Intent, and Status drop-down lists. The modification is automatic, so once you change a value, it is updated.

This topic discusses these subtopics:

- **Activity on Investigations**
- **Notes on Investigations**
- **Evidence on Investigations**

**Activity on Investigations**
This is an informative section, which enables you to see in chronological order every modification of the investigation.

This section displays this information:
• Type of action that has been done. These actions can be:

**Activity: Type of Action**

<table>
<thead>
<tr>
<th>Type of Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment created</td>
<td>A new file is added to the investigation.</td>
</tr>
<tr>
<td>Attachment deleted</td>
<td>A file is removed from the investigation.</td>
</tr>
<tr>
<td>Attachment updated</td>
<td>A file from the investigation has been updated.</td>
</tr>
<tr>
<td>Evidence linked</td>
<td>An alarm or event has been linked to the investigation.</td>
</tr>
<tr>
<td>Evidence unlinked</td>
<td>An alarm or event has been unlinked from the investigation.</td>
</tr>
<tr>
<td>Investigation created</td>
<td>The user has created the investigation.</td>
</tr>
<tr>
<td>Investigation deleted</td>
<td>The user has removed the investigation.</td>
</tr>
<tr>
<td>Investigation updated</td>
<td>The user has updated the investigation.</td>
</tr>
<tr>
<td>Note Created</td>
<td>A note is created.</td>
</tr>
<tr>
<td>Note Deleted</td>
<td>A note is deleted.</td>
</tr>
<tr>
<td>Note Updated</td>
<td>A note is updated.</td>
</tr>
</tbody>
</table>

• Email of the person who has made a change.

• Date on which the action was made. The displayed date depends on your computer's time zone.

**Notes on Investigations**

USM Anywhere enables you to add notes to your investigations.

**Important:** You can link up to 100 notes to each investigation.

**To add a note**

1. Go to **Investigations**.
2. Locate the investigation in the Investigations list.
3. Click the title of an investigation to display its details.
4. Click Add Note.

5. Enter the text you want to include.

   **Note:** There is a maximum length of 4000 characters, which is about 600 words.

6. Click Save.
   
   The new note displays.

**To edit a note**

1. Go to Investigations.
2. Locate the investigation in the Investigations list.
3. Click the title of an investigation to display its details.
4. Locate the note you want to edit and click the icon.

5. In the Edit Note dialog box, change the text for the note as needed.
6. Click Save.

To delete a note
1. Go to Investigations.
2. Locate the investigation in the Investigations list.
3. Click the title of an investigation to display its details.
4. Locate the note you want to delete and click the icon.

5. Click **Delete** in the confirmation dialog box.

Evidence on Investigations

This section displays the alarms, events, and files associated with the investigation.

**Important:** You can link up to 100 alarms and 100 events to each investigation.
You can click an alarm or an event to go to the alarm or event.

The asset name includes the 🔄 icon if the asset is not in the system, or the 🔄 icon if the asset has been added to the system.

Click the 🔄 icon to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.

- **Find in events**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.

- **Look up in OTX**: This option searches the IP address of the source asset in the AT&T Cybersecurity Alien Labs Open Threat Exchange® (OTX™) page. See Using OTX in USM Anywhere for more information.

- **Add asset to system**: Use this option to create the asset in the system. See Adding Assets for more information.

Click the 🔄 icon to access these options:
- **Add to current filter**: Use this option to add the asset name as a search filter. See Searching Events for more information.

- **Find in events**: Use this option to execute a search of the asset name in the Events page. See Searching Events for more information.

- **Look up in OTX**: This option searches the IP address of the asset in the OTX page. See Using OTX in USM Anywhere for more information.

- **Full Details**: See Viewing Assets Details for more information.

- **Assign Credentials**: See Managing Credentials in USM Anywhere for more information.

- **Authenticated Scan**: This option displays depending on the USM Anywhere Sensor associated with the asset. See Running Authenticated Asset Scans for more information.

- **Scan with AlienApp**: This option enables you to run an asset scan through an AlienApp. See Running Asset Scans Using an AlienApp for more information.

- **Configuration Issues**: This option opens the Asset Details page. The Configuration Issues tab is selected in the page. See Viewing Assets Details for more information.

- **Vulnerabilities**: This option opens the Asset Details page. The Vulnerabilities tab is selected in the page. See Viewing Assets Details for more information.

