



# Cisco Secure Network Analytics

Analytics: Detections, Alerts, and Observations 7.4.2



---

# Table of Contents

<b>Overview</b>	<b>6</b>
Enable Analytics	7
Disable Analytics	7
<b>System Requirements</b>	<b>8</b>
<b>APIs</b>	<b>9</b>
<b>Alerts and Observations Overview</b>	<b>10</b>
Alert Prerequisite Chart	10
Alert Descriptions	14
Observation Descriptions	33
<b>Alerts Summary</b>	<b>39</b>
Open Alerts Summary	39
Filter the Alerts Table	39
View the Alerts Table	40
Edit Alerts Table Entries	41
View Related Configuration Pages	42
Download a .CSV File	42
Alerts Workflow	42
Alerts FAQs	43
Why are certain alerts disabled?	43
What does an alert's status mean?	43
How does a subnet's sensitivity affect alerts?	44
Investigating Alerts	44
Triage Open Alerts	45
Snooze an Alert	45
Unsnuzzle a Snoozed Alert	45
Close an Alert	46
Reopen a Closed Alert	46
Update an Alert	46

---

Review an Alert .....	46
Review Supporting Observations and Contextual Details .....	47
Source Entities .....	47
External Entities .....	48
Examine an Entity and Associated Users .....	49
Remediate an Issue .....	49
Fine-Tune Your Secure Network Analytics Settings .....	50
Alert Details .....	50
Open Alert Details .....	50
View Alert Type Details .....	50
View Alert Rule Details .....	51
View descriptions for the Supporting Observations table .....	51
Other Pages You Can Access from the Alert Details Page .....	58
Alert Priorities Configuration .....	58
Flow Search Results .....	58
Device Report .....	58
Alerts Summary .....	59
Observations by Device .....	59
Enter Comments for an Alert .....	59
Device Report .....	59
Open Device Report .....	59
Device Report Overview .....	60
Device Outline .....	60
Alerts .....	60
History .....	60
Edit Time Range .....	60
Summary .....	60
Traffic .....	62
IPs .....	63
<b>Roles .....</b>	<b>64</b>

---

---

Open the Roles page .....	64
Set the time frame .....	64
View the results .....	65
Export results .....	65
<b>Observations Dashboard .....</b>	<b>66</b>
Open Observations Dashboard .....	66
Observations Highlights Overview .....	66
View Observations Highlights .....	67
View Descriptions for the Observations Highlights tables .....	67
<b>Observation Types .....</b>	<b>74</b>
Open Observation Types .....	74
View Observation Types .....	74
<b>Observations by Device .....</b>	<b>75</b>
Open Observations by Device .....	75
View Observations by Device .....	75
<b>Selected Observations .....</b>	<b>77</b>
Open Selected Observations .....	77
View Selected Observations .....	77
View descriptions for the Selected Observations table .....	78
<b>Configuring Priorities .....</b>	<b>85</b>
Open Alerts Priorities Configuration .....	85
Configure Alert Priorities .....	85
<b>Configuring Expiration .....</b>	<b>87</b>
Open Alerts Expiration Configuration .....	87
Configure Alert Expiration Days .....	87
<b>Configuring Country Watchlist .....</b>	<b>88</b>
Open Alerts Country Watchlist Configuration .....	88
View Watched Countries .....	88
<b>Troubleshooting .....</b>	<b>89</b>
Analytics jobs are lagging .....	89

---

The secondary Manager has been promoted to primary Manager .....	89
An appliance went down due to degradation .....	89
<b>Contacting Support .....</b>	<b>90</b>
<b>Change History .....</b>	<b>91</b>

# Overview

We are in the process of updating our alerts for Cisco Secure Network Analytics (formerly Stealthwatch). The new alerts will have greater out-of-the-box value and require less tuning and pre-configuration, all while continuing to provide accurate data. In v7.4.1, we offered early access to a selection of these new alerts and capabilities within a designated space in our product.

Some of the expanded capabilities are as follows:

- Automatic role classification
- Alerts that are aligned to modern threats
- Proprietary capability that currently exists in our SaaS product (Cisco Secure Cloud Analytics) called "Entity Modeling," which greatly enhances baselining for normal behavior

When you enable Analytics, related features are switched on within your deployment. These additional capabilities function in parallel with your existing detections and interfaces. Continue to monitor your alarms, security events, and Manager as you do today, while also taking advantage of our new experimental detections and interface capabilities.

When you open a new alert in the Manager, you can view the supporting observations that led the system to generate the alert. From these observations, you can also view additional context about the entities involved, including the traffic that they transmitted and, if available, external threat intelligence.

The new alerts consume additional system resources. Review your resource consumption prior to enabling this optional feature. Feature sets for the new alerts, as well as their general availability, are limited to specific deployment types and may change with each future release. For more information, see [System Requirements](#).

Please provide feedback using inline feedback forms as you use the new alerts.



- The new alerts support only systems that contain just 1 Cisco Secure Network Analytics Data Store domain. (Your system can also contain 1 or more non-Data Store domains.) If after initially creating 1 Data Store domain on your system, you later create one or more Data Store domains, be aware that we do not provide support for this scenario.
- You cannot enable Analytics until you have deployed a minimum of 1 node and added a minimum of 1 Data Store Flow Collector (NetFlow) on your network.

- If your system is consuming sFlow, the accuracy of your detections and the performance of your system may be impacted.

## Enable Analytics

1. From the main menu, choose **Configure > DETECTION Analytics**.

*The Analytics Welcome page opens.*

2. In the upper right corner of the page, click the switch so that the label displays

*Analytics On*, like this:  .

*The Alerts Summary opens.*



- Only users assigned the role of **Primary Admin** can enable and disable Analytics.
- Users assigned the web role of Analyst cannot access any configuration pages using the menu option (**Configure > Alerts**). However, all users, regardless of their assigned data roles or function roles, can access all pages and data related to the new alerts.

## Disable Analytics

1. From the main menu, choose **Configure > DETECTION Analytics**.

*The Analytics Welcome page opens.*

2. In the upper right corner of the page, click the switch so that the label displays

*Analytics Off*, like this:  .

*The Analytics Welcome page remains open.*

# System Requirements

Feature sets for the new alerts and their general availability are limited to specific deployment types and may change with each future release. Please verify that your system adheres to the required specifications. Systems that don't adhere to applicable specifications, or are under heavy load, may experience adverse impacts to their performance, reliability, and retention capabilities.

For more information about the system requirements required for your deployment type, see the Resource Requirements section in the [Virtual Edition Appliance Installation Guide](#).



- Alerts and Observations data is processed and stored only on the Manager that is currently in the primary role. When you promote the original primary Manager back to the primary role, you will not be able to view any alerts and observations data that was processed on the original secondary Manager while it served in the primary role.
- Only users assigned the role of **Primary Admin** can enable and disable Analytics.

In order to enable Analytics, your deployment must be configured

- on a Virtual or a Hardware Data Store deployment with any number of Flow Collectors.
- with only 1 Secure Network Analytics Data Store domain.

To install appliances, follow the instructions in the [Virtual Edition Appliance Installation Guide](#), the [x2xx Series Hardware Appliance Installation Guide](#), or the [x3xx Series Hardware Appliance Installation Guide](#).



