AT&T Cybersecurity

AT&T Business

USM Anywhere™

Agents Guide

Updated May 18, 2023

Contents

The AlienVault Agent

The AlienVault Agent is a lightweight endpoint agent based on osquery, the leading open-source operating system (OS) instrumentation framework for Microsoft Windows, Apple macOS, and Linux. It enables endpoint detection and monitoring with central management, contributing to complete and effective threat visibility, detection, and compliance.

The AlienVault 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 IDs

The 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. The (OS)se agents use two universally unique identifier (UUID)-formatted IDs to interact with USM Anywhere: a host identifier UUID and an asset identifier UUID. Understanding the two AlienVault Agent IDs is important when you deploy agents in virtual machines (VMs). See AlienVault Agent IDs for more information.

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.

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.

Agent Data Caching

AT&T Cybersecurity has enhanced osquery’s buffered logger to retain data more efficiently if the communication with USM Anywhere fails. Based on the frequency of events being generated on the endpoint, the AlienVault Agent writes those events to batch files. When there is a communication error with USM Anywhere, those files are retained in `osquery3.db/z_cached_logs` within the agent’s working directory. The agent tries resending the files after a back-off period and, at the same time, continues to add more batch files for new events if the communication isn't restored. Under normal conditions, the cache of batch files shouldn't exceed 5 GB of disk space. After the communication is restored, the agent works through the backlog of files in the order of their creation. If the caching limit is reached, the agent issues a warning and stops writing cached data to disk, after which no new events are captured. You may need to remove some or all of the files to allow the agent to capture and cache new events until the communications with USM Anywhere is restored. The amount of time to reach the caching limit depends on the activity on the endpoint and the amount of content in each event.

Agent Updates

When a new agent is registered with your USM Anywhere service, the system checks its version and displays it under the associated asset. You can update the agent manually or use the agent’s auto-update feature, which is disabled by default. Both update methods are performed using the AlienVault Agent script. See the AlienVault Agent updates on the USM Anywhere Product Announcements page to find out the latest agent version and improvement.

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 following table compares some of the most common use cases between the AlienVault Agent and NXLog.

AlienVault Agent vs. NXLog Use Cases

Environmental Demands	Recommended Option
If you need to monitor endpoints outside of the network or in remote locations where it would be impractical to deploy a sensor	AlienVault Agent
If you want the ability to query assets for additional forensic data as part of your investigation activities	AlienVault Agent
If you want the benefits of AT&T Alien Labs actively monitoring endpoints with updated Alien Labs rules, including active process and network activity information	AlienVault Agent
If you a need to restrict off-premise connections for endpoints	NXLog
If you need complete control over agent configuration and filtering rules	NXLog
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	NXLog

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 installing 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, 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 Community Edition (CE) across your Windows hosts to capture events on your end servers and forward them to your USM Anywhere Sensor.
- Use the Windows Event Collector sensor app to manage the NXLog subscription and 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, 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 Microsoft Windows, Linux, or Apple macOS installation for operating system (OS)-specific requirements.

The AlienVault Agent uses osquery. Other endpoint security products may use osquery for similar tasks, perhaps with different paths or file locations. In theory, osquery running under a different process or service name should present no issues, but AT&T Cybersecurity doesn't support installing a second agent that uses osquery. Additionally, it may be necessary to whitelist the service or process that the AlienVault Agent uses in other endpoint security products so that the AlienVault Agent can operate normally. The following table lists the osquery service and process used by the AlienVault Agent and the AlienVault Agent script.

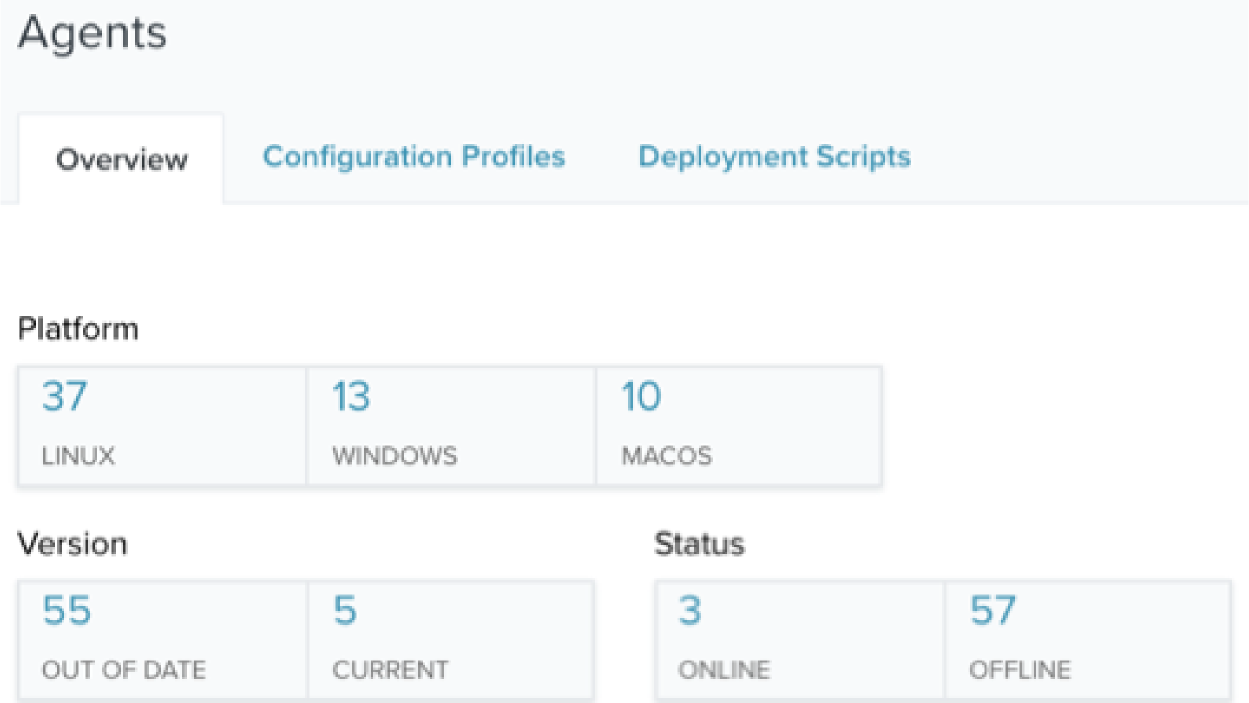
osquery Service and Process Used by the AlienVault Agent

USM Anywhere Component	Platform	osquery Service	osquery Process
AlienVault Agent	Linux	osqueryd	osqueryd
	macOS	osqueryd	osqueryd
	Windows	osqueryd	osqueryd.exe
AlienVault Agent Script	Linux	N/A	osqueryi
	macOS	N/A	osqueryi
	Windows	N/A	osqueryi.exe

Agent Deployment Details

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

Click the displayed numbers to view the agents in the Assets page (Environment > Assets). If there are unassociated agents, this page displays an alert to help you resolve them. See AlienVault Agent and Asset Associations for more information.



Platform

37 LINUX

13 WINDOWS

10 MACOS

Version

55 OUT OF DATE

5 CURRENT

Status

3 ONLINE

57 OFFLINE

AlienVault Agent Installation on Windows Hosts

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

To install the AlienVault Agent on Microsoft Windows, you must run a script that you access from your USM Anywhere environment. When you run the installation script on the 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 in 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 AlienVault Agents on your host systems, you should install just a few to evaluate the events 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 installing the AlienVault Agent on a Windows host system, ensure 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).
- 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.

Note: AT&T Cybersecurity recommends that your host system has a minimum of 4 GB memory and 2 CPU cores.

You must configure your firewall to allow temporary downloads to the host system using the HTTPS application protocol over port 443:

- `download.sysinternals.com/files/Sysmon.zip`

You must configure your firewall to support ongoing event transmission to USM Anywhere.

Standard Firewall Setup

Your firewall needs to be configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `<AWS region>-agent-entrypoint.alienvault.cloud` (for example, `eu-west-1-agent-entrypoint.alienvault.cloud`)

  See the AlienVault Agent Endpoints by AWS Regions table for region-specific IP ranges.
- `agent-packageserver.alienvault.cloud`
- `api.agent.alienvault.cloud`
- `prod-api.agent.alienvault.cloud`
- `agent-packageserver.alienvault.cloud/repo/windows/sysmon_config_schema4_0.xml`
- `agent-packageserver.alienvault.cloud/repo/windows/alienvault-agent-<version>.msi`

Important: The endpoints listed above are inside the 3.235.189.112/28 range.

GovCloud Setup

AT&T Threat Detection and Response for Government (AT&T TDR for Gov) customers need to configure ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `api.agent.gov.alienvault.us`
- `prod-api.agent.gov.alienvault.us`
- `agent-packageserver.gov.alienvault.us/repo/windows/sysmon_config_schema4_0.xml`

- `agent-packageserver.gov.alienvault.us/repo/windows/alienvault-agent-<version>.msi`
- `us-gov-west-1-agent-entrypoint.gov.alienvault.us`

Important: These endpoints are inside the 3.32.190.224/28 range.

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 following table for details. If you are unsure, consult your administrator who set up your USM Anywhere or AT&T TDR for Gov domain.

Note: AT&T Cybersecurity owns the IP ranges listed in the following table. The IP ranges route agent traffic, and connectivity can move within the ranges according to the region.

AlienVault Agent Endpoints by AWS Regions

Region	Endpoint	Reserved Static IP Address Ranges
Asia Pacific (Tokyo)	ap-northeast-1-agent-entrypoint.alienvault.cloud	18.177.156.144/28
Asia Pacific (Mumbai)	ap-south-1-agent-entrypoint.alienvault.cloud	3.7.161.32/28
Asia Pacific (Sydney)	ap-southeast-2-agent-entrypoint.alienvault.cloud	3.25.47.48/28
Canada (Central)	ca-central-1-agent-entrypoint.alienvault.cloud	3.96.2.80/28
EU (Frankfurt)	eu-central-1-agent-entrypoint.alienvault.cloud	18.156.18.32/28
EU (Ireland)	eu-west-1-agent-entrypoint.alienvault.cloud	3.250.207.0/28
EU (London)	eu-west-2-agent-entrypoint.alienvault.cloud	18.130.91.160/28
South America (São Paulo)	sa-east-1-agent-entrypoint.alienvault.cloud	18.230.160.128/28
US East (N. Virginia)	us-east-1-agent-entrypoint.alienvault.cloud	3.235.189.112/28

AlienVault Agent Endpoints by AWS Regions (Continued)

Region	Endpoint	Reserved Static IP Address Ranges
US West (Oregon)	us-west-2-agent-entrypoint.alienvault.cloud	44.234.73.192/28
AWS GovCloud (US-West)	us-gov-west-1-agent-entrypoint.gov.alienvault.us	3.32.190.224/28

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 Agents page (Data Sources > Agents) or from the Asset Details page for the asset.

Note: If the 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.

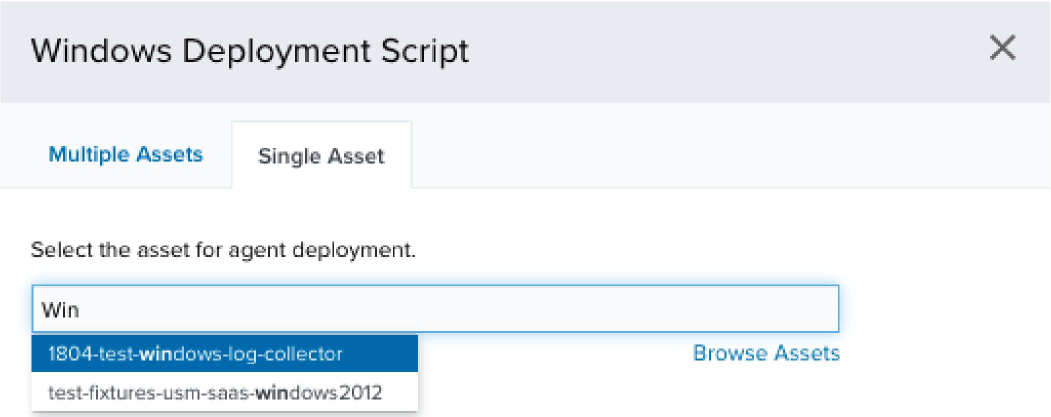
Alternatively, you can use the script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

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 then select the one you want.