- **Alarms**: This option opens the Asset Details page. The Alarms tab is selected in the page. See Viewing Assets Details for more information.

- **Events**: This option opens the Asset Details page. The Events tab is selected in the page. See Viewing Assets Details for more information.

**Link an alarm to an investigation**

1. Go to **Activity > Alarms**.

2. Search for the alarm you want to add to the investigation and select it. See Searching Alarms for more information.
3. Click the 📊 icon and select an investigation. You can also create a new one. See Creating a New Investigation for more information.

4. Click Save.

**Link several alarms to an investigation**

1. Go to Activity > Alarms.
2. Search for the alarms you want to add to the investigation and select them. See Searching Alarms for more information.
3. Click Add to Investigation and select an investigation. You can also create a new one. See Creating a New Investigation for more information.

4. Click Save.
**Link an event to an investigation**

1. Go to **Activity > Events**.
2. Search for the event that you want to add to the investigation and select it. See [Searching Events](#) for assistance.
3. Click the ✎ icon and select an investigation. You can also create a new one. See [Creating a New Investigation](#) for more information.

4. Click **Save**.

**Remove a link from an investigation**

1. Go to **Investigations**.
2. Click the title of an investigation to display its details.
3. In the Evidence section, locate the alarm or the event that you want to remove from the investigation and click the ☄ icon.
4. In the confirmation dialog box, click **Remove**.

**Remove a link from alarms or events**

1. Go to **Activity > Alarms** or **Activity > Events** depending on if you want to remove an alarm or an event.

2. Locate the alarm or event that you want to remove from the investigation and select it. See **Searching Events** for assistance.

3. Click the ✍️ icon located in the Investigation field.

4. Select the investigation from which you want to remove the link.

5. Click **Unlink From Investigation**.

6. In the confirmation dialog box, click **Unlink**.
Add a file to an investigation

When adding a file to an investigation, keep in mind these points:

- There is a maximum file size of 24 MB.
- There is a maximum number of five attachments per investigation.

To add a file to an investigation

1. Go to Investigations.
2. Click the title of an investigation to display its details.
3. In the Evidence section, click **Select the file from your desktop** or drop your file in the section.

4. Select the file and click **Open**.

   The file displays in the list.

Deleting Investigations

If an investigation is no longer needed, you can delete it.
To delete an investigation

1. Go to *Investigations*.
2. Click the title of an investigation to display its details.
3. In the row for the investigation, click the icon.

<table>
<thead>
<tr>
<th>LAST UPDATED</th>
<th>LAST UPDATED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22 2019, 12:46 PM</td>
<td>admin@ci-usm-saas-control-aw...</td>
</tr>
<tr>
<td>Feb 22 2019, 12:46 PM</td>
<td>admin@ci-usm-saas-control-aw...</td>
</tr>
<tr>
<td>Feb 22 2019, 12:43 PM</td>
<td>admin@ci-usm-saas-control-aw...</td>
</tr>
</tbody>
</table>

4. In the confirmation dialog box, click **Delete**.

Notification Rule for Investigations
USM Anywhere creates a default notification rule that sends an email notification when there is a change to an investigation.

This is a system rule, and the allowed actions are Enable, Disable, and Edit. If you try to delete it, the rule is restored during the next system update. Go to Settings > Rules to view this notification rule.

**Note:** By default, this rule is disabled.

**Note:** These rules use the `event_severity` field with the values low, medium, high, and critical, and the `event_action` field with the values created, deleted, and updated.

To enable the notification rule for investigations

1. Go to Settings > Rules.
2. Locate the USM Anywhere Investigations Notification rule and click the icon. This turns the icon green. To disable the rule, toggle the icon to its original status.
3. Click an investigation to display its details.
To edit the notification rule for investigations

1. Go to Settings > Rules.
2. Locate the USM Anywhere Investigations Notification rule and click the pencil icon.

3. Make the changes as needed and click Save Rule.

**Note:** The destination email field includes the emails of the users created in the environment as the role of Managers. See Role-Based Access Control (RBAC) in USM Anywhere for more information.
The USM Anywhere web user interface (UI) enables you to view and modify some data related to the configuration of your environment. These pages give you an overall view about the configuration of your system, which is a useful way to have all the essential information. These are the options:

- Check the status of your environment (see USM Anywhere System Monitor for more information)
- Display the summary of your current network configuration. See USM Anywhere Network System and Network Setup and Configuration for more information
- Display and modify your syslog configuration (see Enabling syslog Connections in an AWS VPC for more information)
- Manage asset fields (see Managing Asset Fields for more information)
- Configure a session timeout (see Configuring Web UI Session Timeout for more information)

**USM Anywhere Network System**

The USM Anywhere Network System page enables the user whose role is Manager to display a summary of the configured network.

