Copyright © 2020 AT&T Intellectual Property. All rights reserved.

AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or affiliated companies. All other marks are the property of their respective owners.

Updated August 25, 2020
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The AlienVault Agent</td>
<td>4</td>
</tr>
<tr>
<td>Agent Communication</td>
<td>4</td>
</tr>
<tr>
<td>AlienVault Agent Use Cases</td>
<td>5</td>
</tr>
<tr>
<td>Using the AlienVault Agent</td>
<td>5</td>
</tr>
<tr>
<td>Using NXLog</td>
<td>6</td>
</tr>
<tr>
<td>AlienVault Agent Deployment</td>
<td>6</td>
</tr>
<tr>
<td>Agent Deployment Details</td>
<td>7</td>
</tr>
<tr>
<td>Subsequent Agent Deployments Through an Image</td>
<td>7</td>
</tr>
<tr>
<td>Agent Data Collection</td>
<td>8</td>
</tr>
<tr>
<td>AlienVault Agent Installation on Windows Hosts</td>
<td>8</td>
</tr>
<tr>
<td>AlienVault Agent Installation on Linux Hosts</td>
<td>14</td>
</tr>
<tr>
<td>AlienVault Agent Installation on macOS Hosts</td>
<td>21</td>
</tr>
<tr>
<td>AlienVault Agent Configuration Profiles</td>
<td>30</td>
</tr>
<tr>
<td>Assign AlienVault Agent Configuration Profiles to Assets</td>
<td>32</td>
</tr>
<tr>
<td>Assign AlienVault Agent Configuration Profiles to Asset Groups</td>
<td>34</td>
</tr>
<tr>
<td>The AlienVault Agent Command Script and Agent Updates</td>
<td>35</td>
</tr>
<tr>
<td>Complete AlienVault Agent Command List</td>
<td>36</td>
</tr>
<tr>
<td>AlienVault Agent Auto-Update</td>
<td>37</td>
</tr>
<tr>
<td>Memory Consumption by AlienVault Agents</td>
<td>38</td>
</tr>
<tr>
<td>AlienVault Agent Events and Queries</td>
<td>39</td>
</tr>
<tr>
<td>AlienVault Agent Queries</td>
<td>40</td>
</tr>
</tbody>
</table>
The AlienVault Agent

The AlienVault Agent is a lightweight endpoint agent based on osquery, the leading open-source operating system instrumentation framework for Windows, Apple macOS, and Linux. It enables endpoint detection and visibility, file integrity monitoring (FIM), and rich endpoint telemetry capabilities that are essential for complete and effective threat visibility, detection, and compliance.

This agent is easy to install on your host and endpoints, and has a small footprint. An installed agent provides continuous endpoint security monitoring, allowing USM Anywhere to quickly detect threats on your essential assets without the time-consuming manual configuration and setup tasks required to implement and integrate a third-party tool.

Agent Communication

The installed AlienVault Agent communicates over an encrypted channel to send data directly to the USM Anywhere service, bypassing the USM Anywhere Sensor, and buffers data locally when the connection to USM Anywhere is unavailable. When a new agent is registered with your USM Anywhere service, the system checks the AlienVault Agent version. Subsequent updates after the initial install are performed manually through the agent command script. To find out more about the most recent Agent versions, see the AlienVault Agent updates on the Product Announcements page.
AlienVault Agent Use Cases

In USM Anywhere, you can centralize the collection and analysis of Microsoft Windows event logs from your servers or desktops, making it easier to track the health and security of these systems. While the AlienVault Agent is ideal for most traditional end-user laptop or desktop environments, there are some situations for which alternative log collection options, such as NXLog, may be preferable. The table below compares some of the more common use cases between the AlienVault Agent and NXLog.

### AlienVault Agent vs. NXLog Use Cases

<table>
<thead>
<tr>
<th>Environmental Demands</th>
<th>Recommended Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you need to monitor endpoints outside of the network or in remote locations where it would be impractical to deploy a sensor</td>
<td>AlienVault Agent</td>
</tr>
<tr>
<td>If you want the ability to query assets for additional forensic data as part of your investigation activities</td>
<td>AlienVault Agent</td>
</tr>
<tr>
<td>If you want the benefits of AT&amp;T Alien Labs actively monitoring endpoints with updated Alien Lab rules, including active process and network activity information</td>
<td>AlienVault Agent</td>
</tr>
<tr>
<td>If you need to restrict off-premise connections for endpoints</td>
<td>NXLog</td>
</tr>
<tr>
<td>If you need complete control over agent configuration and filtering rules</td>
<td>NXLog</td>
</tr>
<tr>
<td>If you have highly active servers that are required to maintain essential business functions where all or most of your resources are dedicated to the server</td>
<td>NXLog</td>
</tr>
</tbody>
</table>

### Using the AlienVault Agent

The AlienVault Agent provides simple installation, configuration, and management for host monitoring in USM Anywhere without requiring a lot of manual configuration and setup tasks of a third-party agent. When you install the agent on a Windows host, it communicates over an encrypted channel to send data directly to USM Anywhere. The agent installation script configures a default set of folders, files, and registries to automatically support file integrity monitoring (FIM). You can set the configuration profile to manage the queries that USM Anywhere runs for an asset associated with a deployed agent.

Using AlienVault Agents is the best choice for monitoring endpoints outside of the network or in remote locations or where deploying a sensor is impractical. Additionally, it provides the ability to query the asset for additional forensic data as part of your investigation activities. See The AlienVault Agent for more information about the AlienVault Agent and how you can use it to simplify your endpoint detection and response (EDR), FIM, and rich endpoint telemetry capabilities.
Using NXLog

You can use NXLog to collect and forward Windows events to a USM Anywhere Sensor. NXLog is a universal log collection and forwarding agent for basic Windows event logs. But, it's also useful in its own right for suppressing spurious events.

This is the best choice when you need complete control over agent configuration and filtering rules or must restrict cloud connections for the endpoint. There are two ways you can implement NXLog and integrate it with USM Anywhere to collect and forward events from your Windows systems:

- **Install and configure NXLog CE across your Windows hosts** to use custom NXLog configurations to capture non-Windows events on your end servers and forward logs to your USM Anywhere Sensor.
- **Use the Windows Event Collector sensor app** to manage the NXLog subscription used to forward your Windows logs directly to a deployed USM Anywhere Sensor. When you use this method, the sensor acts as the collector and the Windows host will forward the logs directly to the sensor using a private IP address, not over the public Internet.