Select the asset for agent deployment.

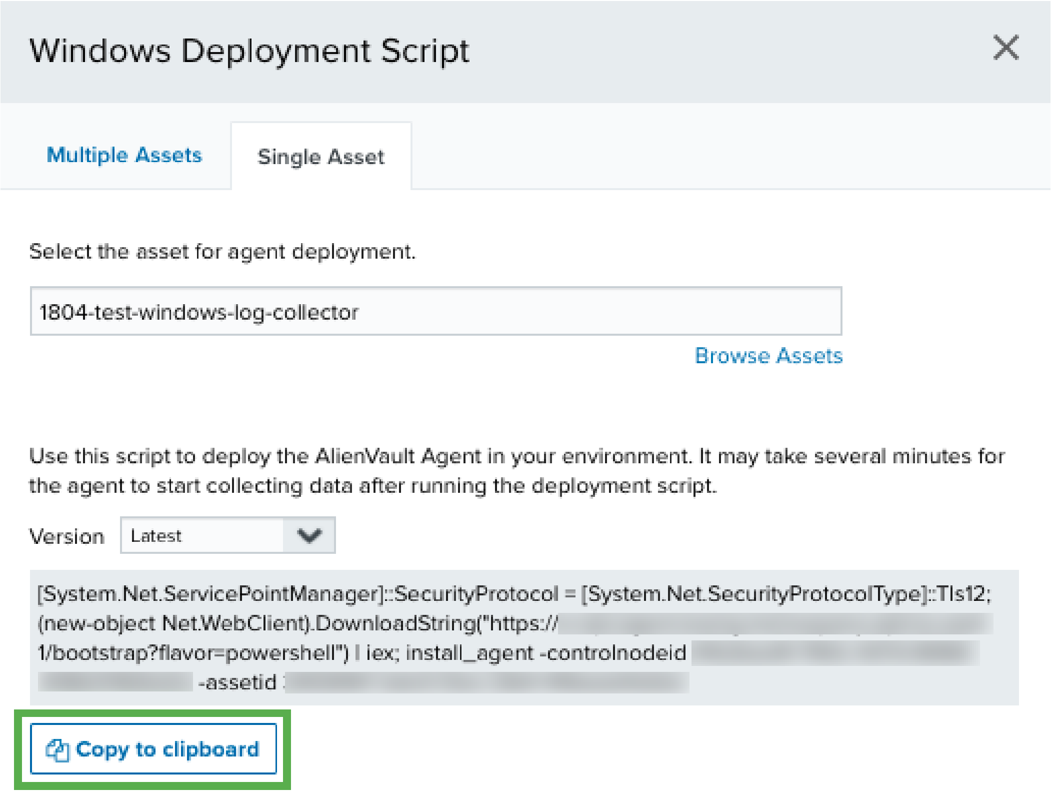
Win

1804-test-windows-log-collector
test-fixtures-usm-saas-windows2012

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

The Windows Deployment Script dialog box opens.

5. Click **Copy to clipboard**.



Select the asset for agent deployment.

1804-test-windows-log-collector

Use this script to deploy the AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

Version: Latest

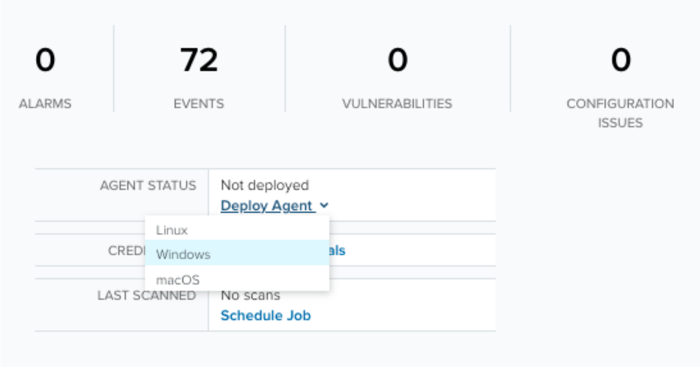
```
[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;
(new-object Net.WebClient).DownloadString("https://[redacted]
1/bootstrap?flavor=powershell") | iex; install_agent -controlnodeid [redacted]
[redacted] -assetid [redacted]
```

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



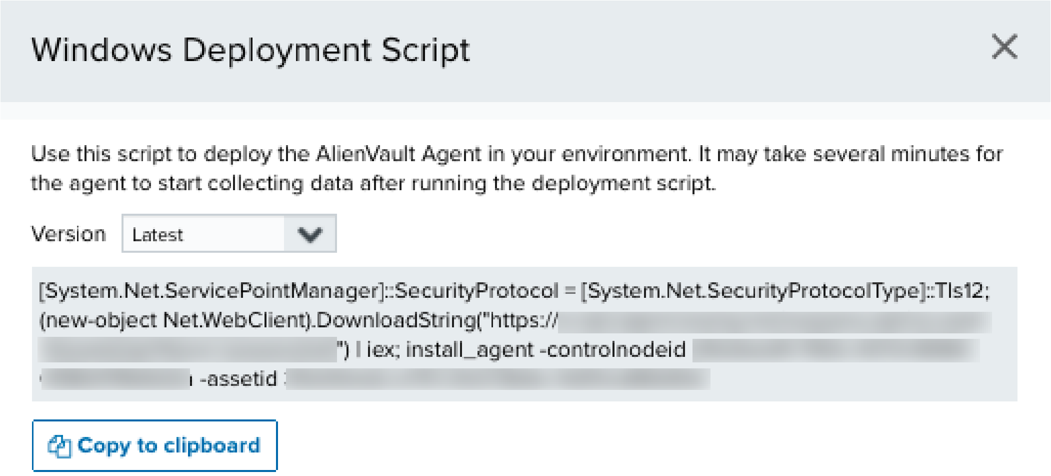
0	72	0	0
ALARMS	EVENTS	VULNERABILITIES	CONFIGURATION ISSUES

AGENT STATUS	Not deployed Deploy Agent ⌄
CREDI	als
LAST SCANNED	No scans Schedule Job

5. Select **Windows**.

   The Windows Deployment Script dialog box opens.

6. Click **Copy to clipboard**.



Windows Deployment Script ✕

Use this script to deploy the AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

Version: Latest ⌄

```
[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;
(new-object Net.WebClient).DownloadString("https://[redacted]
[redacted]") | iex; install_agent -controlnodeid [redacted]
[redacted] -assetid [redacted]
```

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

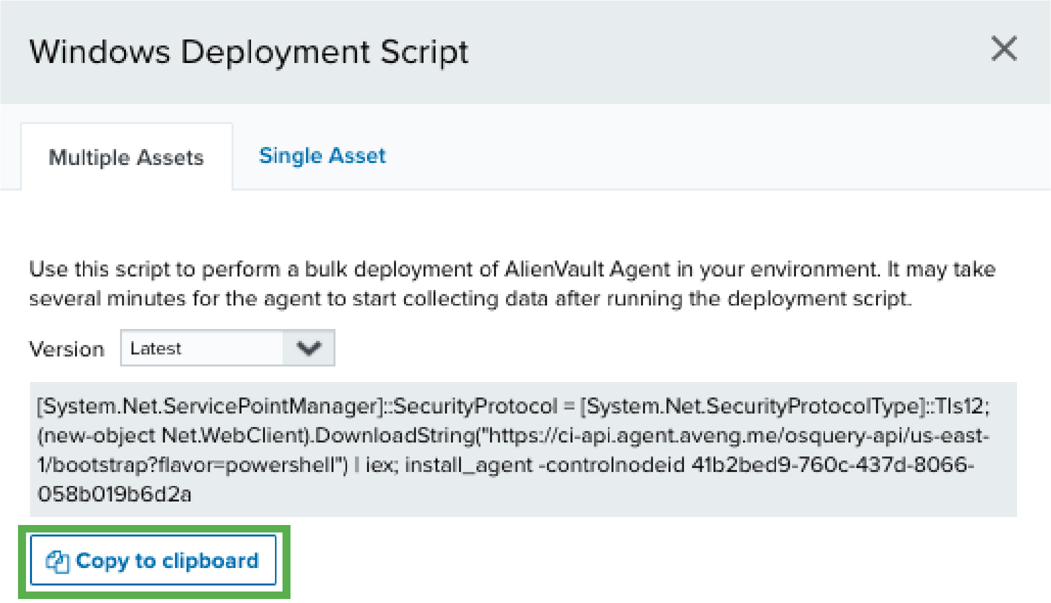
AlienVault Agent Installation on Multiple Host Systems

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 (Data Sources > Agents).

To generate an agent deployment script for multiple host systems

1. In USM Anywhere, go to **Data Sources > Agents**.
2. Click **Windows Deployment Script**.

   Ensure that the **Multiple Assets** tab is selected in the dialog box.
3. Click **Copy to clipboard**.



Use this script to perform a bulk deployment of AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

Version: Latest

```
[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;
(new-object Net.WebClient).DownloadString("https://ci-api.agent.aveng.me/osquery-api/us-east-1/bootstrap?flavor=powershell") | iex; install_agent -controlnodeid 41b2bed9-760c-437d-8066-058b019b6d2a
```

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.

Note: If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script will 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. When a deployed agent does not have an associated asset, you must manually make this association in USM Anywhere to enable queries and log collection for the host system. See AlienVault Agent and Asset Associations for more information.

Installation Error Resolution

If the AlienVault Agent is installed using the single asset deployment script, its host identifier UUID and asset association is 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 the agent associates with the asset if you need to reinstall the agent for any reason.

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

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 Script and Agent Updates for more information on the agent command script, including the file location and a list of the commands.

AlienVault Agent Installation on Linux Hosts

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

To install the AlienVault Agent on Linux, 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 (FIM).

You can generate a script that is specific to a selected asset in 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 operating system (OS). Dependent libraries for 32-bit OS are not available.

Note: When you first deploy AlienVault Agents on your host systems, you should install just a few to evaluate the events 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.

Important: Before installing the Linux AlienVault Agent, you should confirm that auditd is disabled on the targeted endpoint and is not configured to start at boot. This is because the agent uses *syscalls* to the kernel's audit system to generate process events, which are then used in certain detection rules and queries. Official osquery documentation states that auditd should not be running when osquery is configured to use these syscalls because it can create a conflict with the osquery service over access to the audit Netlink socket.

Prerequisites

Before installing the AlienVault Agent on a Linux host system, ensure that you have the prerequisites in place for that system.

- The 64-bit Linux host system runs 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.

- Transport Layer Security (TLS) 1.2 must be enabled on the host system.
- 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.

Note: AT&T Cybersecurity recommends that your host system has a minimum of 4 GB memory and 2 CPU cores.

You must configure your firewall to support ongoing event transmission to USM Anywhere.

Standard Firewall Setup

Your firewall needs to be configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `<AWS region>-agent-entrypoint.alienvault.cloud` (for example, `eu-west-1-agent-entrypoint.alienvault.cloud`)

  See the AlienVault Agent Endpoints by AWS Regions table for region-specific IP ranges.

- `agent-packageserver.alienvault.cloud`
- `api.agent.alienvault.cloud`
- `prod-api.agent.alienvault.cloud`
- The package repo content is located in `agent-packageserver.alienvault.cloud/repo/deb/` or `agent-packageserver.alienvault.cloud/repo/rpm/`

Important: The endpoints listed above are inside the 3.235.189.112/28 range.

GovCloud Setup

AT&T Threat Detection and Response for Government (AT&T TDR for Gov) customers need to configure ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `api.agent.gov.alienvault.us`
- `prod-api.agent.gov.alienvault.us`
- The package repo content is located in `agent-packageserver.gov.alienvault.us/repo/deb/` or `agent-packageserver.gov.alienvault.us/repo/rpm/`
- `us-gov-west-1-agent-entrypoint.gov.alienvault.us`

Important: These endpoints are inside the 3.32.190.224/28 range.

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 following table for details. If you are unsure, consult your administrator who set up your USM Anywhere or AT&T TDR for Gov domain.

Note: AT&T Cybersecurity owns the IP ranges listed in the following table. The IP ranges route agent traffic, and connectivity can move within the ranges according to the region.