---

# APIs

When using APIs in Secure Network Analytics, refer to the [Secure Cloud Analytics API document](#). This document includes all the API endpoints and related documentation that can be leveraged with the new alerts' engine within Secure Network Analytics.

These endpoints are shared among Secure Network Analytics and Secure Cloud Analytics, and can be used for either deployment.



To use these APIs in Secure Network Analytics, you still need to use *api\_key*, which is shown in the following command:  
`cat /lancope/var/services/detections/config/api_key.`

# Alerts and Observations Overview

Secure Network Analytics uses dynamic entity modeling to track the state of your network. In the context of Secure Network Analytics, an entity is something that can be tracked over time, such as a host or endpoint on your network. Dynamic entity modeling gathers information about entities based on the traffic they transmit and activities they perform on your network.

From this information, Secure Network Analytics identifies:

- Roles for the entity, which are a descriptor of what the entity usually does. For example, if an entity sends traffic that is generally associated with email servers, Secure Network Analytics assigns the entity an Email Server role. The role/entity relationship can be many-to-one, as entities may perform multiple roles.
- Observations for the entity, which are facts about the entity's behavior on the network, such as a heartbeat connection with an external IP address, an interaction with an entity on a watchlist, or a remote access session established with another entity. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Based on the combination of roles, observations, and other threat intelligence, Secure Network Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system.

## Alert Prerequisite Chart

The Alert Prerequisites chart provides the list of the new alerts sorted by their baseline requirements as well as a brief description of the alert's meaning.

The following table provides an overview of how much history is required to generate a given alert type and possible reasons for further investigation. Note that the reasons for investigation are not guarantees that this alert indicates the listed behavior or rationale; these reasons should be considered as you further investigate the alert.

This table also lists, where applicable, any MITRE ATT&CK tactics or techniques associated with an alert type.

Alert	History	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Amplification Attack	0 days	Netflow	Impact	Network Denial of Service

Alert	History	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Anomalous Windows Workstation	14 days	Netflow		
Country Set Deviation	36 days	Netflow		
Emergent Profile	14 days	Netflow	Exfiltration	Exfiltration Over Alternative Protocol
Empire Command and Control	1 day	Netflow	Command and Control	Non-Application Layer Protocol
Exceptional Domain Controller	7 days	Netflow		
Excessive Access Attempts (External)	0 days	Netflow	Credential Access	Brute Force
Excessive Connections to Network Printers	0 days	Netflow		
Geographically Unusual Remote Access	30 days	Netflow	Initial Access	External Remote Services
Heartbeat Connection Count	1 day	Netflow	Command and Control	Non-Application Layer Protocol
High Bandwidth Unidirectional Traffic	0 days	Netflow	Exfiltration	Automated Exfiltration
Inbound Port Scanner	1 day	Netflow	Discovery	Network Service Scanning
Internal Connection Spike	0 days	Netflow	Discovery	Network Service Scanning
Internal Port Scanner	7 days	Netflow	Discovery	Network Service Scanning
LDAP Connection Spike	9 days		Discovery	Network Service Scanning

Alert	History	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Meterpreter Command and Control Success	1 day	Netflow	Command and Control	Non-Application Layer Protocol
NetBIOS Connection Spike	9 days	Netflow	Lateral Movement	Remote Services
Network Population Spike	36 days	Netflow		
Network Printer with Excessive Connections	0 days	Netflow		
New Internal Device	21 days	Netflow		
New IP Scanner	9 days	Netflow	Discovery	Network Service Scanning
New Remote Access	36 days	Netflow	Initial Access	External Remote Services
New SNMP Sweep	9 days	Netflow	Discovery	Network Service Scanning
New Unusual DNS Resolver	7 days	Netflow, Passive DNS		
Non-Service Port Scanner	9 days	Netflow	Discovery	Network Service Scanning
Outbound LDAP Spike	0 days		Reconnaissance	Active Scanning
Outbound SMB Connection Spike	0 days	Netflow	Lateral Movement	Remote Services
Persistent Remote Control Connections	7 days	Netflow	Initial Access	External Remote Services
Potential Data Exfiltration	0 days	Netflow	Exfiltration	Automated Exfiltration

Alert	History	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Potential Database Exfiltration	7 days	Netflow	Exfiltration	Exfiltration Over Alternative Protocol
Protocol Forgery	1 day		Command and Control	Non-Standard Port
Protocol Violation (Geographic)	0 days	Netflow	Command and Control	Application Layer Protocol
Remote Access (Geographic)	0 days	Netflow		
Repeated Umbrella Sinkhole Communications	0 days		Command and Control	Application Layer Protocol
Repeated Watchlist Communications	0 days	ETA, Firewall, Netflow, Passive DNS	Command and Control	Application Layer Protocol
Role Violation	0 days	Netflow	Persistence	Create or Modify System Process
SMB Connection Spike	9 days	Netflow	Lateral Movement	Remote Services
Suspected Botnet Interaction	1 day	ETA, Firewall, Netflow, Passive DNS	Command and Control	Application Layer Protocol
Suspected Cryptocurrency Activity	0 days	ETA, Firewall, Netflow, Passive DNS	Impact	Resource Hijacking
Suspected Port Abuse (External)	1 day	Netflow	Discovery	Network Service Scanning
Suspected Remote Access Tool Heartbeat	0 days	Netflow, Passive DNS	Command and Control	Non-Application Layer Protocol

Alert	History	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
Suspected Zerologon RPC Exploit Attempt	0 days	Netflow, Passive DNS	Privilege Escalation	Exploitation for Privilege Escalation
Suspicious SMB Activity	14 days	Netflow	Lateral Movement	Remote Services
Talos Intelligence Watchlist Hits	0 days	ETA, Firewall, Netflow, Passive DNS	Command and Control	Application Layer Protocol
Unusual DNS Connection	1 day	Netflow, Passive DNS		
Unusual External Server	14 days	ETA, Firewall, Netflow, Passive DNS	Command and Control	Application Layer Protocol
Worm Propagation	9 days	Netflow	Lateral Movement	Exploitation of Remote Services

## Alert Descriptions

Listed below are the alert types that Secure Network Analytics can generate. This list contains both published and unpublished alerts.

Unpublished alerts are alerts that Secure Network Analytics still considers to be in the experimental phase and therefore have not yet been officially published. They are Off by default. Unpublished alerts work just as other alerts do (for instance, you can snooze and close them). Additionally, changing the priority of the alert does not affect whether or not an alert is published or unpublished. However, they will behave inaccurately in single node deployments.

The unpublished alerts are as follows (they are also denoted by an asterisk [\*] in the alert list below).