**Note:** NXLog provides an open source version and a paid, enterprise version. The USM Anywhere Sensor integration using the Windows Event Collector app is based on the enterprise version. And the custom configuration method is based on the open source Community Edition.

AlienVault Agent Deployment

To install the AlienVault Agent on your hosts, you generate an installation script in USM Anywhere that is specific to your USM Anywhere environment. When you run the installation script on the host system, the installed agent automatically registers with your USM Anywhere instance and configures the system to automatically collect data from the endpoint for threat detection. AT&T Cybersecurity recommends that the host system has a minimum of 4 GB memory and 2 CPU cores for the agent. See Windows, Linux, or macOS installation for operating system-specific requirements.

**Note:** When you first deploy new AlienVault Agents on your host systems, you should install just a few so that you can assess the events that are collected by the agent and the impact to your data consumption.

While there is no hard limit on the number of agents you can deploy, larger numbers of agents can eventually begin to impact the performance of USM Anywhere by transmitting more data than your pipeline can accommodate, causing latency in receiving and processing information.

Similarly, if your host system is consistently busy, such as a domain controller or an Active Directory (AD) server, deploying an agent on it may slow down its operations.

**Note:** AlienVault Agents do not currently support the use of a proxy server.
Agent Deployment Details

The Agents page (Data Sources > Agents) provides an overview of your deployed AlienVault Agents.

Click the displayed numbers to view a list of the items in the Assets page. If there are unassociated agents, this page displays an alert to help you resolve them. See Agent and Asset Associations for more information.

Subsequent Agent Deployments Through an Image

You can automate the agent installation on other machines by creating an image with the agent group install script. Using the image of the group install script, you need to configure a one-time scheduled task on the new machine to run the script the next time the machine boots. Any asset created from this image will have the agent installed with its own unique UUID.
Agent Data Collection

Each AlienVault Agent must be associated with an asset in USM Anywhere to enable log collection, which should match the host system where it is deployed. When this association is in place, detailed information is available in the Asset Details page. On this page, you can view the number of events associated with the agent, as well as data consumption by the agent over a fixed period of time. See Viewing Assets Details for more information.

When the agent is registered and associated with an asset, the agent configuration profile determines the queries and intervals that USM Anywhere uses to collect logs from the host system.

The agent dashboard displays status information for all agents registered with your USM Anywhere environment, including an indication that an agent is currently sending data. See AlienVault Agent Dashboard for more information.

AlienVault Agent Installation on Windows Hosts

To install the AlienVault Agent, you must run a script that you access from your USM Anywhere environment. When you run the installation script on the Microsoft Windows host system, the script downloads an .msi file directly from USM Anywhere and the agent automatically registers with your USM Anywhere environment. The installation process also configures a default set of folders, files, and registries to automatically support File Integrity Monitoring (FIM).

You can generate a script that is specific to a selected asset and your USM Anywhere environment, or generate a bulk deployment script that you can use to install the agent on multiple Windows host systems.

**Note:** When you first deploy new AlienVault Agents on your host systems, you should install just a few so that you can assess the events that are collected by the agent and the impact to your data consumption.

While there is no hard limit on the number of agents you can deploy, larger numbers of agents can eventually begin to impact the performance of USM Anywhere by transmitting more data than your pipeline can accommodate, causing latency in receiving and processing information.

Similarly, if your host system is consistently busy, such as a domain controller or an Active Directory (AD) server, deploying an agent on it may slow down its operations.

**Note:** AlienVault Agents do not currently support the use of a proxy server.
Prerequisites

Before you install the AlienVault Agent on a Windows host system, make sure that you have the following requirements in place for that system.

- A 64-bit Windows host running Windows 8.1 or later (client version) or Windows Server 2012 or later (server version).
- The Windows host must have a minimum of 4 GB memory and 2 CPU cores.
- Transport Layer Security (TLS) 1.2 must be enabled on the host system.
- PowerShell 3 or higher is installed on the host system.
- You have login credentials for the host system with full admin rights.
- Firewall configuration to support resource downloads executed by the agent installation script and ongoing event log transmission to USM Anywhere.

- Your firewall is configured to allow temporary downloads to the host system using the HTTPS application protocol over port 443 to support resource downloads executed by the agent installation script:
  
  download.sysinternals.com/files/Sysmon.zip
  
  cybersecurity.att.com/documentation/resources/downloads/sysmon_config_schema4_0.xml
  

- Your firewall is configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:
  
  prod-api.agent.alienvault.cloud
  
  api.agent.alienvault.cloud
  
  <AWS region>-agent-entrypoint.alienvault.cloud

For endpoints that rely on the Amazon Web Services (AWS) region, the endpoint to use depends on the AWS region where your USM Anywhere instance is deployed. See the table below for details. If you are unsure, consult your administrator who set up your USM Anywhere domain.

Note: AT&T Cybersecurity does not own the IP addresses of these endpoints. While relatively stable, they are subject to change by AWS.
AlienVault Agent Endpoints by AWS Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Frankfurt)</td>
<td>eu-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Ireland)</td>
<td>eu-west-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (London)</td>
<td>eu-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
</tbody>
</table>

AlienVault Agent Installation on a Single Host System

For a Windows host system that is already identified as an asset in your USM Anywhere environment, you can install the agent using a generated PowerShell script to run on that Windows host system. You can generate this script for the specific asset from the AlienVault Agents page or from the Asset Details page for the asset.

**Note:** If a single host system is not in your Asset inventory through discovery by a deployed USM Anywhere Sensor, you can manually add the asset using its IP address or fully qualified domain name (FQDN). See Adding Assets for more information.

Alternatively, you can use a script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

**Important:** Some antivirus software may block the osqueryd service and prevent it from starting. If your service is not starting because of antivirus software, you need to add the \Program Files\osquery\osqueryd path to your antivirus exclusions policy.

From the Agents page

1. In USM Anywhere, go to Data Sources > Agents.
2. Click Windows Deployment Script.
3. In the dialog box, select the Single Asset tab.
4. Specify the **Asset** where you want to install the agent.

You can start typing the name or IP address of the asset in the field to display matching items and select the one you want.

Or you can click the **Browse Assets** link to open the Select Asset dialog and browse the asset list to make your selection.