AlienVault Agent Endpoints by AWS Regions

Region	Endpoint	Reserved Static IP Address Ranges
Asia Pacific (Tokyo)	ap-northeast-1-agent-entrypoint.alienvault.cloud	18.177.156.144/28
Asia Pacific (Mumbai)	ap-south-1-agent-entrypoint.alienvault.cloud	3.7.161.32/28
Asia Pacific (Sydney)	ap-southeast-2-agent-entrypoint.alienvault.cloud	3.25.47.48/28
Canada (Central)	ca-central-1-agent-entrypoint.alienvault.cloud	3.96.2.80/28

AlienVault Agent Endpoints by AWS Regions (Continued)

Region	Endpoint	Reserved Static IP Address Ranges
EU (Frankfurt)	eu-central-1-agent-entrypoint.alienvault.cloud	18.156.18.32/28
EU (Ireland)	eu-west-1-agent-entrypoint.alienvault.cloud	3.250.207.0/28
EU (London)	eu-west-2-agent-entrypoint.alienvault.cloud	18.130.91.160/28
South America (São Paulo)	sa-east-1-agent-entrypoint.alienvault.cloud	18.230.160.128/28
US East (N. Virginia)	us-east-1-agent-entrypoint.alienvault.cloud	3.235.189.112/28
US West (Oregon)	us-west-2-agent-entrypoint.alienvault.cloud	44.234.73.192/28
AWS GovCloud (US-West)	us-gov-west-1-agent-entrypoint.gov.alienvault.us	3.32.190.224/28

AlienVault Agent 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 (Data Sources > Agents) or from the Asset Details page for the asset.

Note: If the 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.

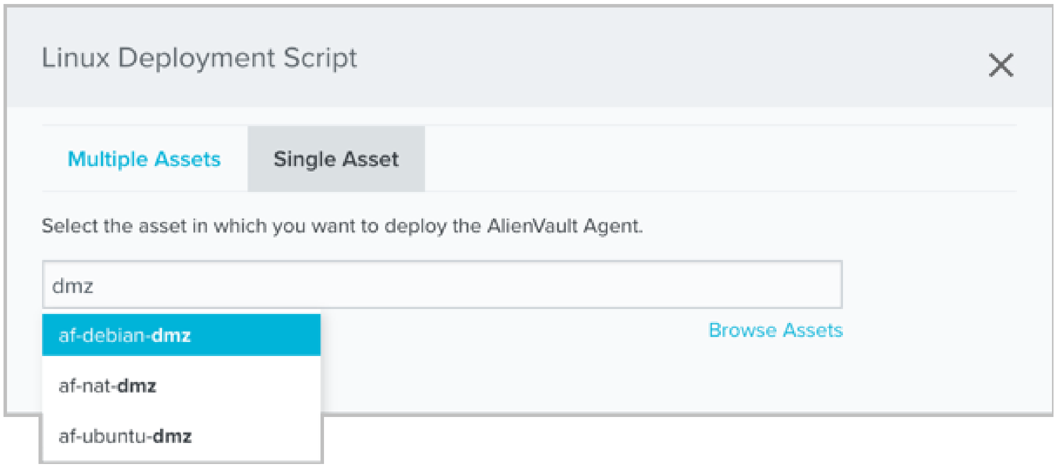
Alternatively, you can use the script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

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.

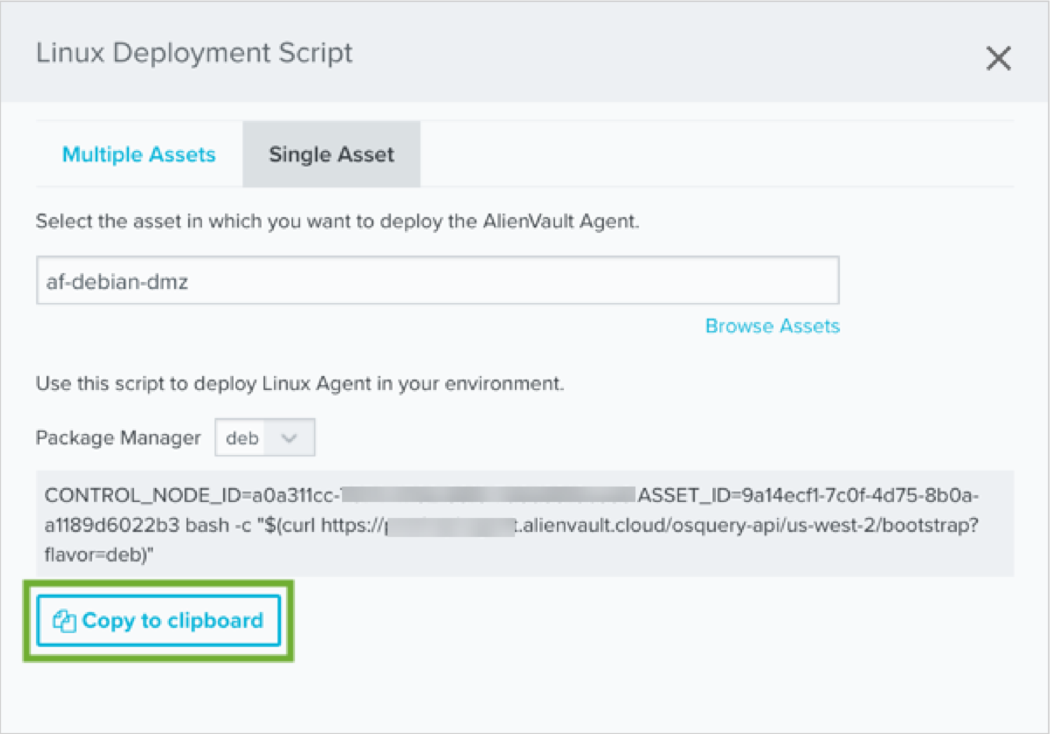
   Linux Deployment Script

   Select the asset in which you want to deploy the AlienVault Agent.

   dmz

   Or you can click the **Browse Assets** link to open the Select Asset dialog box and then 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**.



Linux Deployment Script

Select the asset in which you want to deploy the AlienVault Agent.

af-debian-dmz

Use this script to deploy Linux Agent in your environment.

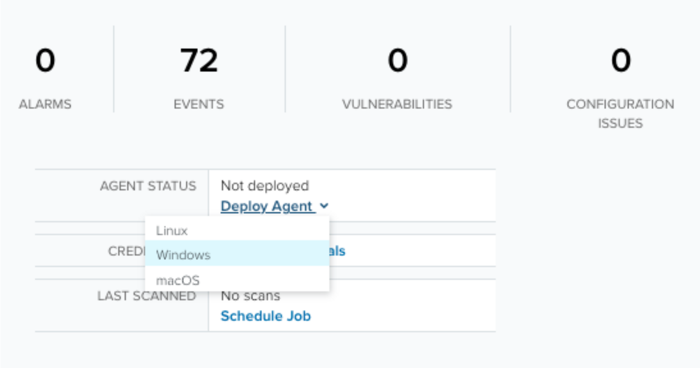
Package Manager: deb

```
CONTROL_NODE_ID=a0a311cc-[redacted]ASSET_ID=9a14ecf1-7c0f-4d75-8b0a-
a1189d6022b3 bash -c "$(curl https://[redacted].alienvault.cloud/osquery-api/us-west-2/bootstrap?
flavor=deb)"
```

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



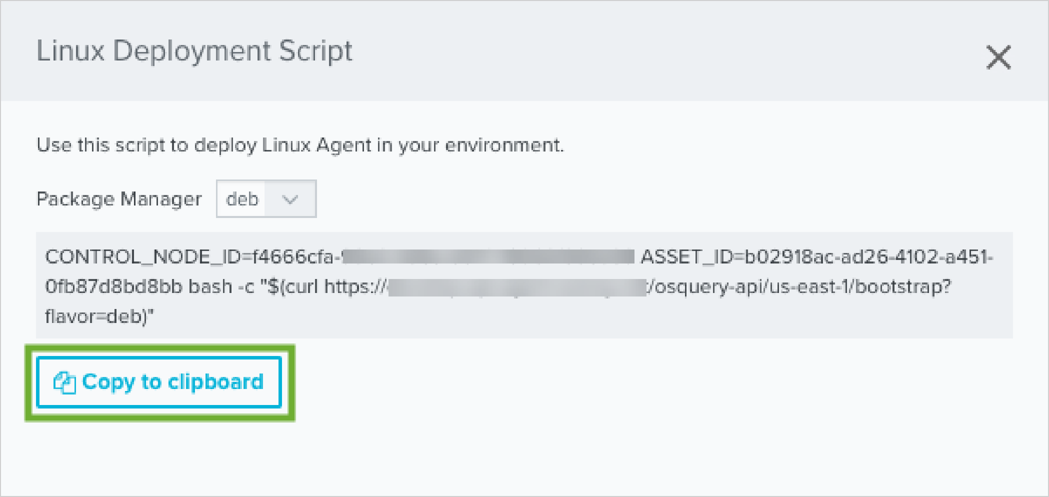
0	72	0	0
ALARMS	EVENTS	VULNERABILITIES	CONFIGURATION ISSUES

AGENT STATUS	Not deployed Deploy Agent ⌄
CREDI	als
LAST SCANNED	No scans Schedule Job

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**.

   Linux Deployment Script

   Use this script to deploy Linux Agent in your environment.

   Package Manager: deb

   ```
   CONTROL_NODE_ID=f4666cfa-[redacted] ASSET_ID=b02918ac-ad26-4102-a451-
   0fb87d8bd8bb bash -c "$(curl https://[redacted]/osquery-api/us-east-1/bootstrap?
   flavor=deb)"
   ```

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 (Data Sources > Agents).

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**.

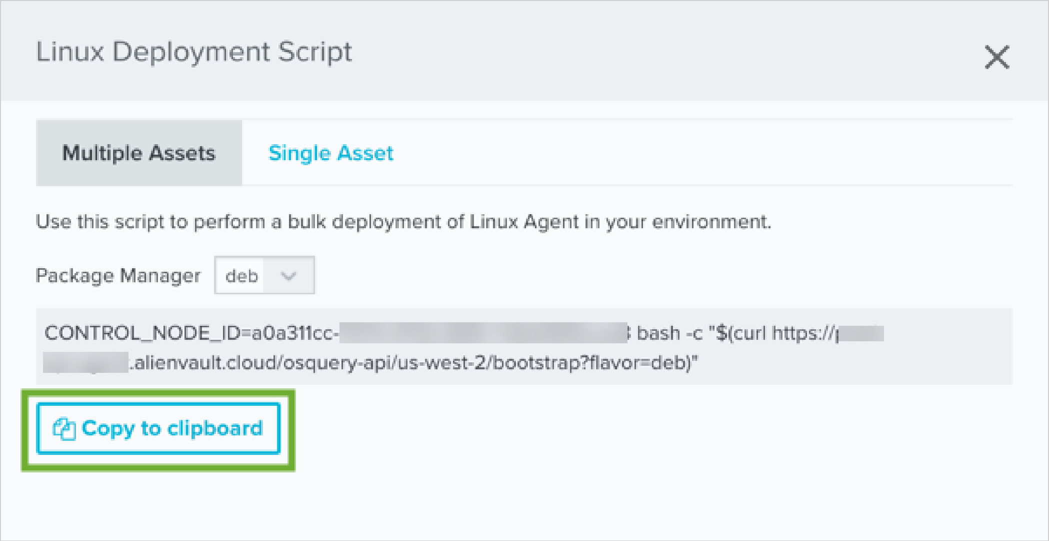
2. Click **Linux Deployment Script**.

   Ensure that the **Multiple Assets** tab is selected in the dialog box.

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**.



Use this script to perform a bulk deployment of Linux Agent in your environment.

Package Manager: deb

```
CONTROL_NODE_ID=a0a311cc-[redacted] bash -c "$(curl https://[redacted]
[redacted].alienvault.cloud/osquery-api/us-west-2/bootstrap?flavor=deb)"
```

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.

Note: If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script will 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. When a deployed agent does not have an associated asset, you must manually make this association in USM Anywhere to enable queries and log collection for the host system. See AlienVault Agent and Asset Associations for more information.

Installation Error Resolution

If the AlienVault Agent is installed using the single asset deployment script, its host identifier UUID and asset association is 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 the agent associates with the asset if you need to reinstall the agent for any reason.

If you encounter an error during the 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.

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 AlienVault Agent Script and Agent Updates for more information on the agent command script, including the file location and a list of the commands.