- Amplification Attack
- Country Set Deviation
- Emergent Profile
- Exceptional Domain Controller

- Excessive Connections to Network Printers
- Heartbeat Connection Count
- High Bandwidth Unidirectional Traffic
- NetBIOS Connection Spike
- Network Population Spike
- Network Printer with Excessive Connections
- New IP Scanner
- New SNMP Sweep
- New Unusual DNS Resolver
- Non-Service Port Scanner
- Outbound SMB Connection Spike
- Persistent Remote Control Connections
- Potential Data Exfiltration
- Potential Database Exfiltration
- Protocol Violation (Geographic)
- Repeated Umbrella Sinkhole Communications
- SMB Connection Spike
- Suspected Remote Access Tool Heartbeat
- Unusual DNS Connection
- Worm Propagation

## Amplification Attack \*

**Description:** This entity sent traffic with a profile that suggests participation in an amplification attack. An amplification attack attempts to overwhelm a server with a massive amount of packets in response to a request, usually involving spoofed IP addresses to allow multiple entities to send traffic in response to a request. Participation in an amplification attack may indicate that an entity has been infected with botnet malware, and is sending these packets unintentionally.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Traffic Amplification Observations

**Next Steps:** Reference the entity information in the alert and supporting observations, and determine whether or not an external entity is responsible for spreading malware. If

so, update your firewall rules to block traffic from the external entity, and any other entities if it is a distributed denial of service (DDoS) attack.

If the entity sending the amplification attack is internal to your network, quarantine the entity from your network, and any other entities if it is a DDoS attack. Examine the entities for, and remove, malware.

## Anomalous Windows Workstation

**Description:** A Windows workstation used a new anomalous behavioral profile (e.g., the host connected to many entities over BitTorrent). This alert uses the Anomalous Profile observation and may be an indication of malware or misuse.

**Prerequisite:** This alert requires 14 days of history to establish an entity's normal activity level.

**Associated Observations:** Anomalous Profile Observations

**Next Steps:** Reference the supporting observations to determine the entity's roles and determine whether or not there is a legitimate business reason for the anomalous behavior. For example, if an entity used BitTorrent to connect to other entities, it may be a test entity or some type of possible testing of firewall rules or other security tests. If there is not a legitimate reason for the anomalous behavior, examine the entity and determine whether or not the entity is functioning as intended, and if it is free of malware.

## Country Set Deviation \*

**Description:** This entity has significantly deviated from the set of countries it usually communicates with. This alert requires 36 days of history.

**Prerequisite:** This alert requires 36 days of history to establish the normal set of countries an entity communicates with.

**Associated Observations:** Country Set Deviation Observations

**Next Steps:** Reference the supporting observations to find the entities to which the entity has established connections, and their geolocation. Determine why it established these connections, and remediate the issue if it was due to malicious behavior. Update your Country Watchlist as necessary to include any countries involved with malicious behavior.

## Emergent Profile \*

**Description:** A highly sensitive entity has traffic that fits a new profile. For example, an entity that starts accepting FTP connections may be exposing sensitive data.



**Prerequisite:** This alert requires 14 days of history to establish entity models and determine expected traffic profiles.

**Associated Observations:** New Profile Observations

**Next Steps:** Reference the entity's new traffic profile in the supporting observations, and whether it is expected, especially in light of the previous profile or role. For example, if an entity has been repurposed from an FTP server to a mail server, this shift in behavior is expected. If it is not expected, investigate why the entity's traffic has changed, and if it is malicious.

## Empire Command and Control

**Description:** An entity has established new periodic connections that appear to be part of an Empire PowerShell Command and Control channel. This alert uses the Heartbeat observation and may indicate the device is compromised. This alert requires 1 day of history.

**Prerequisite:** This alert requires 1 day of history to establish entity models and determine expected traffic profiles.

**Associated Observations:** Heartbeat Observations

**Next Steps:** Review the entity's traffic in the supporting observations, identify the entity to which it is establishing the heartbeat connections, and determine if the traffic is anticipated or malicious. If malicious, determine if other entities on your network are similarly affected. Quarantine the entities and remove any malware. Update your block list and firewall rules to disallow the command and control servers' access to your network.

## Exceptional Domain Controller \*

**Description:** This entity identified as a Domain Controller deviated from its usual behavior. This may indicate abuse. For example, if the entity is establishing many outbound connections, it may be a sign of data exfiltration, botnet malware, or possibly malicious DNS request redirects.

**Prerequisite:** This alert requires 7 days of history to establish normal entity traffic profiles.

**Associated Observations:** New External Server Observations, Exceptional Domain Controller Observations

**Next Steps:** From the alert and supporting observations, view the entity's traffic profile and connections with other entities to determine what types of traffic it is sending, and if it is malicious in nature. Determine if data has been exfiltrated from your network, and if so, the types of data, and how best to remediate the situation.

## Excessive Access Attempts (External)

**Description:** This entity has many failed access attempts from an external entity. For example, a remote entity trying repeatedly to access an internal server using SSH or Telnet would trigger this alert.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Multiple Access Failures Observations

**Next Steps:** Reference the supporting observations and ensure that the external entity is abnormal and unexpected. If it is normal and expected, determine why a user or machine login keeps failing to login, such as if credentials changed, but the user or machine was not given the updated credentials. If the external entity is unknown, update your firewall or security group rules to limit access for the remote control protocol. Update your block list and firewall rules to disallow this entity's access to your network if the entity is potentially malicious.

## Excessive Connections to Network Printers \*

**Description:** This entity initiates too many connections to network printers. This behavior may indicate a denial-of-service attack, or an attempt to exfiltrate data by printing documents.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Excessive Connections to Network Printers Observations

**Next Steps:** Reference the supporting observations and determine how the entity is communicating with the network printers. Quarantine the entity and remove malware if the communications are malicious. Examine the printer job queues to determine what actions they are performing. Clear the queues if the printer is tasked to print confidential documents. Disconnect the printers' internet access if they are tasked to transmit confidential information to external entities. Remove any malware from the printers as necessary.

## Geographically Unusual Remote Access

**Description:** This entity has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source would trigger this alert. Remote access from an unusual geolocation could be an indication of malicious access.

**Prerequisite:** This alert requires 30 days of history to establish sufficient traffic history, and determine normal traffic based on geolocation.

**Associated Observations:** Remote Access Observations

**Next Steps:** Reference the supporting observations and determine what action the entity took, and why it took the action. If the entity is expected, but is accessing the internet from another country than expected, update your firewall settings to allow this traffic. Remediate the action, and update your blocklist and firewall rules to disallow the entity from accessing your network if this is malicious behavior.

## Heartbeat Connection Count \*

**Description:** This entity has established new periodic connections with many remote entities, which might indicate unauthorized P2P traffic or botnet activity.

**Prerequisite:** This alert requires 1 day of history to establish traffic models.

**Associated Observations:** Heartbeat Observations

**Next Steps:** Reference the supporting observations and determine the entities to which the affected entity is establishing the heartbeat connections, and confirm that they are not expected. Understand the purpose for the periodic connections, and update your firewall and blocklist rules to prevent further access.

## High Bandwidth Unidirectional Traffic \*

**Description:** This entity started sending large amounts of data to new remote hosts. This can indicate misuse or misconfiguration. For example, malware might cause an infected host to attack a website by directing a host to send lots of data to a vulnerable service.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** New High Throughput Connection Observations

**Next Steps:** Reference the supporting observations for flow details, and determine why the entity is sending large amounts of traffic. If the traffic is not permissible, investigate what software on the host is responsible for the malicious traffic.

## Inbound Port Scanner

**Description:** This entity was port scanned by an external entity. If an external entity is scanning entities internal to your network, it may be scanning for unpatched vulnerabilities or other ways to infiltrate entities on your network.