5. Click **Copy to clipboard**.

6. Use a remote access client to connect and log in to the Windows host system.
7. Use the **Run as Administrator** option to open the PowerShell window.
8. Run the copied script.
From the Asset Details page

1. Go to Environment > Assets.
2. (Optional.) Use the Search & Filters options 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.
4. In the Agent Status section, click Deploy Agent.

5. Click Copy to clipboard.

6. Use a remote access client to connect and log in to the Windows host system.
7. Use the Run as Administrator option to open the PowerShell window.
8. Run the copied script.

AlienVault Agent Installation on Multiple Host Systems

If you have multiple Windows host systems that are not currently in your USM Anywhere asset inventory or you don't want to generate a separate script for each asset, you can install the AlienVault Agent using a generated PowerShell script on any Windows host system that meets the
prerequisite requirements. You can generate this script from the Agents page.

**Note:** If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script does not have the unique asset ID. In this case, USM Anywhere attempts to associate the AlienVault Agent with an existing asset if there is enough information and it can make a definitive match. After a successful deployment of the agent on a host, it sends only heartbeat events until it has an asset association. These heartbeat events include basic information about the host system, including network interfaces and IP address, as well as the asset UUID.

When a deployed agent does not have an associated asset, you must make this association in USM Anywhere in order to enable queries and log collection for the host system. For more information, see Agent and Asset Associations.

**To generate an agent deployment script for multiple host systems**

1. In USM Anywhere, go to **Data Sources > Agents**.
2. Click **Windows Deployment Script**.
   
   In the dialog box, the Multiple Assets tab is selected by default.

3. Click **Copy to clipboard**.

![Windows Deployment Script](image)

4. Run the script on each Windows host system where you want to deploy the agent.
   
   - Use a remote access client to connect and log in to the Windows host system.
   - Use the **Run as Administrator** option to open the PowerShell window.
   - Run the copied script.
Additional AlienVault Agent Commands

The AlienVault Agent also comes with a PowerShell script to control other features of the agent, such as starting, stopping, restarting, updating, and uninstalling the agent. See the AlienVault Agent Command Script and Agent Updates documentation page for more information of the agent command script, including the file location and a list of the commands.

Installation Error Resolution

After the AlienVault Agent is installed, the Asset UID associations are stored in the osquery.flags file in your system. Asset changes, specifically changes that result in an asset being removed and added back to USM Anywhere, can cause issues with the way an agent associates with those assets in the future if you need to reinstall the agent for any reason.

If you encounter an error during installation of an agent, you need to remove the osquerydirectory before you reinstall the agent. To do this, delete the C:\Program Files\osquery folder.

AlienVault Agent Installation on Linux Hosts

To install the AlienVault Agent, you must run a script that you access from your USM Anywhere environment. When you run the installation on the Linux host system, the script downloads a .deb or .rpm file directly from USM Anywhere and the agent automatically registers with your USM Anywhere environment. The installation process also configures a default set of paths to automatically support File Integrity Monitoring.

You can generate a script that is specific to a selected asset and your USM Anywhere environment, or generate a bulk deployment script that you can use to install the agent on multiple Linux host systems.

At this time, agent support is limited to host systems running a 64-bit OS. Dependent libraries for 32-bit to support the agent are not currently available.

**Note:** When you first deploy new AlienVault Agents on your host systems, you should install just a few so that you can assess the events that are collected by the agent and the impact to your data consumption.

While there is no hard limit on the number of agents you can deploy, larger numbers of agents can eventually begin to impact the performance of USM Anywhere by transmitting more data than your pipeline can accommodate, causing latency in receiving and processing information.

Similarly, if your host system is consistently busy, such as a domain controller or an Active Directory (AD) server, deploying an agent on it may slow down its operations.

**Note:** AlienVault Agents do not currently support the use of a proxy server.
Prerequisites

Before you install the AlienVault Agent on a Linux host system, make sure that you have the prerequisites in place for that system.

- The 64-bit Linux host system is running a Red Hat or Debian-based distribution, such as Ubuntu or Mint

  Note: The AlienVault Agent installation has been tested on Ubuntu 14 and 16, a recent version of CentOS, Amazon Linux, and a handful of other Linux types. It is designed to work on any Linux version on 64-bit Intel that uses either APT or RPM to install packages.

- rsyslog is installed on the host system (see https://www.rsyslog.com/).
- curl is installed on the host system (see https://curl.haxx.se/download.html).
- You have login credentials for the host system with sudo privileges.
- Your firewall is configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

  prod-api.agent.alienvault.cloud
  api.agent.alienvault.cloud
  <AWS region>-agent-entrypoint.alienvault.cloud

For endpoints that rely on the Amazon Web Services (AWS) region, the endpoint to use depends on the AWS region where your USM Anywhere instance is deployed. See the table below for details. If you are unsure, consult your administrator who set up your USM Anywhere domain.

  Note: AT&T Cybersecurity does not own the IP addresses of these endpoints. While relatively stable, they are subject to change by AWS.
### AlienVault Agent Endpoints by AWS Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Frankfurt)</td>
<td>eu-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Ireland)</td>
<td>eu-west-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (London)</td>
<td>eu-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
</tbody>
</table>

### AlienVaultAgent Installation on a Single Host System

For a Linux host system that is already identified as an asset in your USM Anywhere environment, you can install the agent using a generated bash script to run on that Linux host system. You can generate this script for the specific asset from the Agents page or from the Asset Details page for the asset.

**Note:** If a single host system is not in your Asset inventory through discovery by a deployed USM Anywhere Sensor, you can manually add the asset using its IP address or fully qualified domain name (FQDN). See Adding Assets for more information.

Alternatively, you can use a script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

**Important:** Some antivirus software may block the osqueryd service and prevent it from starting. If your service is not starting because of antivirus software, you need to add the `/usr/bin/` path to your antivirus exclusions policy.

**From the Agents page**

1. In USM Anywhere, go to **Data Sources > Agents**.
2. Click **Linux Deployment Script**.
3. In the dialog box, select the **Single Asset** tab.
4. Specify the **Asset** where you want to install the agent.
You can start typing the name or IP address of the asset in the field to display matching items and select the one you want.

Or you can click the **Browse Assets** link to open the Select Asset dialog and browse the asset list to make your selection.

5. **Select the Package Manager** type for the Linux distribution.
   The *deb* type is selected by default. If the asset uses a Red Hat distribution, select the *rpm* type.

6. Click **Copy to clipboard**.

7. Use an SSH client to connect and log in to the asset host system.
8. Run the copied bash script.

**From the Asset Details page**

1. Go to Environment > Assets.
2. (Optional.) Use the Search & Filters options 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.
4. In the Agent Status section, click Deploy Agent.