AlienVault Agent Installation on macOS Hosts

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

To install the AlienVault Agent on macOS, 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 (FIM).

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

Note: When you first deploy AlienVault Agents on your host systems, you should install just a few to evaluate the events 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 installing the AlienVault Agent on a macOS host system, ensure that these prerequisites are met:

- You are running macOS Sierra 10.12 or later.
- You have login credentials for the host system with sudo privileges.
- Transport Layer Security (TLS) 1.2 must be enabled on the host system

Note: AT&T Cybersecurity recommends that your host system has a minimum of 4 GB memory and 2 CPU cores.

You must configure your firewall to support ongoing event transmission to USM Anywhere.

Standard Firewall Setup

Your firewall needs to be configured to allow ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `<AWS region>-agent-entrypoint.alienvault.cloud` (for example, `eu-west-1-agent-entrypoint.alienvault.cloud`)

  See the AlienVault Agent Endpoints by AWS Regions table for region-specific IP ranges.
- `agent-packageserver.alienvault.cloud`
- `api.agent.alienvault.cloud`
- `prod-api.agent.alienvault.cloud`
- `agent-packageserver.alienvault.cloud/repo/osx/alienvault-agent-<version>.pkg`

Important: The endpoints listed above are inside the 3.235.189.112/28 range.

GovCloud Setup

AT&T Threat Detection and Response for Government (AT&T TDR for Gov) customers need to configure ongoing outbound connectivity from the host system using the HTTPS application protocol over port 443 to these USM Anywhere endpoints:

- `api.agent.gov.alienvault.us`
- `prod-api.agent.gov.alienvault.us`
- `agent-packageserver.gov.alienvault.us/repo/osx/alienvault-agent-<version>.pkg`
- `us-gov-west-1-agent-entrypoint.gov.alienvault.us`

Important: These endpoints are inside the 3.32.190.224/28 range.

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 following table for details. If you are unsure, consult your administrator who set up your USM Anywhere or AT&T TDR for Gov domain.

Note: AT&T Cybersecurity owns the IP ranges listed in the following table. The IP ranges route agent traffic, and connectivity can move within the ranges according to the region.

AlienVault Agent Endpoints by AWS Regions

Region	Endpoint	Reserved Static IP Address Ranges
Asia Pacific (Tokyo)	ap-northeast-1-agent-entrypoint.alienvault.cloud	18.177.156.144/28
Asia Pacific (Mumbai)	ap-south-1-agent-entrypoint.alienvault.cloud	3.7.161.32/28
Asia Pacific (Sydney)	ap-southeast-2-agent-entrypoint.alienvault.cloud	3.25.47.48/28
Canada (Central)	ca-central-1-agent-entrypoint.alienvault.cloud	3.96.2.80/28
EU (Frankfurt)	eu-central-1-agent-entrypoint.alienvault.cloud	18.156.18.32/28
EU (Ireland)	eu-west-1-agent-entrypoint.alienvault.cloud	3.250.207.0/28
EU (London)	eu-west-2-agent-entrypoint.alienvault.cloud	18.130.91.160/28
South America (São Paulo)	sa-east-1-agent-entrypoint.alienvault.cloud	18.230.160.128/28

AlienVault Agent Endpoints by AWS Regions (Continued)

Region	Endpoint	Reserved Static IP Address Ranges
US East (N. Virginia)	us-east-1-agent-entrypoint.alienvault.cloud	3.235.189.112/28
US West (Oregon)	us-west-2-agent-entrypoint.alienvault.cloud	44.234.73.192/28
AWS GovCloud (US-West)	us-gov-west-1-agent-entrypoint.gov.alienvault.us	3.32.190.224/28

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 (Data Sources > Agents) or from the Asset Details page for the asset.

Note: If the 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.

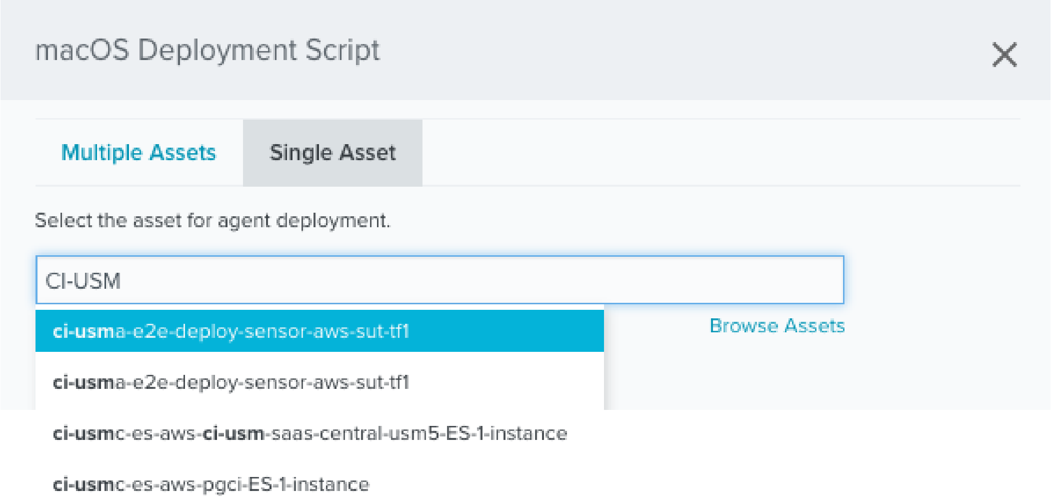
Alternatively, you can use the script for multiple assets and then use the information provided by the unassociated agent to create a new asset.

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 then select the one you want.



Select the asset for agent deployment.

ci-usma-e2e-deploy-sensor-aws-sut-tf1

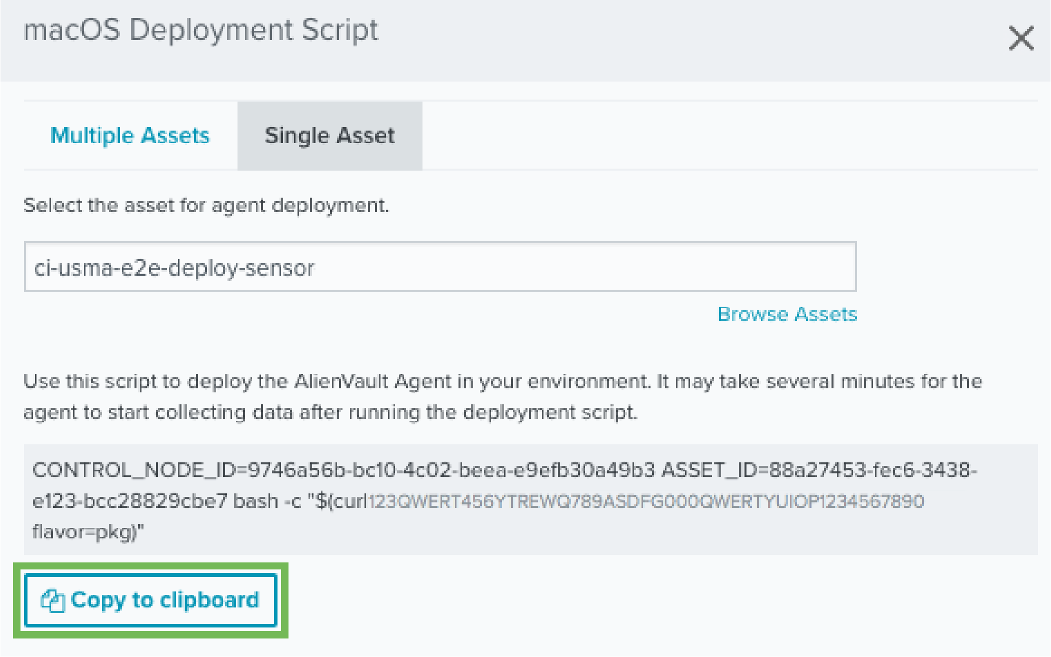
ci-usma-e2e-deploy-sensor-aws-sut-tf1

ci-usmc-es-aws-ci-usm-saas-central-usm5-ES-1-instance

ci-usmc-es-aws-pgci-ES-1-instance

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

5. Click **Copy to clipboard**.



Select the asset for agent deployment.

Use this script to deploy the AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

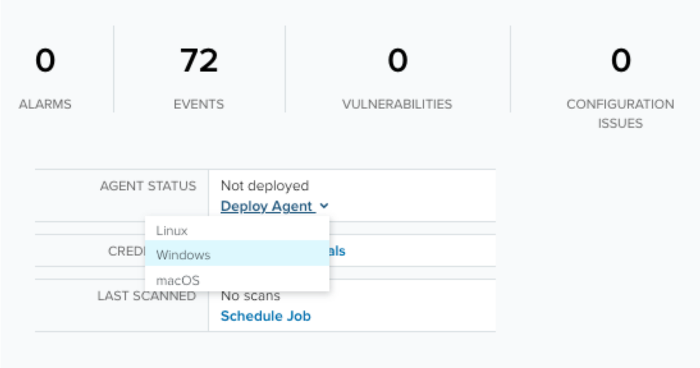
```
CONTROL_NODE_ID=9746a56b-bc10-4c02-beea-e9efb30a49b3 ASSET_ID=88a27453-fec6-3438-
e123-bcc28829cbe7 bash -c "$(curl123QWERT456YTREWQ789ASDFG000QWERTYUIOP1234567890
flavor=pkg)"
```

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

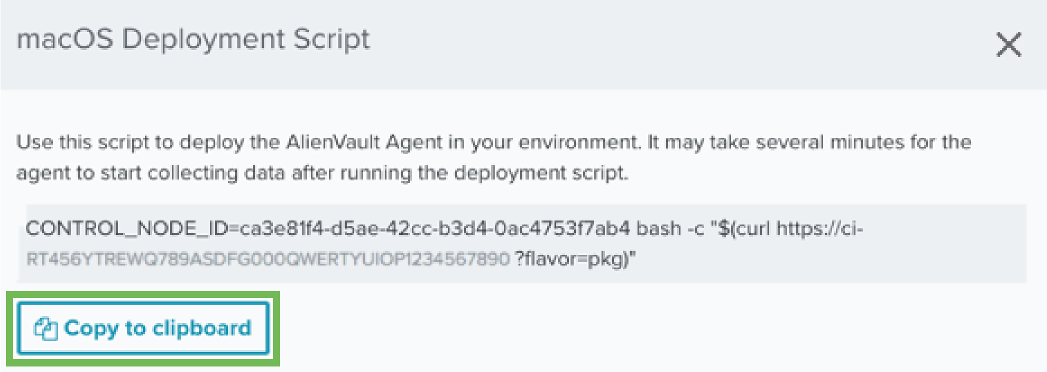
7. Open the Terminal and enter a sudo command containing the script you copied to the clipboard.

From the Asset Details page

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



5. Click **Copy to clipboard**.



Use this script to deploy the AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

```
CONTROL_NODE_ID=ca3e81f4-d5ae-42cc-b3d4-0ac4753f7ab4 bash -c "$(curl https://ci-
RT456YTREWQ789ASDFG000QWERTYUIOP1234567890 ?flavor=pkg)"
```

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 (Data Sources > Agents).

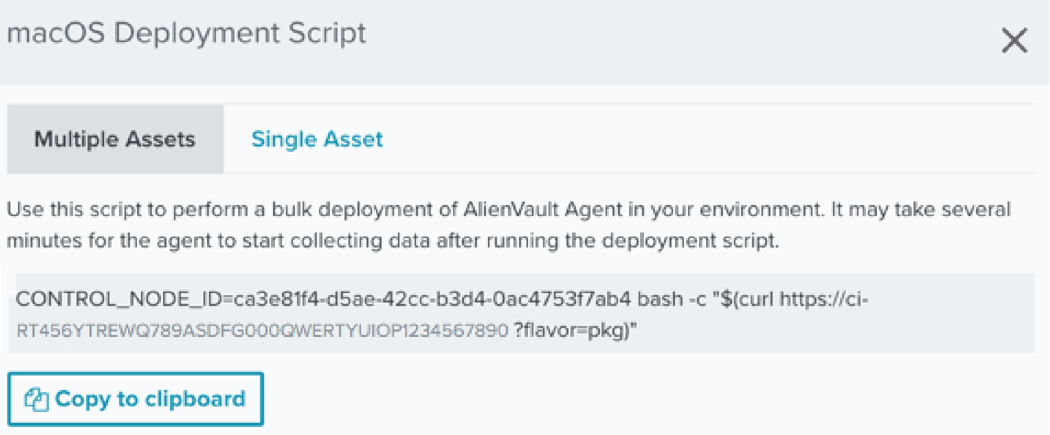
After you use the script to deploy the agent on your macOS host systems, you can view the list of unassigned agents and then associate each agent with an existing asset or add a new asset using the information provided by the agent.