**Prerequisite:** This alert requires 1 day of history to establish entity models and determine normal behavior.

**Associated Observations:** External Port Scanner Observations

**Next Steps:** Reference the supporting observations to identify the external entity that port scanned your internal entity. Determine if it is the result of planned penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and allow list rules to allow the traffic if it is intended. Block the traffic if it is not intended. Update your firewall rules as necessary, including port access.

## Internal Connection Spike

**Description:** This entity had a sudden increase in internal connections, which is suggestive of scanning activity.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Record Metric Outlier Observations

**Next Steps:** Reference the supporting observations to determine why the entity is establishing multiple connections. Determine if it is performing scanning activity because of penetration testing or another allowed purpose, or if it is malicious behavior. Remediate the behavior as necessary.

## Internal Port Scanner

**Description:** This entity has started a port scan on an entity internal to your network. If an internal entity is scanning entities internal to your network, it may be a penetration test by your network security team, or it may be malicious behavior from an entity on your network.

**Prerequisite:** This alert requires 7 days of history to establish entity models and normal entity behavior.

**Associated Observations:** Internal Port Scanner Observations

**Next Steps:** Reference the supporting observations to understand the type of scanning activity. Scanning activity is often associated with a compromised host that is searching for data or other hosts to infect. To gain more context, search for observations related to the entity that the system logged around the same time (such as watchlist interactions). This may provide additional information about the behavior.

## LDAP Connection Spike

**Description:** This entity attempted to contact an unusually large number of internal LDAP servers. This alert may be an indication of malware or abuse.

**Prerequisite:** This alert requires 9 days of history to establish normal behavior.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations and determine why the entity is establishing connections with multiple LDAP servers, what types of actions the entity is taking, and if this is malicious behavior. If data was exfiltrated, follow your organization's guidelines for dealing with data exfiltration. Quarantine the entity as necessary to remove malware.

## Meterpreter Command and Control Success

**Description:** This Device has established new periodic connections that appear to be part of a Meterpreter Command and Control channel. This alert uses the Heartbeat observation and may indicate that the device is compromised.

**Prerequisites:** This alert requires 1 day of history.

**Associated Observations:** Heartbeat Observations

**Next Steps:** Review the entity's traffic in the supporting observations, identify the entity for which it is establishing the heartbeat connections, and determine if the traffic is anticipated or malicious. If malicious, determine if other entities on your network are similarly affected. Quarantine the entities and remove any malware. Update your block list and firewall rules to disallow the command and control servers' access to your network.

## NetBIOS Connection Spike \*

**Description:** Source attempted to contact large number of hosts using NetBIOS. This can be an indication of malware or abuse.

**Prerequisite:** This alert requires 9 days of history to establish entity traffic models and determine normal traffic behavior.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations to determine the host and analyze the traffic flow details. NetBIOS is not a commonly used protocol, so any connection spike events would likely be malicious. If detected, review what applications are using NetBIOS and if that traffic is legitimate. If so, snooze this alert for the host.

## Network Population Spike \*

**Description:** A record number of IP addresses were observed communicating on the network. This might indicate spoofing of source addresses or scanning activity.

**Prerequisite:** This alert requires 36 days of history to establish a sufficient amount of days to count the total number of entities communicating on the network.

**Associated Observations:** Population Spike Observations

**Next Steps:** Reference the supporting observations associated with the alert and determine if the IP addresses are legitimate entities. If they are not legitimate, locate the source of the spoofed addresses, and remediate as necessary.

## Network Printer with Excessive Connections \*

**Description:** This printer initiates too many connections. This may indicate malicious behavior, such as botnet malware infection.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Network Printer with Excessive Connections Observations

**Next Steps:** Review the established connections, and the entities that established connections with the printer. Reference the supporting observations to see what type of connections were established by the printer. If the connections indicate the printer is compromised, quarantine the printer and consider removing and re-installing the operating systems.

## New Internal Device

**Description:** A new entity has appeared on a restricted subnet range after not being seen in the lookback period.

**Prerequisite:** This alert requires 21 days of history to learn which entities are normally seen on the network. This alert also requires selecting **New Internal Device** on the Subnet Configuration page.

**Associated Observations:** New Internal Device Observations

**Next Steps:** Reference the supporting observations to determine if this entity is an expected entity, and is merely new to your network. If the entity is expected and not malicious, close the alert; future new entities will continue to generate alerts. If the entity is suspicious, determine the MAC address by accessing the local switch.

## New IP Scanner \*

**Description:** This entity started scanning the local IP network. This could indicate, for example, reconnaissance by an attacker.

**Prerequisite:** This alert requires 9 days of history to establish entity traffic models and determine normal traffic behavior.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations and investigate why the external entity is scanning the network. Determine if it is the result of penetration testing or other

intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for the entity or user who owns the machine to determine what software caused the scanning activity.

## New Remote Access

**Description:** This entity has been accessed (e.g., via SSH) from a remote host for the first time in recent history. This remote access may indicate malicious behavior, especially if the entity is not expected to accept connections from external entities.

**Prerequisite:** This alert requires 36 days of history to establish sufficient traffic history and entity models.

**Associated Observations:** Remote Access Observations

**Next Steps:** Reference the supporting observations to determine why the entity is being accessed by the external entity, and if it is a legitimate form of access. Also determine (based on the observations) if there were multiple access attempts to the source entity prior to this access, whether from this external entity or another external entity. Update your firewall and blocklist rules based on this information.

## New SNMP Sweep \*

**Description:** This entity attempted to reach a large number of hosts using SNMP. This can be an indication of network reconnaissance cause by malicious software. An SNMP sweep, when performed by a malicious actor, could result in gathering information about your network, or malicious entity configuration updates.

**Prerequisite:** This alert requires 9 days of history to establish entity traffic models and determine normal traffic behavior.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations to determine if the entity is intended to track network entities over SNMP, and if this behavior is malicious. If the activity is not part of planned penetration testing or otherwise intended behavior, quarantine the entity and remediate the issue. Determine if any of the entities have been affected, such as updated configuration or compromised security settings, and remediate any issues. If the entity is expected to perform SNMP sweeps, add the entity to the Scanner allowed list.



## New Unusual DNS Resolver \*

**Description:** This entity contacted a DNS resolver that it doesn't normally use. This can indicate misconfiguration or the presence of malware. For example, an attacker could cause a DNS resolver to redirect a popular website to a domain that serves additional malware.

**Prerequisite:** This alert requires 7 days of history to establish entity roles and model normal traffic.

**Associated Observations:** Unusual DNS Resolver Observations

**Next Steps:** Verify the entity's configuration to ensure that it is configured with the proper DNS settings. If so, determine what software is making the DNS lookup. Block the external IP address if the traffic is deemed malicious.

## Non-Service Port Scanner \*

**Description:** This device started scanning the local network on a port not associated with a common service. This alert uses the IP Scanner observation and may indicate that an attacker is inside the network, scanning for vulnerabilities.

**Prerequisite:** This alert requires 9 days of history to establish entity roles and model normal traffic

**Associated Observations:** IP Scanner Observation

**Next Steps:** Reference the supporting observations and investigate why the external entity is scanning the network. Determine if it is the result of penetration testing or other intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for the entity or user who owns the machine to determine what software caused the scanning activity.