5. Select the Package Manager type for the Linux distribution.
   - The deb type is selected by default. If the asset uses a Red Hat distribution, select the rpm type.
6. Click Copy to clipboard.

7. Use an SSH client to connect and log in to the asset host system.
8. Run the copied bash script.
AlienVault Agent Installation on Multiple Host Systems

If you have multiple Linux host systems that are not currently in your USM Anywhere asset inventory or you don't want to generate a separate script for each asset, you can install the AlienVault Agent using a generated bash script on any Linux host system that meets the prerequisite requirements and supports the package type for the script. You can generate this script from the Agents page.

**Note:** If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script does not have the unique asset ID. In this case, USM Anywhere attempts to associate the AlienVault Agent with an existing asset if there is enough information and it can make a definitive match. After a successful deployment of the agent on a host, it sends only heartbeat events until it has an asset association. These heartbeat events include basic information about the host system, including network interfaces and IP address, as well as the asset UUID.

When a deployed agent does not have an associated asset, you must make this association in USM Anywhere in order to enable queries and log collection for the host system. For more information, see Agent and Asset Associations.

You can generate this script from the Agents page. After you use the script to deploy the agent on your Linux host systems, you can view the list of unassigned agents and then associate each agent with an existing asset or add a new asset using the information provided by the agent.

**To generate an agent deployment script for multiple host systems**

1. In USM Anywhere, go to Data Sources > Agents.
2. Click Linux Deployment Script.
   
   In the dialog box, the Multiple Assets tab is selected by default.
3. Select the Package Manager type for the Linux distribution.
   
   The deb type is selected by default. If the asset uses a Red Hat distribution, select the rpm type.
4. Click Copy to clipboard.
5. Run the script on each Linux host system where you want to deploy the agent.
   - Use an SSH client to connect and log in to the asset host system.
   - Run the copied bash script.

Additional AlienVault Agent Commands

The AlienVault Agent also comes with a bash script to control other features of the agent, such as starting, stopping, restarting, updating, and uninstalling the agent. See the The AlienVault Agent Command Script and Agent Updates documentation page for more information of the agent command script, including the file location and a list of the commands.

Installation Error Resolution

After the AlienVault Agent is installed, the Asset UID associations are stored in the `osquery.flags` file in your system. Asset changes, specifically changes that result in an asset being removed and added back to USM Anywhere, can cause issues with the way an agent associates with those assets in the future if you need to reinstall the agent for any reason.

If you encounter an error during installation of an agent, you need to remove the `osquery` directory before you reinstall the agent. To do this, enter either `apt-get purge alienvault-agent` or `yum remove alienvault-agent` in the command line, and then reinstall the agent.
AlienVault Agent Installation on macOS Hosts

To install the AlienVault Agent, you must run a script accessible from your USM Anywhere environment. When you run the installation on an Apple macOS host system, the script downloads a .pkg file directly from USM Anywhere and the agent automatically registers with your USM Anywhere environment. The installation process also configures a default set of paths to automatically support File Integrity Monitoring.

You can generate a script that is specific to a selected asset and your USM Anywhere environment, or generate a bulk deployment script that you can use to install the agent on multiple macOS host systems.

Prerequisites

Before you install the AlienVault Agent on a macOS host system, make sure that

- You are running macOS Sierra 10.12 or later.
- You have login credentials for the host system with sudo privileges.
- Your firewall is configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:
  
  prod-api.agent.alienvault.cloud
  
  api.agent.alienvault.cloud
  
  <AWS region>-agent-entrypoint.alienvault.cloud

For endpoints that rely on the Amazon Web Services (AWS) region, the endpoint to use depends on the AWS region where your USM Anywhere instance is deployed. See the table below for details. If you are unsure, consult your administrator who set up your USM Anywhere domain.

**Note:** AT&T Cybersecurity does not own the IP addresses of these endpoints. While relatively stable, they are subject to change by AWS.

<table>
<thead>
<tr>
<th>Region</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>ap-south-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2-agent-entrypoint.alienvault.cloud</td>
</tr>
</tbody>
</table>
AlienVault Agent Endpoints by AWS Regions (Continued)

<table>
<thead>
<tr>
<th>Region</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada (Central)</td>
<td>ca-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Frankfurt)</td>
<td>eu-central-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (Ireland)</td>
<td>eu-west-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>EU (London)</td>
<td>eu-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>sa-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1-agent-entrypoint.alienvault.cloud</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2-agent-entrypoint.alienvault.cloud</td>
</tr>
</tbody>
</table>

AlienVault Agent Installation on a Single Host System

For a macOS host system that is already identified as an asset in your USM Anywhere environment, you can install the AlienVault Agent using a generated Terminal script to run on that macOS host system. You can generate this script for the specific asset from the Agents page or from the Asset Details page for the asset.

**Note:** If a single host system is not in your Asset inventory through discovery by a deployed USM Anywhere Sensor, you can manually add the asset using its IP address or fully qualified domain name (FQDN). See Adding Assets for more information.

Alternatively, you can use a script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

**Important:** Some antivirus software may block the osqueryd service and prevent it from starting. If your service is not starting because of antivirus software, you need to add the `/usr/local/bin/` path to your antivirus exclusions policy.

**From the Agents page**

1. In USM Anywhere, go to **Data Sources > Agents**.
2. Click **macOS Deployment Script**.
3. In the dialog box, click the **Single Asset** tab.
4. Specify the **Asset** where you want to install the agent.
   - You can start typing the name or IP address of the asset in the field to display matching items and select the one you want.
Or you can click the Browse Assets link to open the Select Asset dialog and browse the asset list to make your selection.

5. Click Copy to clipboard.

6. Use a remote access client to connect and log in to the macOS host system.

7. Open the Terminal and enter a sudo command containing the script you copied to the clipboard.

From the Asset Details page

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

4. In the Agent Status section, click **Deploy Agent**.

5. Click **Copy to clipboard**.

6. Use an SSH client to connect and log in to the asset host system.

7. Run the copied bash script.

**AlienVault Agent Installation on Multiple Host Systems**

If you have multiple macOS host systems that are not currently in your USM Anywhere asset inventory or you don’t want to generate a separate script for each asset, you can install the AlienVault Agent using a generated Terminal script on any macOS host system that meets the prerequisite requirements and supports the package type for the script. You can generate this script from the **Agents page**.
**Note:** If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script does not have the unique asset ID. In this case, USM Anywhere attempts to associate the AlienVault Agent with an existing asset if there is enough information and it can make a definitive match. After a successful deployment of the agent on a host, it sends only heartbeat events until it has an asset association. These heartbeat events include basic information about the host system, including network interfaces and IP address, as well as the asset UUID.