To generate an agent deployment script for multiple host systems

1. In USM Anywhere, go to **Data Sources > Agents**.
2. Click **macOS Deployment Script**.

   Ensure that the **Multiple Assets** tab is selected in the dialog box.
3. Select the **Package Manager** type for the macOS distribution.

   Click **Copy to clipboard**.

   Use this script to perform a bulk deployment of AlienVault Agent in your environment. It may take several minutes for the agent to start collecting data after running the deployment script.

   ```
   CONTROL_NODE_ID=ca3e81f4-d5ae-42cc-b3d4-0ac4753f7ab4 bash -c "$(curl https://ci-
   RT456YTREWQ789ASDFG000QWERTYUIOP1234567890 ?flavor=pkg)"
   ```

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

Note: If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the script will 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. When a deployed agent does not have an associated asset, you must manually make this association in USM Anywhere to enable queries and log collection for the host system. See AlienVault Agent and Asset Associations for more information.

Installation Error Resolution

If the AlienVault Agent is installed using the single asset deployment script, its host identifier UUID and asset association is 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 the agent associates with the asset if you need to reinstall the agent for any reason.

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

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 AlienVault Agent Script and Agent Updates for more information on the agent command script, including the file location and a list of the commands.

AlienVault Agent IDs

The AlienVault Agent uses two universally unique identifier (UUID)-formatted IDs to interact with the USM Anywhere infrastructure: a *host identifier UUID* and an *asset identifier UUID*.

The host identifier UUID, `hostIdentifier`, signifies a specific agent installation. This UUID is generated in one of two ways:

- If you deploy the agent with the single asset deployment script, then you must choose which existing asset the deployment can be associated with or create the asset on the fly. This appends the install command with the `-assetid` flag followed by a pre-determined ID. The pre-determined ID is the asset ID of the associated asset.
- If you deploy the agent with the multiple assets deployment script, then the installation process generates a random host identifier, which starts with a block of 8 zeros (`00000000-`).

The agent's host identifier UUID is stored under the `--specified_identifier` flag in the `osquery.flags` file, which is located in the following directories on the endpoint:

- **Microsoft Windows:** `C:\Program Files\osquery\osquery.flags`
- **Linux:** `/etc/osquery/osquery.flags`
- **Apple macOS:** `/var/osquery/osquery.flags`

The second ID used by the agent is the asset identifier UUID, `souce_asset_id`, which is generated by USM Anywhere whenever an asset is created. USM Anywhere uses this ID to associate events with an asset. The agent does not store its asset identifier UUID; instead, it is provided in its designated AlienVault Agent Configuration Profiles, which is served over Transport Layer Security (TLS) to the agents as they run.

Note: Once associated with an asset, the agent reports both its host identifier UUID and asset identifier UUID to USM Anywhere through events, providing USM Anywhere a means of correlating those events to an asset. If the agent has been deployed with the single asset deployment script, the host identifier UUID and asset identifier UUID should match.

AlienVault Agent ID Usage

When USM Anywhere receives an event from the AlienVault Agent, it looks for the asset ID in the metadata of the event. If the asset ID belongs to a valid and existing asset, USM Anywhere will correlate that event to the asset using that asset ID. If the agent has not been associated with an asset or the asset ID is not recognized, USM Anywhere will identify the agent as unassociated or “orphan”, on the Data Sources > Agents page. See AlienVault Agent and Asset Associations for more information on associating assets with the agents.

If you install the agents using the single asset deployment script, the agents are automatically associated with their designated assets. When the agent is updated, the installation process detects the presence of an existing `osquery.flags` file and uses its `--specified_identifier` flag to identify the agent, thus maintaining its continuity. However, if you run the single asset deployment script on a host that already has an AlienVault Agent installed, the deployment script will overwrite the `-controlnodeid` and `-assetid` flags found on the host system.

Agent Deployments in Virtual Environments

Understanding the two AlienVault Agent IDs detailed previously is important when you deploy agents in virtual machines (VMs), especially when deploying the same image to multiple VMs. Consider the following use cases:

- If the VM can be identified by the same host identifier UUID every time it starts up, then you can install the agent and snapshot the image containing the installation’s host identifier UUID in the `osquery.flags` file.

  > **Note:** If the image is reverted to that snapshot, or applied to another machine, the same host identifier UUID will be used on each machine, and all events reported by these instances of the agent will be associated with the same asset in USM Anywhere.

- If you require that every instance of the VM carries a host identifier UUID to be discernible from another instance of the same VM, then you need to set up a scheduled task to run the multiple asset deployment script at the first start-up so that a unique host identifier UUID is generated during installation.
- If you are building a template, or *golden image*, to be distributed to individual systems that need to be uniquely identifiable, then you should also set up a scheduled task to run the multiple assets deployment script at the first start-up so that a unique host identifier UUID is generated during installation.

In the last two use cases, each agent will be designated as unassociated by USM Anywhere because their events will contain no asset identifier information. Agents installed this way must be associated with a new or existing asset after installation. You only need to do it once per instance, and they can be done in bulk if creating new assets from the agent's associations page. See AlienVault Agent and Asset Associations for more information.

Warning: If multiple VMs carry the same host identifier UUID and are associated with the same asset in USM Anywhere, you may see some strange behaviors. For example:

- The asset changes its name from time to time.
- The agent's heartbeat events appear more frequently than every 10 minutes.
- The asset has alarms that are false positive because not all events aggregated under this asset originated from the same endpoint.

AlienVault Agent and Asset Associations

Role Availability	✗ Read-Only	✗ Analyst	✓ Manager

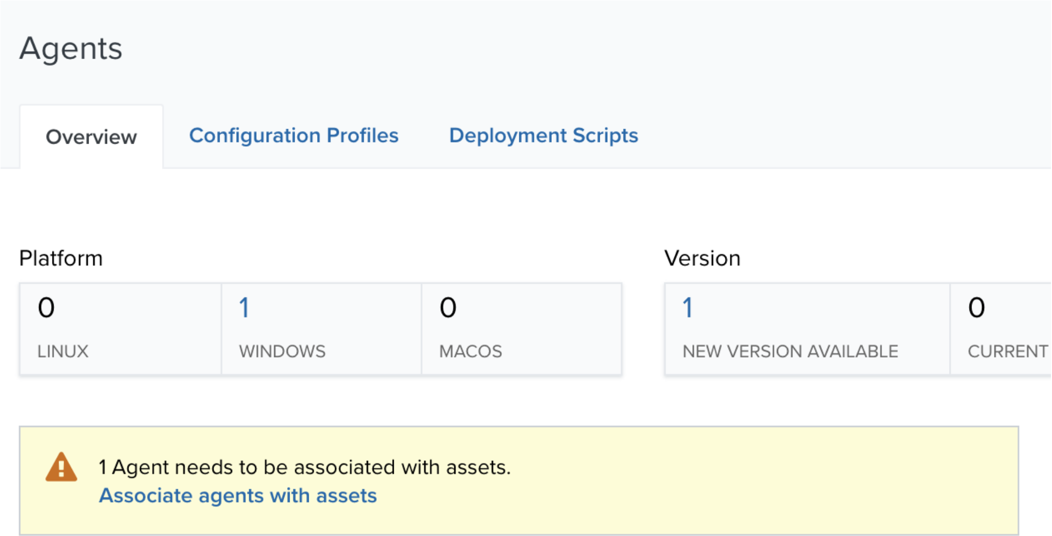
If you use a single asset installation script, the USM Anywhere asset universally unique identifier (UUID) for the selected asset is incorporated into that script. During the installation process, the deployed AlienVault Agent registers with your USM Anywhere instance, makes the asset association, and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

If you use a multiple asset installation script to execute bulk deployment across multiple host systems, the resulting installation will create a random UUID for the agent installation (see AlienVault Agent IDs for more information on UUIDs). For Linux hosts, USM Anywhere attempts to associate the agent with an existing asset based on Amazon Elastic Compute Cloud (EC2) instance metadata gathered from the endpoint. Before installing the agent on a Linux host, AT&T Cybersecurity recommends that you perform an asset scan. This way, USM Anywhere will have identified the asset and, therefore, can automatically associate the asset with the agent. For Linux agents not running on EC2 instances, or any Microsoft Windows or Apple macOS agents, the agent must be associated to an existing or new asset through the Associate Agents With Assets page before you use the multiple asset installation script.

After successfully deploying the agent on a host, it sends heartbeat events every 10 minutes 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 ID if available.

> 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.

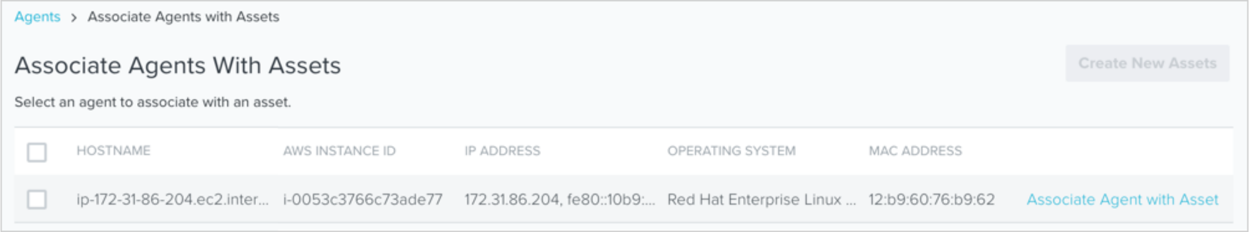
When a deployed agent does not have an associated asset, you must make this association in USM Anywhere to enable queries and log collection for the host system. The Agents page (Data Sources > Agents) displays an alert when there are one or more unassociated assets, and provides tools designed to help 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.



Platform			Version	
0	1	0	1	0
LINUX	WINDOWS	MACOS	NEW VERSION AVAILABLE	CURRENT

1 Agent needs to be associated with assets.
Associate agents with assets

When you see this alert, click **Associate agents with assets** to open the Associate Agents With Assets page and complete the association.



Associate Agents With Assets

Select an agent to associate with an asset.

□	HOSTNAME	AWS INSTANCE ID	IP ADDRESS	OPERATING SYSTEM	MAC ADDRESS	
□	ip-172-31-86-204.ec2.inter...	i-0053c3766c73ade77	172.31.86.204, fe80::10b9:...	Red Hat Enterprise Linux ...	12:b9:60:76:b9:62	Associate Agent with Asset

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.

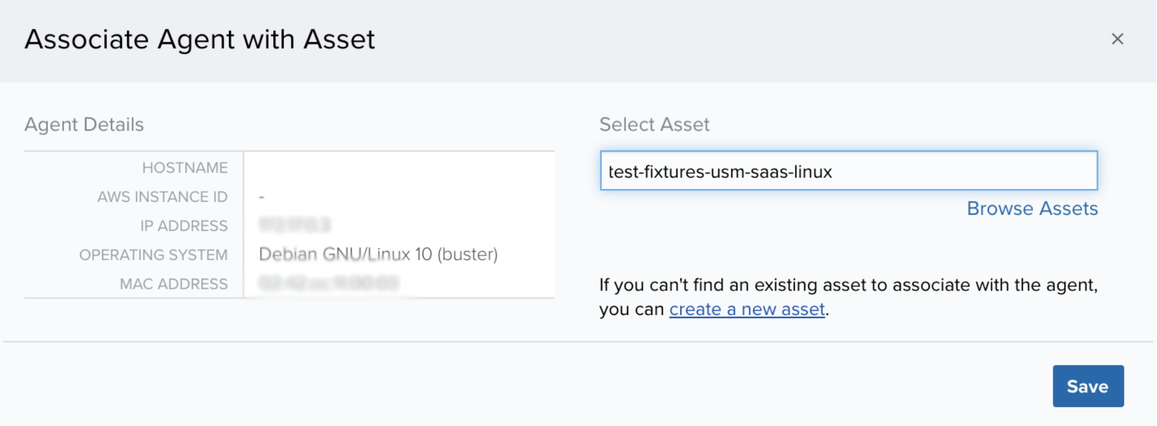
To make an association to an existing asset

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.