## Outbound LDAP Connection Spike

**Description:** This entity is communicating with a large number of external hosts using an LDAP port. This alert may indicate a possible infected host or an internally-initiated port scan.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations and determine to which entities the source entity is sending traffic, what type of traffic, and if this is an update to the entity's



roles or responsibilities, or if this is unintended. If this is unintended, remediate the issue. Update your firewall and blocklist rules to prevent this access.

## Outbound SMB Connection Spike \*

**Description:** This entity is communicating with a large number of external hosts using SMB ports. This can indicate a possible infected host, externally-initiated abuse (e.g., a spoof attack), or an internally-initiated port scan.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations and determine to which entities the source entity is sending traffic, what type of traffic, and if this is an update to the entity's roles or responsibilities, or if this is unintended. If this is unintended, remediate the issue. Update your firewall and blocklist rules to prevent this access.

## Persistent Remote Control Connections \*

**Description:** This entity is receiving persistent connections from a new host on a remote control protocol like Remote Desktop or SSH. This may indicate that a firewall rule or ACL is overly permissive.

**Prerequisite:** This alert requires 7 days of history to establish traffic models and determine normal traffic behavior.

**Associated Observations:** New External Server Observations, Persistent External Server Observations

**Next Steps:** Adjust firewall or security group rules to prevent malicious attempts to repeatedly access the entity. Confirm that the local entity has not been breached by checking Remote Access Observations or the entity.

## Potential Data Exfiltration \*

**Description:** This entity downloaded a sizeable chunk of data from an internal entity that it doesn't communicate with regularly. Shortly after that, the entity uploaded a similar amount of data to an external entity. This may indicate an unauthorized transfer of information, or other malicious behavior.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Potential Data Forwarding Observations

**Next Steps:** Reference the supporting observation to determine the volume of traffic and the client entity to determine if the behavior is expected in the normal course of business,

such as a new scheduled backup. If it is malicious, determine what was transferred. Follow your organization's guidelines on data exfiltration.

## Potential Database Exfiltration \*

**Description:** A statistically unusual amount of data was transferred from a database server to a client. This may indicate an unauthorized transfer of information, or other malicious behavior.

**Prerequisite:** This alert requires 7 days of history to establish which entities normally serve as databases, and what their normal traffic profiles are.

**Associated Observations:** New High Throughput Connection Observations

**Next Steps:** Examine the client entity to determine if the behavior is expected in the normal course of business, such as a new scheduled backup. If it is malicious, determine what was transferred. Follow your organization's guidelines on data exfiltration.

## Protocol Forgery

**Description:** This entity was observed running a potentially restricted service (such as SSH) on a non-standard port. This can indicate evasion of security controls.

**Prerequisite:** This alert requires 1 day of history to establish entity models and see which entities use potentially restricted services. This alert also requires Encrypted Traffic Analytics capabilities.

**Associated Observations:** Insecure Transport Protocol Observations

**Next Steps:** Reference the supporting observations to determine why the entity used the unusual protocol/port combination to communicate. Update your firewall and blocklist rules to prevent further access with this protocol/port combination, if deemed a security risk.

## Protocol Violation (Geographic) \*

**Description:** This entity tried to communicate with a host in a watchlisted country on an illegal protocol / port combination (e.g., UDP on port 22).

**Prerequisites:** This alert requires 0 days of history. You must configure the Country Watchlist with at least one country.

**Associated Observations:** Bad Protocol Observations

**Next Steps:** Reference the supporting observations to determine why the entity used the unusual protocol/port combination to communicate with the entity in the watchlisted country. Determine what was transferred in the communication. If deemed malicious,

update your firewall and blocklist rules to prevent further access with this protocol/port combination, and with this geolocation, unless there is a business reason for allowing it.

### To Configure a Watchlist via an API

Currently there is no ability to configure watchlists or blocklists in the Manager. Therefore, you need to make an API call to the backend (onsite) as explained below. For example, to configure a watchlist for a country ("CN" - China in this case), the following call can be made on the Manager, which would add this country to a watchlist.



For both of the following commands, the beginning character of each line after the first line immediately follows the last character in the preceding line.

To get the API key from here:

```
cat /lancope/var/services/detections/config/api_key
```

Make a note of the key to pass into next commands.

#### 1. Enter this command:

```
curl -X POST -d '{"identifier":"US", "list_on": "watchlist"}' -v
-H 'Content-Type: application/json' -H 'Authorization: ApiKey _
customer_01-api[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

#### 2. To confirm, enter this command:

```
curl -X GET -v -H 'Content-Type: application/json' -H
'Authorization: ApiKey _customer_01-api:[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

## Remote Access (Geographic)

**Description:** This device has been accessed from a remote host in a user-supplied watchlisted country. This alert uses the Remote Access observation and may indicate a device is compromised.

**Prerequisite:** This alert requires 0 days of history. This alert requires configuring the Country Watchlist with at least one country.

**Associated Observations:** Remote Access Observation

**Next Steps:** Reference the supporting observations to identify the external entity, and how the external entity interacted with your internal entity. Determine if the behavior was malicious, and if any data was exfiltrated, as well as what actions were taken on the internal entity. If needed, add additional firewall or security group rules to prevent future access.

## To Configure a Watchlist via an API

Currently there is no ability to configure watchlists or blocklists in the Manager. Therefore, you need to make an API call to the backend (onsite) as explained below. For example, to configure a watchlist for a country ("CN"- China in this case), the following call can be made on the Manager, which would add this country to a watchlist.



For both of the following commands, the beginning character of each line after the first line immediately follows the last character in the preceding line.

To get the API key from here:

```
cat /lancope/var/services/detections/config/api_key
```

Make a note of the key to pass into next commands.

1. Enter this command:

```
curl -X POST -d '{"identifier":"US", "list_on": "watchlist"}' -v
-H 'Content-Type: application/json' -H 'Authorization: ApiKey _
customer_01-api[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

2. To confirm, enter this command:

```
curl -X GET -v -H 'Content-Type: application/json' -H
'Authorization: ApiKey _customer_01-api:[key]'
http://0.0.0.0:8086/api/v3/watchlist/listedcountry/
```

## Repeated Umbrella Sinkhole Communications \*

**Description:** This entity has established periodic connections with a Cisco Umbrella Sinkhole. This alerts uses the Umbrella Sinkhole Hit and Heartbeat observations and may indicate a device is compromised.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Heartbeat Observations, Umbrella Sinkhole Hit Observations

**Next Steps:** Reference the supporting observations and examine the affected entity and log information. Determine why the entity is establishing periodic communications to the sinkhole and remediate the situation.

## Repeated Watchlist Communications

**Description:** This entity has established periodic connections with a watchlisted IP. This may indicate the presence of malware, or a compromised entity on your network.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Watchlist Interaction Observations, Heartbeat Observations

**Next Steps:** Reference the supporting observations and examine the affected entity and log information. Determine why the entity is establishing periodic communications, and remediate the situation. As necessary, contact the organization that maintains a given watchlist, either for advice to remediate the situation, or to verify that the entity is no longer infected with malware.

## Role Violation

**Description:** This entity is identified with a particular role (e.g., User entity), but was observed acting in an atypical manner for that role (e.g., SSH server). If an entity changes roles, it may be an indication of malicious behavior, such as malware changing how an entity functions.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Role Violation Observations

**Next Steps:** Reference the supporting observations and determine whether the new role behavior is intended and part of the normal course of business. If it is not, quarantine the entity. If it is intended, snooze the alert.

## SMB Connection Spike \*

**Description:** This entity attempted to contact an unusually large number of SMB servers. This can be an indication of malware or abuse. As SMB is used primarily for file sharing, but can also be used for accessing network printers or browsing other hosts on a network, this could indicate data exfiltration or network resource misuse.

**Prerequisite:** This alert requires 9 days of history to establish entity traffic models and determine normal traffic behavior.

**Associated Observations:** IP Scanner Observations

**Next Steps:** Reference the supporting observations and determine why the entity is establishing connections with multiple SMB servers, what types of actions the entity is taking, and if this is malicious behavior. If data was exfiltrated, follow your organization's guidelines for dealing with data exfiltration. Quarantine the entity as necessary to remove malware.

## Suspected Botnet Interaction

**Description:** This entity exchanged traffic with IP addresses associated with botnets, or attempted to resolve domain names associated with botnets.

**Prerequisite:** This alert requires 1 day of history to establish entity models.

**Associated Observations:** Watchlist Interaction Observations

**Next Steps:** Quarantine the entity, and remove all malware. Update your block list and firewall rules to disallow the botnet entities from accessing your network. Reference the supporting observations and determine if any other entities on your network are also infected, based on communications that the entity may have established, and remediate as necessary.

## Suspected Cryptocurrency Activity

**Description:** Source exchanged a significant amount of traffic with multiple addresses known to be operating cryptocurrency nodes, based on Talos intelligence, and other sources. This behavior may indicate that an entity is being used to mine cryptocurrency.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Watchlist Interaction Observations

**Next Steps:** Quarantine the entity, and remove all cryptocurrency mining software, whether it is malware or installed by a user.

## Suspected Port Abuse (External)

**Description:** This entity is communicating with an external host on unusual range of ports. This can indicate externally-initiated abuse (e.g., a spoof attack) or an internally-initiated port scan.

**Prerequisite:** This alert requires 1 day of history to establish entity models.

**Associated Observations:** Port Scanner Observations, External Port Scanner Observations

**Next Steps:** Reference the supporting observations to review the entity's activity, and determine if it is consistent with planned penetration testing, or malicious behavior. Determine the origin of the malicious behavior, and remediate the issue. Update your firewall and blocklist rules as needed.

## Suspected Remote Access Tool Heartbeat \*

**Description:** Traffic with a signature matching Remote Access Tools (e.g., RevengeRAT) was seen on this device. This alert uses the Suspicious Network Activity observation and may indicate that the device is compromised.

**Prerequisites:** This alert requires 0 days of history.

**Associated Observations:** Suspicious Network Activity Observation

**Next Steps:** Ensure this device has the most recent security updates applied and investigate the device for signs of compromise.

## Suspected Zerologon RPC Exploit Attempt

**Description:** Traffic with a signature matching the Zerologon RPC exploit was seen on this device. This alert uses the Suspicious Network Activity observation and may indicate the device is being targeted for exploitation.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Suspicious Network Activity Observation

**Next Steps:** Ensure this device has the most recent security updates applied. Follow mitigation steps in reference to CVE-2020-1472.

## Suspicious SMB Activity

**Description:** Multiple new SMB servers have communicated with common SMB peers. This can be an indication of malware or abuse.

**Prerequisite:** This alert requires 14 days of history.

**Associated Observations:** Suspicious SMB Activity Observations

**Next Steps:** Reference the supporting observations to examine the entity's traffic profile to determine if there is further evidence of botnet activity or other malicious behavior. Check for other entities on your network which may be exhibiting similar behavior, and remediate it.

## Talos Intelligence Watchlist Hits

**Description:** This entity exchanged a significant amount of traffic with multiple addresses on the Cisco Talos IP Blocklist.

**Prerequisite:** This alert requires 0 days of history.

**Associated Observations:** Watchlist Interaction Observations

**Next Steps:** Quarantine the entity and remove all malware. Investigate the external IP address by selecting **Talos Intelligence** from the menu to see what the traffic indicates and take appropriate remediation actions.



## Unusual DNS Connection \*

**Description:** This entity contacted an unusual DNS resolver and then established periodic connections with a remote entity. This behavior may indicate a malicious redirect of traffic, or a malware infection on an entity.

**Prerequisite:** This alert requires 1 day of history to establish entity models.

**Associated Observations:** Unusual DNS Resolver Observations, Heartbeat Observations

**Next Steps:** Reference the supporting observations and determine if this behavior is malicious, and remove malware if it is present. Update your block list and firewall rules to disallow access.

## Unusual External Server

**Description:** This entity has repeatedly communicated with a new external server with suspicious traffic profiles. This could indicate, for example, a new piece of software that is acting as a server to an external entity, such as syslog or TeamViewer.

**Prerequisite:** This alert requires 14 days of history to establish normal traffic patterns, and determine expected external entity traffic.

**Associated Observations:** New External Server Observations, Persistent External Server Observations, Watchlist Lookup Observations, Watchlist Interaction Observations

**Next Steps:** Reference the supporting observations to examine the entity's traffic profile to determine the nature of the traffic and if it is permitted. Quarantine the entity and remove offending software. Determine if other entities on your network exhibit similar behavior, and remediate that behavior.

## Worm Propagation \*

**Description:** A previously scanned device started scanning the local IP network. This alert uses the Worm Propagation observation and may indicate that a worm is propagating itself inside the network.

**Prerequisites:** This alert requires 9 days of history.

**Associated Observations:** Worm Propagation Observation

**Next Steps:** Reference the supporting observations and investigate why the internal entities are scanning the network. Determine if it is the result of penetration testing, other intended behavior, or if it is malicious. Update your IP scanner and firewall rules to allow the traffic if it is intended. If potentially malicious, search for associated observations for



the entity or user who owns the machine to determine which software caused the scanning activity.