When a deployed agent does not have an associated asset, you must make this association in USM Anywhere in order to enable queries and log collection for the host system. For more information, see Agent and Asset Associations.

You can generate this script from the Agents page. After you use the script to deploy the agent on your macOS host systems, you can view the list of unassigned agents and then associate each agent with an existing asset or add a new asset using the information provided by the agent.

**To generate an agent deployment script for multiple host systems**

1. In USM Anywhere, go to Data Sources > Agents.
2. Click macOS Deployment Script.
   
   In the dialog box, the Multiple Assets tab is selected by default.
3. Select the Package Manager type for the macOS distribution.
   
   Click Copy to clipboard.

   ```bash
   CONTROL_NODE_ID=ce3e814d5ae-42cc-b3d4-0ac4753f7ab4 bash -c "$(curl https://ci-rt45fyrewq789asdfg00oqwertylipj234557890?flavor=pkgi)"
   ``

4. Use a remote access client to connect and log into the macOS host system.
5. Open the Terminal and enter a sudo command containing the script you copied to the clipboard.

**Additional AlienVault Agent Commands**

The AlienVault Agent also comes with a bash script to control other features of the agent, such as starting, stopping, restarting, updating, and uninstalling the agent. See the The AlienVault Agent Command Script and Agent Updates documentation page for more information of the agent.
command script, including the file location and a list of the commands.

Installation Error Resolution

After the AlienVault Agent is installed, the Asset UID associations are stored in the osquery.flags file in your system. Asset changes, specifically changes that result in an asset being removed and added back to USM Anywhere, can cause issues with the way an agent associates with those assets in the future if you need to reinstall the agent for any reason.

If you encounter an error during installation of an agent, you need to remove the osquery directory before you reinstall the agent. To do this, delete the /var/osquery folder.

Agent and Asset Associations

If you use a single asset installation script, the USM Anywhere asset universally unique identifier (UUID) for the selected asset is incorporated into that script. During the installation process, the deployed AlienVault Agent registers with your USM Anywhere instance, makes the asset association, and updates the operating system (OS) name and network interface information on the asset.

However, if you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script does not contain any UIDs. In this case, USM Anywhere attempts to associate the agent with an existing asset. The agent then attempts to make a definitive match by using either the Microsoft Azure virtual machine (VM) UIDs or Amazon Web Services (AWS) instance IDs; otherwise, it will attempt to pair based on other asset data fields including media access control (MAC) address, IP address, and hostname. Before installing the agent, AT&T Cybersecurity recommends that you perform a full asset scan. This way, USM Anywhere will have identified the asset and, therefore, can automatically associate the asset with the agent, rather than having the agent create the association independently.

After a successful deployment of the agent on a host, it sends only heartbeat events until it is has an asset association. These heartbeat events include basic information about the host system, including network interfaces and IP address, as well as the asset UUID.

The heartbeat events are important for monitoring AlienVault Agent connectivity; therefore, it is important that you do not create any filtering rules to remove these notifications. If you don’t want to see heartbeat events, AT&T Cybersecurity recommends that you create a suppression rule instead.

When a deployed agent does not have an associated asset, you must make this association in USM Anywhere to enable queries and log collection for the host system. The Agents page displays an alert when there are one or more unassociated assets, and provides tools designed to help you associate these agents with assets. It provides a list of suggested assets for selection and an easy way to create a new asset using the information provided by the agent.
When you see this alert, click **Associate agents with assets** to open the Associate Agents With Assets page and complete the association.

**Associate or Unassociate the AlienVault Agent with an Existing Asset**

If you believe that the asset for the host system exists in the USM Anywhere asset inventory or you are unsure, you can allow USM Anywhere to suggest one or more matching assets. If the suggested asset does not display a correct item, you can find the asset yourself and select it for the association.

**Note:** There is currently no way to remove the association between an AlienVault Agent and an asset. If you need to change an association, you must uninstall the agent on the host system, redeploy the agent, and then make the new association as needed.

**To make an association to an existing asset**

1. In the row for the unassociated agent, click **Associate Agent with Asset**.
   - The dialog box displays a list of one or more suggested asset matches if USM Anywhere is able to locate potential matches in the asset library.
2. Select an asset for the agent:
- If one of the suggested assets is correct, select the asset.
- If the correct asset is not displayed or there are no suggested assets, enter part of the name or IP address of the asset in the Search field to display matching items and select the asset you want.

Or you can click the **Browse Assets** link to open the Select Asset dialog box and browse the asset list to make your selection.

If you are unable to locate the correct asset and determine that it does not currently exist in the asset inventory, you can click the **create a new asset** link to generate a new asset for the agent.

3. Click **Save**.

A confirmation dialog box opens.

4. If you want to display the Asset Details page for the associated asset, click **View Asset**.

Otherwise, click **Cancel** to close the dialog box and return to the Associate Agents with Assets page.
To remove the link between an asset and an agent

1. Go to Data Sources > Agents.

2. Click Unassociate assets.

The link between the asset and the agent is removed.

When an asset is deleted, all of its associated AlienVault Agents automatically become unassociated.

Create New Assets for the Association

If the asset does not yet exist in the USM Anywhere asset inventory, you can automatically create an asset for one or more selected AlienVault Agents. When USM Anywhere creates a new asset for the agent, it uses the hostname value for the asset name. After creation, you can modify various asset details as needed. See Editing the Assets for more information.

To create new assets for unassigned agents

1. For each of the listed agents where an asset does not already exist in the asset inventory, select the checkbox for that row.

   If you want to create new assets for all of the listed agents, you can select the checkbox at the top.

2. At the top-right of the page, click the Create New Assets button.
A confirmation dialog box opens.

3. Close the dialog box to return to the Associate Agents with Assets page.