     Associate Agent with Asset ×

     Agent Details

HOSTNAME	
AWS INSTANCE ID	-
IP ADDRESS	[redacted]
OPERATING SYSTEM	Debian GNU/Linux 10 (buster)
MAC ADDRESS	[redacted]

     Select Asset

     test-fixtures-usm-saas-linux

     Browse Assets

     If you can't find an existing asset to associate with the agent, you can create a new asset.

     Save

     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 is 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**.

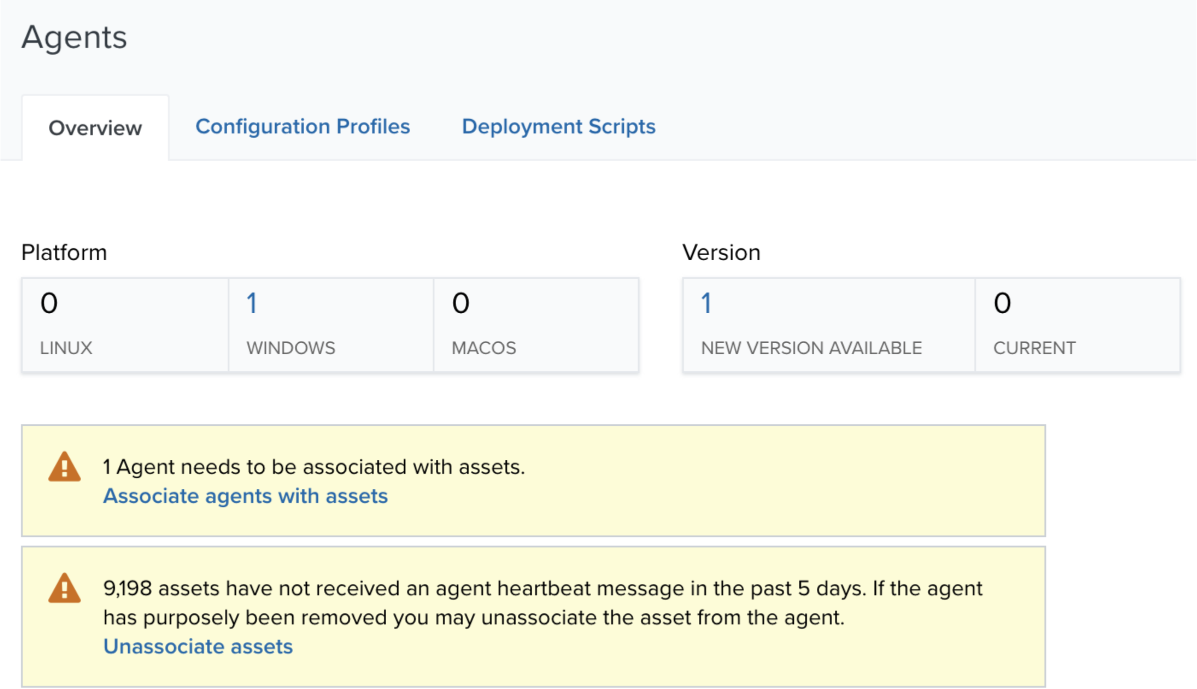
   A confirmation dialog box opens.

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**.



1 Agent needs to be associated with assets.
Associate agents with assets

9,198 assets have not received an agent heartbeat message in the past 5 days. If the agent has purposely been removed you may unassociate the asset from the agent.
Unassociate assets

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

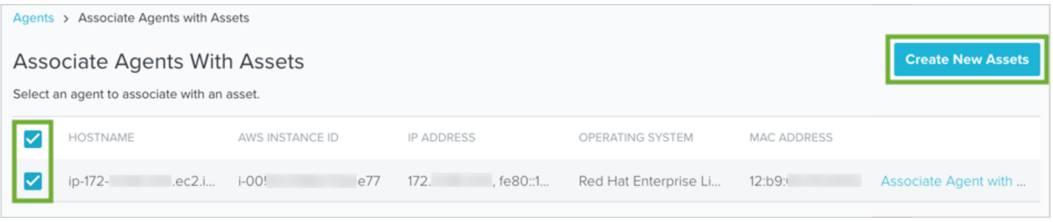
If the asset does not yet exist in the USM Anywhere asset inventory, you can automatically create an asset for one or more selected AlienVault Agents. When USM Anywhere creates a new asset for the agent, it uses the hostname value for the asset name. After creation, you can modify various asset details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

   Agents > Associate Agents with Assets

   Associate Agents With Assets

   Select an agent to associate with an asset.

   Create New Assets

☑	HOSTNAME	AWS INSTANCE ID	IP ADDRESS	OPERATING SYSTEM	MAC ADDRESS	
☑	ip-172-[redacted].ec2.i...	i-00[redacted]e77	172.[redacted], fe80::1...	Red Hat Enterprise Li...	12:b9:[redacted]	Associate Agent with ...

   A confirmation dialog box opens.

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

AlienVault Agent Configuration Profiles

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

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 filtering certain events that are not correlated with alarms.
    - 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.
  - Collects Sysmon Windows Event Log and correlates for threat detection purposes, but stores them only when they are associated with an alarm.

  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 **Full** 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 and stores all macOS 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.

In the Configuration Profiles view, you can click the individual profile name to display the queries executed by the agent and their frequencies. If you are looking for a specific type of log, 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.

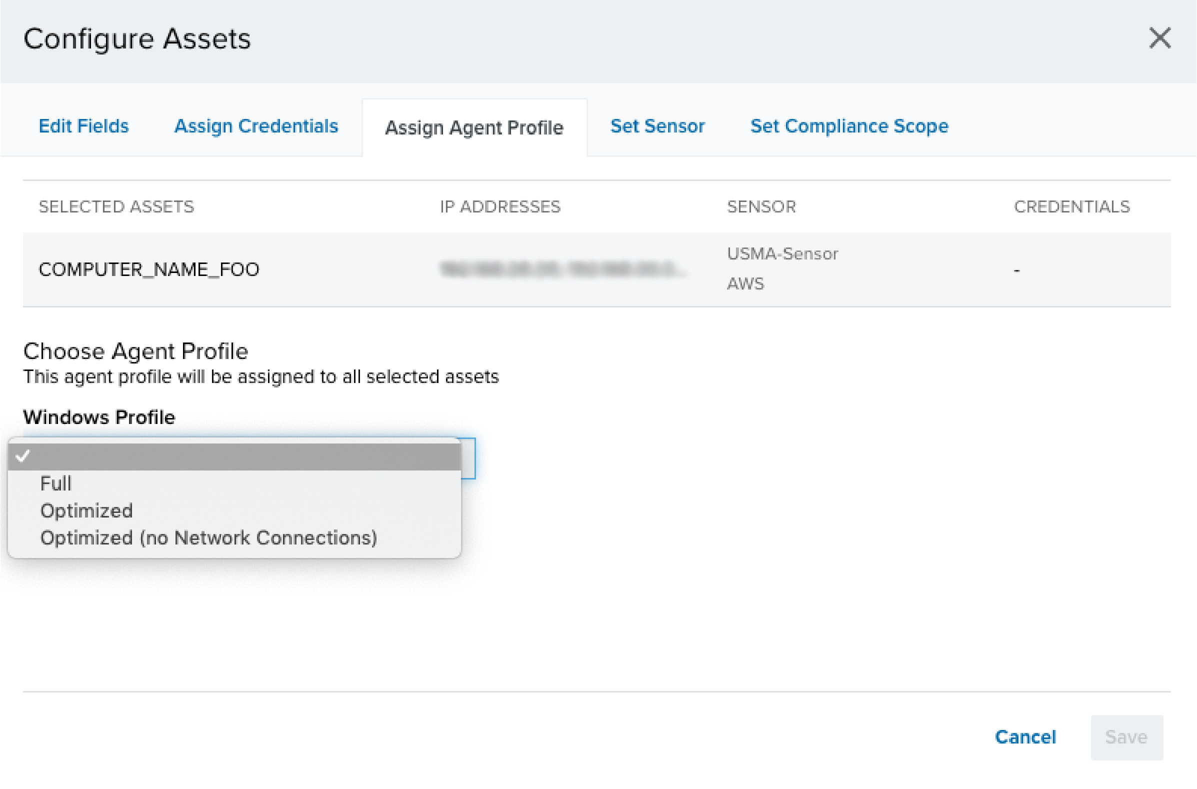
   Important: The Experimental Profiles are temporary and internal. Do not use them unless you have instructions from the AlienVault Technical Support department.

Assign AlienVault Agent Configuration Profiles to Assets

You can assign a specific AlienVault Agent configuration profile to an asset, and you can do it from the assets list page or asset details page.

To assign an agent profile using the actions list

1. Go to **Environment > Assets**.
2. Select the asset and click **Actions > Assign Agent Profile**.
3. Choose the agent profile you want to assign to the selected asset.



SELECTED ASSETS	IP ADDRESSES	SENSOR	CREDENTIALS
COMPUTER_NAME_FOO	[redacted]	USMA-Sensor AWS	-

Choose Agent Profile

This agent profile will be assigned to all selected assets

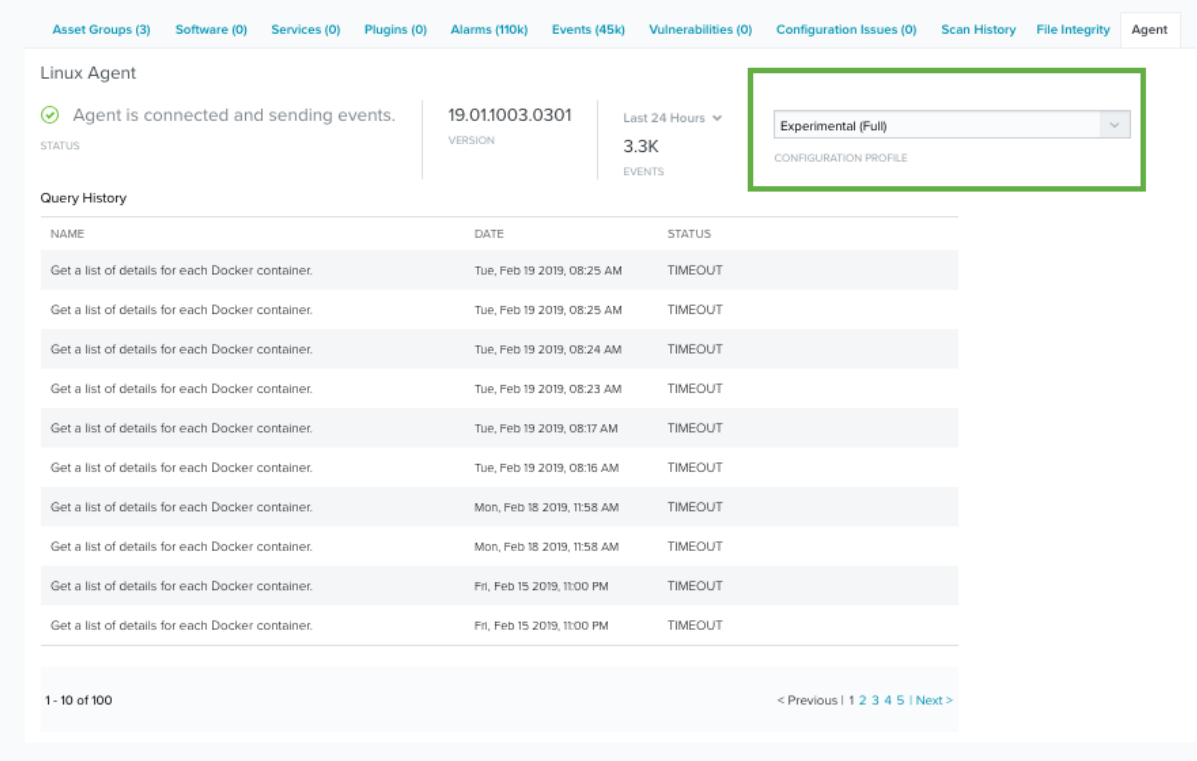
Windows Profile

USM Anywhere displays an informative message if assets exist but do not have agents deployed.