## Observation Descriptions

Listed below are the observation types that Secure Network Analytics can generate.

### Anomalous Profile Observation

**Description:** An entity or entities used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of entities using the profile for the first time, sending anomalous traffic).

**Prerequisite:** None.

**Associated Alerts:** Anomalous Windows Workstation Alerts

### Bad Protocol Observation

**Description:** An entity used a non-standard protocol on a standard port (e.g., UDP on port 22).

**Prerequisite:** None.

**Associated Alerts:** Protocol Violation (Geographic) Alerts

### Country Set Deviation Observation

**Description:** An entity communicated with a set of countries different from its usual one.

**Prerequisite:** None.

**Associated Alerts:** Country Set Deviation Alerts

### Exceptional Domain Controller Observation

**Description:** Domain Controller entity communicated with unusual external ports.

**Prerequisite:** None.

**Associated Alerts:** Exceptional Domain Controller Alerts

### Excessive Connections to Network Printers Observation

**Description:** An entity initiated excessive connections to network printers.

**Prerequisite:** None.

**Associated Alerts:** Excessive Connections to Network Printers Alerts

## External Port Scanner Observation

**Description:** An entity on the local network scanned (or was scanned by) a remote IP address.

**Prerequisite:** None.

**Associated Alerts:** Inbound Port Scanner Alerts, Suspected Port Abuse (External) Alerts

## Heartbeat Observation

**Description:** An entity maintained a heartbeat with a remote host.

**Prerequisite:** None.

**Associated Alerts:** Empire Command and Control Alert, Heartbeat Connection Count Alerts, Unusual DNS Connection Alerts, Meterpreter Command and Control Success, Repeated Umbrella Sinkhole Communications

## Internal Port Scanner Observation

**Description:** An entity scanned a large number of ports.

**Prerequisite:** None.

## IP Scanner Observation

**Description:** An entity scanned a large number of entities.

**Prerequisite:** None.

**Associated Alerts:** LDAP Connection Spike, NetBIOS Connection Spike Alerts, New IP Scanner Alerts, New SNMP Sweep Alerts, Outbound LDAP Connection Spike, Outbound SMB Connection Spike Alerts, SMB Connection Spike Alerts

## Multiple Access Failures Observation

**Description:** An entity had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

**Prerequisite:** None.

**Associated Alerts:** Excessive Access Attempts (External) Alerts

## Network Printer with Excessive Connections Observation

**Description:** Network printer initiated excessive connections to other entities.

**Prerequisite:** None.

**Associated Alerts:** Network Printer with Excessive Connections Alerts

## New External Server Observation

**Description:** An entity started communicating with an external server.

**Prerequisite:** None.

**Associated Alerts:** Exceptional Domain Controller Alerts, Persistent Remote Control Connections Alerts, Unusual External Server Alerts

## New High Throughput Connection Observation

**Description:** An entity has exchanged a large amount of traffic with a new host.

**Prerequisite:** None.

**Associated Alerts:** High Bandwidth Unidirectional Traffic Alerts, Potential Database Exfiltration Alerts

## New Internal Device Observation

**Description:** After not being seen in the lookback period, a new entity emerges on the network.

**Prerequisite:** None.

**Associated Alerts:** New Internal Device Alerts

## New Profile Observation

**Description:** An entity matches a profile tag (e.g., FTP server) that it hasn't matched recently.

**Prerequisite:** None.

**Associated Alerts:** Emergent Profile Alerts

## Persistent External Server Observation

**Description:** This entity has regularly communicated with the same external server (FTP, SSH, etc.).

**Prerequisite:** None.

**Associated Alerts:** Persistent Remote Control Connections Alerts, Unusual External Server Alerts

## Population Spike Observation

**Description:** A record number of IP addresses were observed communicating on the local network.

**Prerequisite:** None.

**Associated Alerts:** Network Population Spike Alerts

## Port Scanner Observation

**Description:** An entity scanned a large number of ports.

**Prerequisite:** None.

**Associated Alerts:** Internal Port Scanner Alerts

## Potential Data Forwarding Observation

**Description:** A similarly sized, and closely timed, data transfer was detected between an internal data source to this entity (the "download"), and then from this entity to an external data sink (the "upload").

**Prerequisite:** None.

**Associated Alerts:** Potential Data Exfiltration Alerts

## Record Metric Outlier Observation

**Description:** An entity sent or received a record amount of traffic.

**Prerequisite:** None.

**Associated Alerts:** Internal Connection Spike Alerts, Outbound Traffic Spike Alerts

## Remote Access Observation

**Description:** An entity was accessed from a remote source.

**Prerequisite:** None.

**Associated Alerts:** Geographically Unusual Remote Access Alerts, New Remote Access Alerts, Remote Access (Geographic) Alerts

## Role Violation Observation

**Description:** An entity has new traffic that doesn't fit its role (e.g., FTP server communicating on port 80).

**Prerequisite:** None.

**Associated Alerts:** Role Violation Alerts

## Suspicious Network Activity Observation

**Description:** Suspicious activity was detected that matches a Talos signature.

**Prerequisite:** None

**Associated Alerts:** Suspected Remote Access Tool Heartbeat

## Suspicious SMB Activity Observation

**Description:** Multiple entities have performed anomalous activity using the SMB protocol for the first time.

**Prerequisite:** None.

**Associated Alerts:** Suspicious SMB Activity Alerts

## Traffic Amplification Observation

**Description:** An entity's outbound and inbound traffic did not match the typical ratio associated with the profile it was using. This could indicate participation in an amplification attack. An amplification attack attempts to overwhelm a server with a massive amount of packets in response to a request, involving spoofed IP addresses or other identifying information. Participation in an amplification attack may also indicate that an entity has been infected with botnet malware, and is sending these packets unintentionally.

**Prerequisite:** None.

**Associated Alerts:** Amplification Attack Alerts

## Umbrella Sinkhole Hit Observation

**Description:** The entity communicated with a known Cisco Umbrella sinkhole.

**Prerequisite:** None.

**Associated Alerts:** Repeated Umbrella Sinkhole Communications Alerts

## Unusual DNS Resolver Observation

**Description:** An entity communicated with an unusual DNS resolver.

**Prerequisite:** None.

**Associated Alerts:** New Unusual DNS Resolver Alerts, Unusual DNS Connection Alerts

## Watchlist Interaction Observation

**Description:** An entity communicated with an IP address that is on a watchlist (either explicitly or implicitly via a domain name).

**Prerequisite:** None.

**Associated Alerts:** Repeated Watchlist Communications Alerts, Suspected Botnet Interaction Alerts, Suspected Cryptocurrency Activity Alerts, Talos Intelligence Watchlist Hits Alerts, Unusual External Server Alerts, User Watchlist Hit Alerts, Watchlist Hit Alerts

## Worm Propagation

**Description:** A previously scanned device started scanning the local IP network.

**Prerequisite:** None

**Associated Alerts:** Worm Propagation

# Alerts Summary

The Alerts Summary displays the alerts generated by the system according to your filter settings. It generates these alerts, representing potential malicious activity, based on an analysis of various information about your network, including the following:

- Monitored entities roles, and the observations logged for those entities
- Alert type priority
- IP scanner rules



Use Host Group Management to add known valid IP scanners to the default Network Scanners group (Host Group ID: 48). These devices should be listed by single comma separated IP or CIDR notation. By adding known scanners, you will prevent alerts from occurring when these devices scan external or internal hosts.

## Open Alerts Summary

From the main menu, choose **Monitor > Alerts**.

OR

In the Supporting Observations section on the Alert Details page, from the drop-down list for the desired device, choose **Alerts**.

*The Alerts Summary opens with a list of all the alerts related to that device.*

### Alerts Summary Overview



For more information on how to use this page, see [Investigating Alerts](#)

## Filter the Alerts Table

Refer to the following information to learn how to filter for various settings. In the top left corner of the page in the Filters field, click the ► (**Triangle Right**) icon to see the Search and the Time Range fields.