**AlienVault Agent Configuration Profiles**

USM Anywhere includes out-of-the-box AlienVault Agent configuration profiles to manage the queries that it runs for an asset associated with a deployed agent. For each configuration profile, you can view the list of queries, a description of the collected logs, and the query frequency. Depending on your needs, you can change the default configuration profile so that you collect the log data and generate the events for the newly deployed agents.

USM Anywhere provides two configuration profiles for each of the agent deployment types: optimized and full. There are both preferable and less-than-preferable data security and data consumption reasons for choosing either configuration profile. Use the following information to help you determine which configuration profile works best for your setup.

**Linux**

- **Optimized**: The optimized profile reduces data consumption by modifying the query behavior in the following ways.
  - Does not collect syslog events.
  - Collects New Process events and correlates for threat detection purposes, but stores them only when they are associated with an alarm.
  - Collects Outbound Socket events and correlates for threat detection purposes, but stores them only when they are associated with an alarm.

**Note:** The optimized configuration profile monitors files in a specific set of locations. Because the locations of the monitored files are limited, the optimized profile cannot guarantee that the AlienVault Agent is tracking all user interaction with secured files. This means that the optimized agent profile on its own doesn't satisfy PCI DSS Requirement 10.
• **Full**: The full (verbose) profile collects and stores all Linux log events, including syslog events, New Process events, and Outbound Socket events.

Using this profile could have a significant impact on your data consumption. See Subscription Management for more information about how USM Anywhere manages data consumption and storage.

**Windows**

• **Optimized**: The optimized profile reduces data consumption by modifying the Windows Events query to retrieve only the event types that impact threat detection.

For a list of the log collection paths monitored by this profile, go to Data Sources > Agents > Configuration Profiles and click the Optimized profile for Windows, and then click the Log Collection tab to display the full list of paths.

• **Note**: The optimized configuration profile monitors files in a specific set of locations. Because the locations of the monitored files are limited, the optimized profile cannot guarantee that the AlienVault Agent is tracking all user interaction with secured files. This means that the optimized agent profile on its own doesn’t satisfy PCI DSS Requirement 10.

• **Full**: The full (verbose) profile collects and stores most Windows event types, ignoring a few events that provide little value as determined by the AT&T Alien Labs™ team.

For a list of the log collection paths monitored by this profile, go to Data Sources > Agents > Configuration Profiles and click the Optimized profile for Windows, then click the Log Collection tab to display the full list of paths.

Using this profile could have a significant impact on your data consumption. See Subscription Management for more information about how USM Anywhere manages data consumption and storage.

**macOS**

• **Optimized**: The optimized profile reduces data consumption by filtering certain events that are not correlated with alarms.

• **Note**: The optimized configuration profile monitors files in a specific set of locations. Because the locations of the monitored files are limited, the optimized profile cannot guarantee that the AlienVault Agent is tracking all user interaction with secured files. This means that the optimized agent profile on its own doesn’t satisfy PCI DSS Requirement 10.

• **Full**: The profile collects all event collection and storage, which may have a significant impact on data consumption.

Using this profile could have a significant impact on your data consumption. See Subscription Management for more information about how USM Anywhere manages data consumption and storage.
In the Configuration Profiles view you can click the individual profile name to display detailed information about the queries and the collected log information included for a profile. If you are looking for a specific type of log information, enter text in the search field and click the search icon (🔍) to filter the query list. If you want to see the specific file paths included in the profile’s file integrity monitoring (FIM), click the File Integrity tab to display these paths by category.

Note: Currently, the Windows FIM paths are as follows:

- C:\Windows\System32\drivers\etc\hosts
- C:\autoexec.bat
- C:\config.sys
- C:\boot.ini

More Windows FIM paths will be added in future updates.

To display the agent configuration profiles

1. Go to Data Sources > Agents.
2. Click Configuration Profiles.
3. Review and select the configuration profile you want to use by default.

Important: The Experimental Profiles are temporary and internal. Do not use them unless you have instructions from the AlienVault Technical Support department.

Assign AlienVault Agent Configuration Profiles to Assets

To assign a specific AlienVault Agent configuration profile to an asset from the Assets list view

1. Go to Environment > Assets.
2. Search the asset and select Actions > Assign Agent Profile.
3. Choose the agent profile you want to assign to the selected asset.
USM Anywhere™ Agents Guide

**USM Anywhere™** displays an informative message if assets exist that do not have agents deployed.

**4. Click Save.**

**To assign a specific agent configuration profile to an asset from the details of an asset**

1. **Go to Environment > Assets.**
2. **Search the asset and click the **icon located next to the asset name you want to assign to the specific agent configuration profile, select Full Details.**
3. Click Agent.

4. Click the Configuration Profile combo and select the profile you want to assign.

Assign AlienVault Agent Configuration Profiles to Asset Groups

To assign an AlienVault Agent configuration profile to an asset group

1. Go to Environment > Asset Groups.

2. Next to the asset group that you want to assign the profile, click the icon and select Full Details.

3. Select Actions > Assign Agent Profile.
4. Choose the agent profile you want to assign to the selected asset group.

![Configure Asset Group Members](image)

Some of the selected assets do not have agents deployed. Profiles will only be applied to assets with agents.

<table>
<thead>
<tr>
<th>SELECTED ASSETS</th>
<th>IP ADDRESSES</th>
<th>SENSOR</th>
<th>CREDENTIALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>develop-usma-testFixtures-windows2016-...</td>
<td>IP ADDRESS</td>
<td>USMA-Sensor AWS</td>
<td>-</td>
</tr>
<tr>
<td>windowsTrainingAgent2</td>
<td>IP ADDRESS</td>
<td>USMA-Sensor AWS</td>
<td>-</td>
</tr>
<tr>
<td>develop-usma-testFixtures-windows2012-...</td>
<td>IP ADDRESS</td>
<td>USMA-Sensor AWS</td>
<td>-</td>
</tr>
<tr>
<td>win2018core</td>
<td>IP ADDRESS</td>
<td>USMA-Sensor AWS</td>
<td>-</td>
</tr>
<tr>
<td>tpoyatowin-2008-r2</td>
<td>IP ADDRESS</td>
<td>USMA-Sensor AWS</td>
<td>-</td>
</tr>
</tbody>
</table>

1 - 5 of 16

Choose Agent Profile
This agent profile will be assigned to the members of asset group

Windows Profile

5. Click **Save**.

The AlienVault Agent Command Script and Agent Updates