4. Click **Save**.

To assign an agent profile from the asset details page

1. Go to **Environment > Assets**.
2. Locate the asset and click the ⌄ icon next to name of the asset you want to assign the specific agent configuration profile, and then select **Full Details**.
3. Click **Agent**.
4. Click the Configuration Profile combo and select the profile you want to assign.



Linux Agent

Agent is connected and sending events.
STATUS

19.01.1003.0301
VERSION

Last 24 Hours ⌄
3.3K
EVENTS

Experimental (Full)
CONFIGURATION PROFILE

Query History

NAME	DATE	STATUS
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:25 AM	TIMEOUT
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:25 AM	TIMEOUT
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:24 AM	TIMEOUT
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:23 AM	TIMEOUT
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:17 AM	TIMEOUT
Get a list of details for each Docker container.	Tue, Feb 19 2019, 08:16 AM	TIMEOUT
Get a list of details for each Docker container.	Mon, Feb 18 2019, 11:58 AM	TIMEOUT
Get a list of details for each Docker container.	Mon, Feb 18 2019, 11:58 AM	TIMEOUT
Get a list of details for each Docker container.	Fri, Feb 15 2019, 11:00 PM	TIMEOUT
Get a list of details for each Docker container.	Fri, Feb 15 2019, 11:00 PM	TIMEOUT

1 - 10 of 100

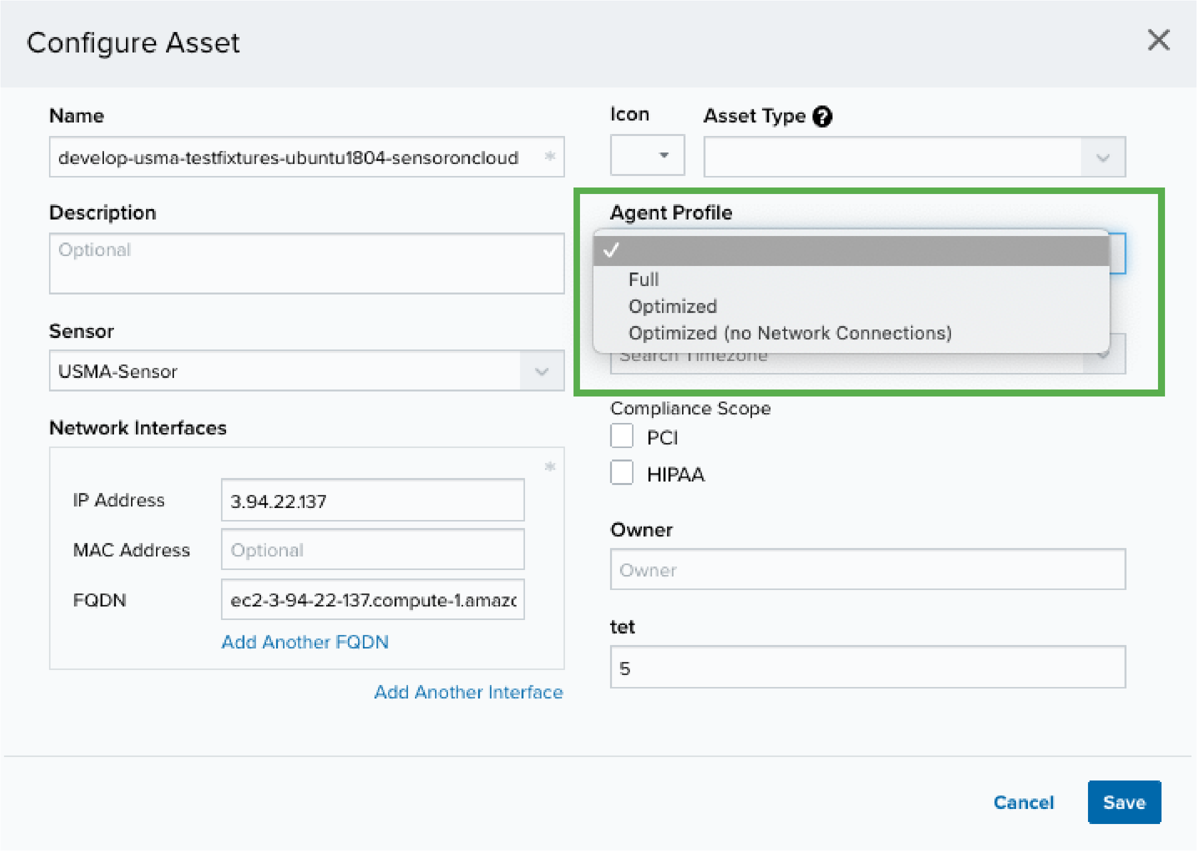
< Previous | 1 2 3 4 5 | Next >

To assign an agent profile from the Configure Asset dialog box

1. Go to **Environment > Assets**.
2. locate the asset, click the ⌄ icon next to the name of the asset you want to assign the specific agent configuration profile, and select **Configure Asset**.

> **Important:** The Agent Profile field displays if the agent is connected and if the user has the role Manager.

3. Choose the agent profile you want to assign to the selected asset.



Configure Asset

Name: develop-usma-testfixtures-ubuntu1804-sensoroncloud

Description: Optional

Sensor: USMA-Sensor

Network Interfaces

IP Address: 3.94.22.137

MAC Address: Optional

FQDN: ec2-3-94-22-137.compute-1.amazc

Agent Profile: ✓

Compliance Scope: □ PCI □ HIPAA

Owner: Owner

tet: 5

USM Anywhere displays an informative message if assets exist but do not have agents deployed.

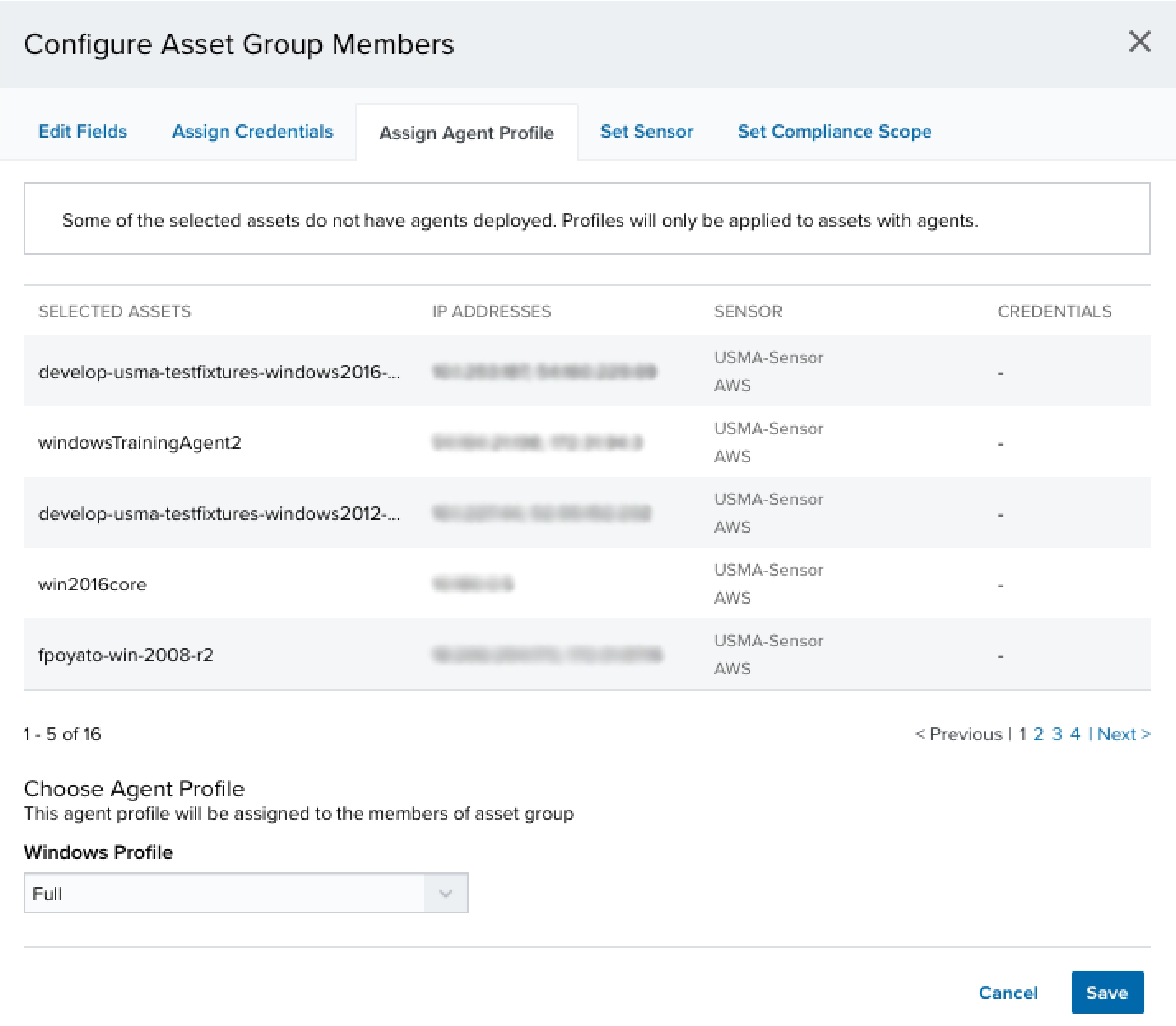
4. Click **Save**.

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

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

SELECTED ASSETS	IP ADDRESSES	SENSOR	CREDENTIALS
develop-usma-testfixtures-windows2016-...	[redacted]	USMA-Sensor AWS	-
windowsTrainingAgent2	[redacted]	USMA-Sensor AWS	-
develop-usma-testfixtures-windows2012-...	[redacted]	USMA-Sensor AWS	-
win2016core	[redacted]	USMA-Sensor AWS	-
fpoyato-win-2008-r2	[redacted]	USMA-Sensor AWS	-

1 - 5 of 16

Choose Agent Profile

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

Windows Profile: Full

5. Click **Save**.

The AlienVault Agent Script and Agent Updates

The AlienVault Agent script enables you to run several 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.

> **Note:** The AlienVault Agent is not configured to auto-update on its own. See AlienVault Agent Auto-Update below for details on how to enable the auto-update feature.

Location and Notes for the AlienVault Agent Script

System	Script	Location	Notes
Microsoft Windows	`alienvault-agent.ps1`	`C:\Program Files\osquery`	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.
Linux	`alienvault-agent.sh`	`/usr/bin`	Opened from the command line.
Apple macOS	`alienvault-agent.sh`	`/usr/local/bin`	Opened in Terminal.

AlienVault Agent Commands

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

Command	Explaination
start	Start the agent service.
stop	Stop the agent service.

Commands Available for the AlienVault Agent Script (Continued)

Command	Explaination
restart	Restart the agent service.
update	Update the agent version.
enable-auto-update [time]	Enable auto-update to check daily for new version. Time can optionally be designated for the check (24-hour format HH:MM). If no time is supplied, the daily check will occur between 09:00 and 17:00.
disable-auto-update	Disable agent auto-update.
force-update	Reinstall the agent service with the newest version. (This reinstalls the agent even if you are running the most recent version.)
uninstall	Uninstall the agent.
version	Print the agent version number.
help	Print help.
config	Connect to the agent API server to print or download your agent configuration.
osqueryi	Start an interactive osqueryi shell within your agent's configuration. (Typically used for prototyping and troubleshooting queries against your current configuration.)
report	Print a report containing pertinent information regarding agent information, including whether the auto-update feature is active. (Contains version, platform information, host identification, and other information. This command is most useful for relaying information to AT&T Cybersecurity Technical Support.)

AlienVault Agent Auto-Update

The AlienVault Agent has an auto-update feature, but it's disabled by default. You can enable auto-update and specify a time to check for updates, then the agent will update automatically 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.

ℹ **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 attain the auto-update feature.

The following procedure provides the steps for enabling the agent's auto-update function for each operating system (OS). You can use the agent script's `report` command to verify that the auto-update function is active.