**To open the USM Anywhere Network System page**

1. Go to **Settings > System**.
2. In the left navigation panel, click **Network Settings**.
3. In case of having more than one sensor in your environment, select a sensor.
   
   The **Network Status Test** starts running.
Note: See Network Setup and Configuration for more information.

USM Anywhere System Monitor

The USM Anywhere System Monitor page enables the user whose role is manager to display statistics of the data coming from sensors inside a time-frame. See Role-Based Access Control (RBAC) in USM Anywhere for more information.

You can choose between the last 24 or 7 hours. If you have more than one sensor configured in your environment, you need to select a sensor.

Go to Settings > System, and then click System Monitor in the left navigation panel. These are the displayed data:
System Monitor Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Events Per Second</td>
<td>Graph displaying the total events received per second. (You can see the current and the filtered events.)</td>
</tr>
<tr>
<td>Fuzzied Events</td>
<td>Graph displaying the total fuzzied events received per second. See About the Was Fuzzied Filter for more information.</td>
</tr>
<tr>
<td>CPU</td>
<td>Graph displaying in percentages the total CPU used.</td>
</tr>
<tr>
<td>CPU Load Average</td>
<td>Graph displaying the load average of the CPU.</td>
</tr>
<tr>
<td>Disk (Software)</td>
<td>Graph displaying in percentages the total disk (software) used.</td>
</tr>
<tr>
<td>Disk (Data)</td>
<td>Graph displaying in percentages the total disk (data) used.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Memory | Graph displaying in percentages the total memory used.
Swap | Graph displaying in percentages the total swap used.

USM Anywhere Log Collection

Syslog is a message-logging standard supported by most devices and operating systems (OSes). USM Anywhere can collect syslog data from devices in your environment and produce corresponding security events and alarms. You can forward syslog data from specific device types to the USM Anywhere Sensor IP address and port.

**Note:** See The Syslog Server Sensor App, Data Sources and Log Processing, and Enable Connections in an AWS VPC for more information.

**To open the Log Collection page**

1. Go to **Settings > System**.
2. In the left navigation panel, click **Log Collection > Syslog Configuration**.
3. If you have more than one USM Anywhere Sensor deployed, use the drop-down menu to select the sensor that you want to configure log collection.

### SysLog Configuration

USM Anywhere can collect syslog data from devices in your environment and produce corresponding security events and alarms.

Please click the button below to learn how to forward syslog data from specific device types to the IP address and port of the USM Anywhere Sensor.

The system is ready to collect data via syslog.

You need to configure your device to point to the following.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IP Address</th>
<th>Port</th>
<th>Packets Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog UDP</td>
<td>[redacted]</td>
<td>514</td>
<td>5,509,243</td>
</tr>
<tr>
<td>Syslog TCP</td>
<td>[redacted]</td>
<td>601</td>
<td>0</td>
</tr>
<tr>
<td>Syslog TLS</td>
<td>[redacted]</td>
<td>634</td>
<td>0</td>
</tr>
<tr>
<td>Syslog EFTP</td>
<td>[redacted]</td>
<td>602</td>
<td>0</td>
</tr>
<tr>
<td>Syslog EFTLS</td>
<td>[redacted]</td>
<td>6515</td>
<td>0</td>
</tr>
</tbody>
</table>

Learn how to configure your device.
Note: If the sensor is receiving syslog messages from your network, you will see IP addresses listed under *Device Sending Data*. For performance reasons, this list only includes devices sending logs in the last 15 minutes. The list refreshes every 30 seconds. After the sensor is updated or the syslog-ng server used by the sensor restarts, the list is reset.

4. Click **How do I configure my device?** to see the instructions for your operating system:
   - **Windows**: This is a link to the [Collecting Windows System Logs](#) page.
   - **Linux**: This is a link to the [Collecting Linux System Logs](#) page.