The AlienVault Agent script enables you to run a number of commands for the installed agent. Each operating system (OS) has its own script, but the commands function the same across all systems. To use the command script, locate and run the file listed in the following table and follow any additional instructions that are noted.
Location and Notes for the AlienVault Agent Scripts

<table>
<thead>
<tr>
<th>System</th>
<th>Script</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>alienvault-agent.ps1</td>
<td>C:\Program Files\osquery</td>
<td>This is not part of the default Microsoft Windows path, so you must either use cd commands to point to the path, or input the path directly to run the script.</td>
</tr>
<tr>
<td>Linux</td>
<td>alienvault-agent.sh</td>
<td>/usr/bin</td>
<td>Opened from the command line.</td>
</tr>
<tr>
<td>macOS</td>
<td>alienvault-agent.sh</td>
<td>/usr/local/bin</td>
<td>Opened in Terminal.</td>
</tr>
</tbody>
</table>

Complete AlienVault Agent Command List

The following table contains the complete list of commands for the AlienVault Agent script. The agent configuration, which includes information such as osquery data point checks and file integrity monitoring (FIM) paths, is checked and updated independently.

Commands Available for the AlienVault Agent Script

<table>
<thead>
<tr>
<th>Command</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Start the agent service.</td>
</tr>
<tr>
<td>stop</td>
<td>Stop the agent service.</td>
</tr>
<tr>
<td>restart</td>
<td>Restart the agent service.</td>
</tr>
<tr>
<td>update</td>
<td>Update the agent version.</td>
</tr>
<tr>
<td>enable-auto-update [time]</td>
<td>Enable auto-update to check daily for new version.</td>
</tr>
<tr>
<td></td>
<td>Time can optionally be designated for the check (24-hour format HH:MM).</td>
</tr>
<tr>
<td></td>
<td>If no time is supplied, the daily check will occur between 09:00 and 17:00.</td>
</tr>
<tr>
<td>disable-auto-update</td>
<td>Disable agent auto-update.</td>
</tr>
<tr>
<td>force-update</td>
<td>Reinstall the agent service with the newest version.</td>
</tr>
<tr>
<td></td>
<td>(This reinstall the agent even if you are running the most recent version.)</td>
</tr>
<tr>
<td>uninstall</td>
<td>Uninstall the agent.</td>
</tr>
<tr>
<td>version</td>
<td>Print the agent version number.</td>
</tr>
<tr>
<td>help</td>
<td>Print help.</td>
</tr>
<tr>
<td>config</td>
<td>Connect to the agent API server to print or download your agent configuration.</td>
</tr>
</tbody>
</table>
## AlienVault Agent Auto-Update

The AlienVault Agent can be configured to automatically update using your system's task scheduler, provided that your system is online at the time the update is scheduled and there are no local configurations preventing the scheduled task from being enacted. The agent script's `report` command can be used to verify that the auto-update function is active. The following information provides the steps for enabling the agent's auto-update function for each OS.

**Note:** The auto-update feature only exists in agent version 20.07.0003.0301 and later. If you are on an earlier version of the agent, you need to manually update the agent to access the auto-update feature.

### Linux

**To enable agent auto-updates on Linux**

1. Run the following command from a bash shell:

   ```bash
   alienvault-agent.sh enable-auto-update HH:MM
   ```

   Entering the time (HH:MM) is optional and, if not entered, the system will check for an update between 09:00 and 17:00.

2. Verify that osquery is running in your Linux terminal.

### Windows

**To enable agent auto-updates on Windows**

1. Run the following command from PowerShell as an admin:

   ```bash
   C:\'Program Files'\osquery\alienvault-agent.ps1 enable-auto-update HH:MM
   ```

   Entering the time (HH:MM) is optional and, if not entered, the system will check for an update.
between 09:00 and 17:00.

2. Verify that osquery is running in the Windows Task Manager.

**macOS**

To enable agent auto-updates on macOS

1. Run the following command from a bash shell:

   ```bash
   alienvault-agent.sh enable-auto-update HH:MM
   ```

   Entering the time \((HH:MM)\) is optional and, if not entered, the system will check for an update between 09:00 and 17:00.

2. Verify that osquery is running in the macOS Activity Monitor.

**Memory Consumption by AlienVault Agents**

The AlienVault Agent is configured to have two osquery processes running: an initial osquery process that functions as a watchdog, and the child worker processes that creates the scheduled queries. The initial watchdog process manages child and terminates any processes that exceed the memory limitations configured in the watchdog settings. The agent uses the default watchdog settings, but you may need to reconfigure it through the command line using the daemon control flags.

Once the watchdog limit is reached, osquery closes child processes and encounters errors. Because the watchdog limits are a percentage of total CPU and memory resources available, this means that the available resources scale with the system memory. Therefore, if the osqueryd process is using 100MB memory, that equates to 2.5% of resources of a 4GB system, 10% of the resources of a 1GB system, or 20% of the resources of a 500MB system. Similarly, if a virtual machine (VM) only has 1 CPU core available, the watchdog percentages are twice those for a 2-core system.

If the osquery processes are exceeding their allocated resources, that could result in the watchdog truncating the process without giving any error message. A good indicator that this has happened can be found by looking at the logs subdirectory and looking at the timestamps of the files: if there is a high number of files with timestamps that are close together, it could be that the watchdog has been killing processes due to resource allocation limits.
AlienVault Agent Events and Queries

Edition: This feature is available in the Standard and Premium editions of USM Anywhere.

USM Anywhere enables you to use the AlienVault Agent data source to filter the AlienVault Agent-related events.

These Data Source are related to the agent:

- **AlienVault Agent**: This data source parses the events from the agent, with the exception of Windows events.
- **AlienVault Agent - Windows EventLog**: This data source parses Microsoft Windows events sent through the agent.

**To search events using the filter related to the agent**

1. Go to **Activity > Events**.
2. Locate the Data Source section.
3. Click an event and the result of your search displays.
AlienVault Agent Queries

USM Anywhere enables you to run a user-initiated AlienVault Agent query based on the events sent by connected agents. There are several ad-hoc queries, which are in your environment by default. These queries, listed below, generate events that can be used for a forensic investigation, so you can focus on fast response and remediation.

To run a user-initiated agent query from the Agents page

1. Go to Data Sources > Agents.
2. Click Run Agent Query.
   
   All Assets With Agent
   
   You can select the operating system (OS):
   
   - All
   - Windows
   - Linux
   - macOS
   
   Single Asset
   
   Select the asset in which you want to run the agent query. You can enter the asset name or browse assets.

3. Select a query in the Action field.
4. Click Run.

   Note: The queries generate events when you run them. They do not generate events continuously; you have to run the query again if you want to generate new events.