Linux

To enable agent auto-updates on Linux

1. Run the following command from a bash shell:

   ```
   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:

   ```
   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:

   ```
   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.

When the AlienVault Agent is updated, the installation process detects the presence of an existing `osquery.flags` file and uses its `--specified_identifier` flag for identification, thus maintaining the continuity.

AlienVault Agents Memory Consumption and the osquery Watchdog

The AlienVault Agent is configured to have two osquery processes running: an initial osquery process that functions as a watchdog, and the child worker process that creates the scheduled queries. The initial watchdog process manages the child worker and terminates any processes that exceed the memory limitations configured in the watchdog settings.

Watchdog Overview

The max threshold settings for the watchdog resources are:

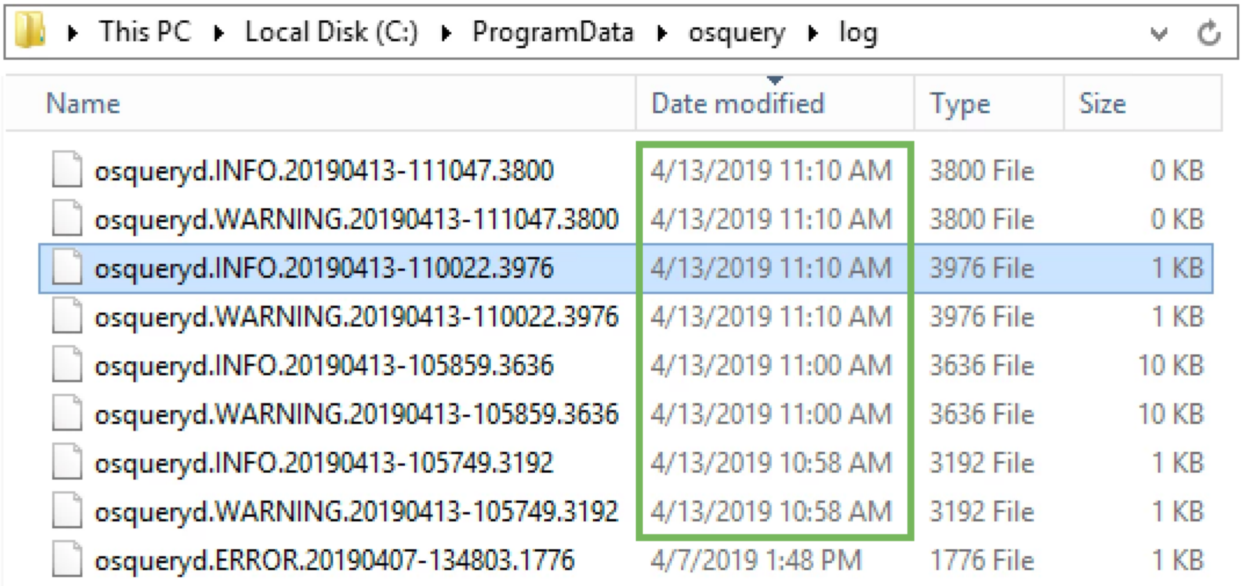
- CPU: Above 25% usage for over 9 consecutive seconds.
- Memory: When 350MB is reached (AlienVault Agent default setting).

The watchdog profiles the memory footprint at startup and subtracts that from the monitored value. It only restarts the worker if that difference exceeds the watchdog level set at that time. So, if a watchdog level is set to 350MB and the agent starts up with an initial worker process footprint of 30MB, the watchdog limit will be triggered at 380MB (350MB limit + 30MB initial memory footprint = 380MB threshold limit).

Watchdog Threshold Limits and Errors

Once the watchdog limit is reached, the osquery watchdog respawns the child worker process. After osquery is restarted, the previously active queries are referenced by osquery to see which ones did not finish normally. It is possible that one or more of these queries caused the watchdog limit to be exceeded, therefore the unfinished queries are blacklisted from the scheduler for 24 hours.

If the osquery processes exceed their allocated resources, there is the possibility that the watchdog may respawn the process without giving any error message. A good indicator that this has happened can be found by looking at the logs subdirectory and 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. Here is an example:



This PC ▸ Local Disk (C:) ▸ ProgramData ▸ osquery ▸ log

Name	Date modified	Type	Size
osqueryd.INFO.20190413-111047.3800	4/13/2019 11:10 AM	3800 File	0 KB
osqueryd.WARNING.20190413-111047.3800	4/13/2019 11:10 AM	3800 File	0 KB
osqueryd.INFO.20190413-110022.3976	4/13/2019 11:10 AM	3976 File	1 KB
osqueryd.WARNING.20190413-110022.3976	4/13/2019 11:10 AM	3976 File	1 KB
osqueryd.INFO.20190413-105859.3636	4/13/2019 11:00 AM	3636 File	10 KB
osqueryd.WARNING.20190413-105859.3636	4/13/2019 11:00 AM	3636 File	10 KB
osqueryd.INFO.20190413-105749.3192	4/13/2019 10:58 AM	3192 File	1 KB
osqueryd.WARNING.20190413-105749.3192	4/13/2019 10:58 AM	3192 File	1 KB
osqueryd.ERROR.20190407-134803.1776	4/7/2019 1:48 PM	1776 File	1 KB

Scheduled Query Failure Messages

The watchdog enforces limits on the worker process to protect systems from CPU-expensive and memory-intensive queries. If the watchdog observes limit violations, it will display an error similar to the following:

```
Scheduled query may have failed: <<...>>
```

This line is created when a child worker starts and finds what osquery calls a "dirty bit" toggled for the currently-executing query. If a child worker process is stopped abruptly and a query does not finish, a similar line may display.

Lines that indicate the watchdog exceeded one of its limits include the following:

```
osqueryd worker (1234) system performance limits exceeded
osqueryd worker (5678) memory limits exceeded: 442494
```

The process identifier (PID) of the offending child worker is included in parenthesis.

If the child worker finds itself in a reoccurring error state, or if the watchdog continues to stop the worker, additional lines like the following are created:

```
osqueryd worker respawning too quickly: 1 times
```

The watchdog implements an exponential backoff when respawning child workers, and the offending query is blacklisted from running for 24 hours.

The osquery watchdog is only used for the worker process. It is enabled by default and can be disabled with a control flag.

See the official osquery documentation on query failures with the watchdog for more information on osquery errors and debugging options.

Work Process Control Flags

Many of the parameters of the watchdog are controlled by default settings that can be adjusted with optional command-line interface (CLI) flags. For experienced users who need more advanced control over the osquery watchdog, such as changing the CPU and memory limits, or toggling the watchdog's monitoring functions, refer to the osquery CLI flags documentation.

AT&T Cybersecurity only supports the agent's default watchdog settings. Adjusted settings should be tested before applying any changes to your environment.

AlienVault Agent Events and Queries

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

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 events from the agent except for Microsoft Windows events.
- **AlienVault Agent - Windows EventLog**: This data source parses 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. connected. 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 must 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 opens confirming 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 must 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 opens confirming 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 must 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 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.

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

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

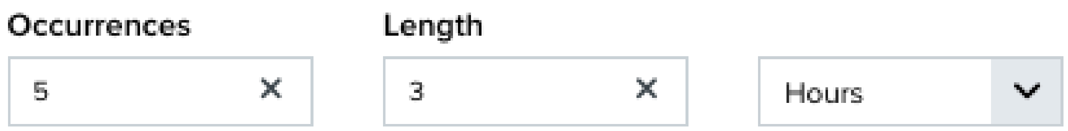
7. (Optional.) Click **Add Group** to group your conditions.

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

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.



Occurrences	Length	
5	3	Hours

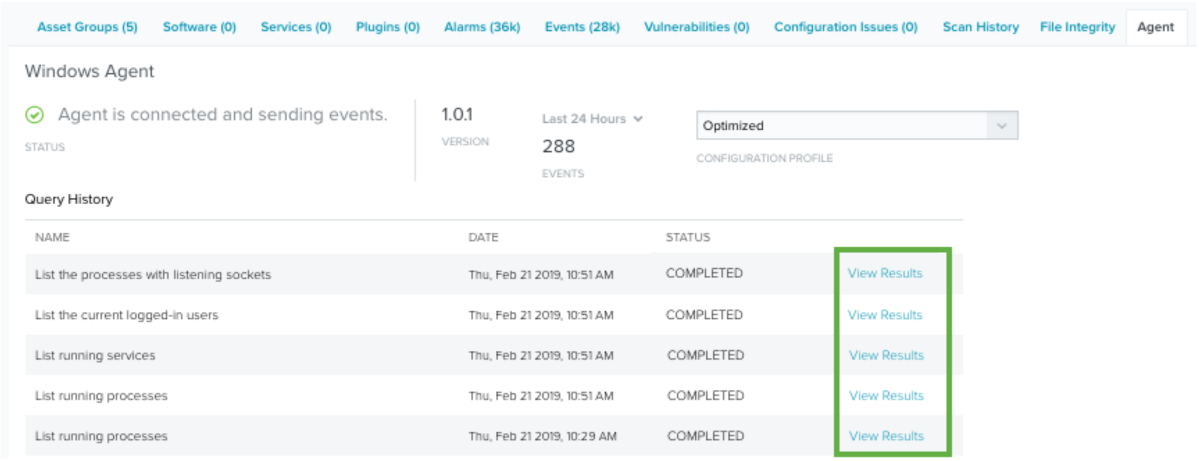
In this example, the rule applies when the configured conditions happen five times every three hours.

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 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.



Windows Agent

Agent is connected and sending events.
STATUS

1.0.1
VERSION

Last 24 Hours
288
EVENTS

Optimized
CONFIGURATION PROFILE

Query History

NAME	DATE	STATUS	
List the processes with listening sockets	Thu, Feb 21 2019, 10:51 AM	COMPLETED	View Results
List the current logged-in users	Thu, Feb 21 2019, 10:51 AM	COMPLETED	View Results
List running services	Thu, Feb 21 2019, 10:51 AM	COMPLETED	View Results
List running processes	Thu, Feb 21 2019, 10:51 AM	COMPLETED	View Results
List running processes	Thu, Feb 21 2019, 10:29 AM	COMPLETED	View Results

The full list of queries are available in the following table.

Available AlienVault Agent Queries

Query Name	Platform	Description
Get Docker container running processes	Linux, macOS	Get the list of processes running in each Docker container.
Get Docker containers details	Linux, macOS	Get a list of details for each Docker container.
Get Docker containers open ports	Linux, macOS	Get a list with open ports and network information for each Docker container.
Get file information	Linux, macOS, and Windows	Get information from the file specified in the first parameter. You must include the file path of the file.
Get files downloaded in the system	macOS	Generate a list of all files downloaded in the system.
Get IE typed URLs	Windows	Get the list of Microsoft Internet Explorer (IE)'s entered URLs.
Get firewall configuration	Windows	Get a list of firewall configurations for different profiles and rules.
Get installed packages history	macOS	Get the list of the latest installed packages in the system.
Get logged-in users	Linux, macOS, and Windows	Get the list of currently logged-in users.
Get listening processes	Linux, macOS, and Windows	Get the list of the processes with listening sockets.
Get network connections	Linux, macOS, and Windows	Get the list of the current network connections.
Get network connection information	Linux	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.
Get network shares	Windows	Get the list of network-shared resources from the system.

Available AlienVault Agent Queries(Continued)

Query Name	Platform	Description
Get persistence registry keys	Windows	Get registry key values commonly used for persistence by attackers.
Get recent files	Windows	Get the list of recent files.
Get recent items	macOS	Get the list of recently opened files.
Get running processes	Linux, macOS, and Windows	Get the list of running processes.
Get running services	Windows	Get the list of running services.
Get SSH authorized keys	Linux, macOS	Get the list of SSH-authorized keys allowed in the system.
Get users launched services	macOS	Get the list of LaunchAgents and LaunchDaemons services installed in the system.
Get Wi-Fi connection status	macOS	Get information from the current Wi-Fi connection.
Get Wi-Fi preferred connections	macOS	Get information from the preferred Wi-Fi connections.
Hunt for potential library injection - .so deleted from disk	Linux	Hunt for the potential library injection of a memory map with a deleted shared object on disk and rwxp memory.
Hunt for potential library injection - no .so on disk and rwxp memory	Linux	Hunt for the potential library injection of a memory map with no shared object on disk and rwxp memory.
Hunt for potential library injection - no common .so isolation	Linux	Hunt for the potential library injection of a shared library loaded from an uncommon location.
Hunt for running processes with no binary on disk	Linux, macOS, and Windows	Hunt for running processes that do not have a matching binary on disk.
Hunt for traffic to remote IP	Linux, macOS, and Windows	Hunt for non-web traffic to remote IP addresses not using port 0, 80, or 443.