   To run a user-initiated agent query from the details view of an Alarm
   
   1. Go to Activity > Alarms.
   2. Click the alarm to display its details.
   3. Select Select Action > Agent Query.
   4. Select an action.
   5. Click Run.
      
      A dialog box displays to confirm the action has been initiated.
   6. Click OK.
      
      Or click Create rule for similar events if you want to create a new rule. See Response Action Rules from the Orchestration Rules Page for more details.
When the query is complete, the results are visible in events. You can also click the Agent tab in the details of the asset to see the Query History. You can see the name of the query, the date on which the query was run, the status (Query In Progress, Processing Events, and Completed), and, once the query is complete, there is the View Results link. This link goes to the filtered events.

**Note:** The queries generate events when you run them. They do not generate events continuously; you have to run the query again if you want to generate new events.

### To run a user-initiated agent query from the details view of an Event

1. Go to **Activity > Events**.
2. Click the event to display its details.
3. Select **Select Action > Agent Query**.
4. Select an action.
5. Click **Run**.
   
   A dialog box displays to confirm the action has been initiated.

6. Click **OK**.

   Or click **Create rule for similar events** if you want to create a new rule. See **Response Action Rules from the Orchestration Rules Page** for more details.

When the query is complete, the results are visible in events. You can also click the Agent tab in the details of the asset to see the Query History. You can see the name of the query, the date on which the query was run, the status (Query In Progress, Processing Events, and Completed), and, once the query is complete, there is the View Results link. This link goes to the filtered events.

**Note:** The queries generate events when you run them. They do not generate events continuously; you have to run the query again if you want to generate new events.

### To run a user-initiated agent query from the details view of an asset

1. Go to **Environment > Assets**.
2. Search the asset, click the blue chevron icon (▶) located next to the asset name on which you want to run the agent query and select **Full Details**.
3. Select **Actions > Agent Query**.
4. Select the query you want to run.
5. Click **Run**.

   A message displays at the top of the page to inform you the query is in progress. When the query is complete, the results are visible in events. You can also click the Agent tab in the details of the
To see the Query History. You can see the name of the query, the date on which the query was run, the status (Query In Progress, Processing Events, and Completed), and, once the query is complete, there is the View Results link. This link goes to the filtered events.

To run a user-initiated agent query from the Orchestration Rules page

1. Go to Settings > Rules.
2. Select Create Orchestration Rule > Create Response Action Rule.
3. Enter a name for the rule.
4. Select Agent Query as the Action Type.
5. Select the specific asset.
6. Select a query in the Action field.
7. 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:** Keep in mind that 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.

8. (Optional.) Click Add Group of Conditions to group your conditions.

   **Note:** See Operators in the Orchestration Rules for more information.

9. (Optional.) Click the More link to include a multiple occurrence parameter.

   These 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. These are the two options that you can modify:

   - **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 window used to identify a match for multiple occurrences. Enter the number and choose a time-unit value of seconds, minutes, or hours.

   This duration identifies the amount of time that transpires from the first to last. 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.

10. Click **Save Rule**.

The created rule will display in the list of rules.

You can also click the Agent tab in the details of the asset to see the Query History. You can see the name of the query, the date on which the query was run, the status (**Query In Progress**, **Processing Events**, and **Completed**), and, once the query is complete, there is the **View Results** link. This link goes to the filtered events.

The full list of queries available is presented below.

**Available AlienVault Agent Queries**

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Docker container running processes</td>
<td>macOS, Linux</td>
<td>Get the list of processes running in each Docker container.</td>
</tr>
<tr>
<td>Get Docker containers details</td>
<td>macOS, Linux</td>
<td>Get a list of details for each Docker container.</td>
</tr>
<tr>
<td>Get file information</td>
<td>Windows, Linux, and macOS</td>
<td>Get information from the file specified in the first parameter. You must include the file path of the file.</td>
</tr>
<tr>
<td>Get IE typed URLs</td>
<td>Windows</td>
<td>Get the list of Internet Explorer’s entered URLs.</td>
</tr>
<tr>
<td>Get firewall configuration</td>
<td>Windows</td>
<td>List firewall configurations for different profiles and rules.</td>
</tr>
<tr>
<td>Get installed packages history</td>
<td>macOS</td>
<td>Get the list of latest installed packages in the system.</td>
</tr>
</tbody>
</table>
### Available AlienVault Agent Queries (Continued)

<table>
<thead>
<tr>
<th>Query Name</th>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get logged-in users</td>
<td>Windows, Linux, and macOS</td>
<td>List the current logged-in users.</td>
</tr>
<tr>
<td>Get listening processes</td>
<td>Windows, Linux, and macOS</td>
<td>List the processes with listening sockets.</td>
</tr>
<tr>
<td>Get network connections</td>
<td>Windows, Linux, and macOS</td>
<td>List the current network connections.</td>
</tr>
<tr>
<td>Get network connection</td>
<td>Linux</td>
<td>Get information from a network connection based on the remote address (first parameter) and the remote port (second parameter). You must include the port and the IP address.</td>
</tr>
<tr>
<td>Get network shares</td>
<td>Windows</td>
<td>Get the list of network-shared resources from the system.</td>
</tr>
<tr>
<td>Get persistence registry</td>
<td>Windows</td>
<td>Get registry key values commonly used for persistence by attackers.</td>
</tr>
<tr>
<td>Get recent files</td>
<td>Windows</td>
<td>Get the list of recent files.</td>
</tr>
<tr>
<td>Get recent items</td>
<td>macOS</td>
<td>Lists recently opened files.</td>
</tr>
<tr>
<td>Get running processes</td>
<td>Windows, Linux, and macOS</td>
<td>List running processes.</td>
</tr>
<tr>
<td>Get running services</td>
<td>Windows</td>
<td>List running services.</td>
</tr>
<tr>
<td>Get SSH authorized keys</td>
<td>macOS, Linux</td>
<td>Get the list of SSH-authorized keys allowed in the system.</td>
</tr>
<tr>
<td>Get users launched services</td>
<td>macOS</td>
<td>Get the list of LaunchAgents and LaunchDaemons services installed in the system.</td>
</tr>
<tr>
<td>Get Wi-Fi connection status</td>
<td>macOS</td>
<td>Get information from the current Wi-Fi connection.</td>
</tr>
<tr>
<td>Get Wi-Fi preferred connections</td>
<td>macOS</td>
<td>Get information from the preferred Wi-Fi connections.</td>
</tr>
</tbody>
</table>