**Search** In the Search field, type the entry by which you want to filter the table. You can filter by any content that would potentially be displayed in any of the table columns, such as alert type, source type, time, etc. When finished, click **Apply** to the right of the Time Range fields.

**Time Range** To filter by date and time, click the **Select Date drop-down arrow**. You can choose from the entries in the left column or configure a custom entry. You can click the same date in both the From Date/Time and the To Date/Time calendars, or you can choose different dates. Specify the times using the scrolling lists. When finished, click

**Select range** in the lower right corner of the dialog, and then click **Apply** to the right of the Time Range fields. To exit without saving, click outside the calendars on any white space on the page.




**Set alerts by status** By clicking the desired option in this field, you can choose to view All alerts or only Open, Snoozed, Unpublished, or Closed alerts. By default, the table displays alerts that are assigned the All status.

- Snoozed alerts: When you close an alert (see [Edit Alerts Table Entries](#)), the Close Alert dialog opens. In this dialog you can specify if you want to snooze the alert for a certain period of time.
- Unpublished alerts: Unpublished alerts are alerts that Secure Network Analytics still considers to be in the experimental phase and therefore have not yet been officially published. They are Off by default. Unpublished alerts work just as other alerts do (for instance, you can snooze and close them). Additionally, changing the priority of the alert does not affect whether or not an alert is published or unpublished. However, they will behave inaccurately in single node deployments.

To know which alerts are unpublished, see [Alert Descriptions](#).

## View the Alerts Table

The following information is displayed in the Alerts table.

Field	Description
Alert	<p>The alert type that was generated.</p> <ul style="list-style-type: none"> <li>• To access the Alert Details page for an alert, click the alert. For information about the Alert Details page, see <a href="#">Alert Details</a>.</li> <li>• To see the status of an alert, hover over the  (<b>Information</b>) icon that is beside the desired alert.</li> </ul> <p>Use the Filter drop-down list to filter by a specific alert type.</p>
Source	<p>The source entity that caused the alert to be generated. To view details for an alert, hover over the  (<b>Alert</b>) icon or the  (<b>Eye</b>) icon that is beside the IP address. (If the source is associated with a minimum of one open alert, the <b>Alert</b> icon is displayed. If the source is not associated with an open alert, the <b>Eye</b> icon is displayed.)</p>



	<p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see <a href="#">Flow Search Results: Overview</a>.</li> </ul>
Time	The time the alert was last updated.
Tags	<p>A tag is any type of label or text that you add to an alert so that it can be filtered by that label or text.</p> <p>Use the Tags drop-down list to filter by a specific tag.</p>
Assignee	<p>The user assigned to the alert.</p> <p>Use the Assignee drop-down list to filter by Any Assignee or No Assignee.</p>

## Edit Alerts Table Entries

You can assign tags and users to specific alerts as well as change the status of alerts by using the drop-down lists in the Actions field (located immediately above the Alert table).

1. In the Alerts table, check the checkbox next to each alert for which you want to make one or more changes. Note that if you check multiple alerts, the changes you make will be uniformly applied to all of the alerts you selected.
2. In the Actions field, make your selection(s) from one of the following drop-down lists, one at a time:
  - Assign Tag
  - Assign User
  - Change Status


You can change the status to Open, Close, or Unsnnooze. When you close an alert, the Close Alert dialog opens. In this dialog you can specify if you want to snooze the alert for a certain period of time. If you snooze an alert and then decide you want to reopen it, choose the Unsnnooze option for that alert.

To choose more than one option at a time from a particular drop-down list, press the **Shift key** while clicking each option. To de-select a choice, click it again.


3. To save your options, click outside the drop-down list on any white space on the page.

*The applicable entries in the table change to reflect your selections.*

## View Related Configuration Pages

Click the  (**Related Config Links**) icon, located in the upper right corner of the page, and then click the appropriate option to access either the Alert Priorities Configuration page or the Alerts Country Watchlist Configuration page.

## Download a .CSV File

To download a .csv file containing either all available observations or just the current filtered view (if you have already filtered the table), click the  (**Download CSV**) icon located in the top right corner of the page and click the appropriate option.

 You can download a maximum of 65,000 records.

## Alerts Workflow

An alert's workflow is based around its status. When the system generates an alert, its default status is Open. On the Alert Details page, all open alerts are displayed by default since these are of immediate concern.

As you review the Alerts Summary, you can update their statuses as an initial triage. You can use the filters and search functionality to locate specific alerts, or you can display alerts of different statuses or those with different tags or assignees.



When you close an alert, you can set the alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove Snoozed status from an alert to display it as an open alert again.

As you review alerts, you can assign them to yourself or another user in the system. Users can search for all alerts assigned to their username.

When you click an alert on the Alerts page, you can view its details. From this page you can click an alert's associated device.

This information can help you pinpoint the actual issue, in order to further research the issue on your network, and potentially resolve malicious behavior. As you research within the Manager and on your network, you can leave comments that describe your findings on the alert. This helps create a record for your research that you can reference in the future.

If you complete your analysis, you can update the status to Closed so that it no longer appears by default as an open alert.

## Alerts FAQs

### Why are certain alerts disabled?

Certain alerts are disabled by default because only alerts that are likely to affect the broadest cross-section of customers have been enabled. Users can enable alerts per their network needs, especially as part of fine-tuning their deployment.

### What does an alert's status mean?

An alert's workflow is based around its status. When the system generates an alert, its default status is Open, and no user is assigned. On the Alerts page, all open alerts are displayed by default since these are of immediate concern.

As you review the Alerts Summary, you can assign and tag alerts as well as update their statuses as an initial triage. You can use the filters and search functionality to locate specific alerts, or you can display alerts of different statuses or those with different tags or assignees. When you close an alert, you can set the alert's status to Snoozed, in which case it does not reappear in the list of open alerts until the snooze period elapses. You can also remove the Snoozed status from an alert to display it as an open alert again.

If you complete your analysis, you can update the status to Closed so that it no longer appears by default as an open alert. You can also re-open a closed alert in the future if circumstances change.

## How does a subnet's sensitivity affect alerts?

The only subnets in Secure Network Analytics that this feature currently applies to are the following:



- 10.0.0.0/8 (Default RFC1918)
- 172.16.0.0/12 (Default RFC1918)
- 192.168.0.0/16 (Default RFC1918)
- fc00::/7 (Default RFC4193)

By default, the sensitivity type for these subnets is Medium.

A subnet's sensitivity and an alert's priority type determine when a specific alert is generated, based on that particular subnet's traffic. The alert priority type influences the degree to which subnet traffic is monitored.

Refer to the following matrix to learn which combinations of subnet sensitivity and alert priority type generate alerts for the previously mentioned subnets.

Subnet Sensitivity Status	Alert Priority Type		
	Low	Medium	High
Low	No open alert.	No open alert.	Generates an open alert.
Medium	No open alert.	Generates an open alert.	Generates an open alert.
High	Generates an open alert.	Generates an open alert.	Generates an open alert.

## Investigating Alerts

The following presents general guidelines and suggestions for how to investigate a given alert. Because Secure Network Analytics provides additional context when it logs an alert, you can use this context to help guide your investigation.



These steps are meant to be neither comprehensive, nor all-inclusive. They merely offer a general framework with which to start investigating an alert.

In general, you can take the following steps when you review an alert:

## Triage Open Alerts

It's particularly useful to triage the open alerts if more than one have yet to be investigated.

On the Alerts Summary, in the **See alerts by status** field, click **Open** to filter by Open status.

Ask the following questions:

- Have you configured this alert type as high priority?
- Did you set a high sensitivity for the affected subnet?
- Is this unusual behavior from a new entity on your network?
- What is the entity's normal role, and how does the behavior in this alert fit that role?
- Is this an exceptional deviation from normal behavior for this entity?
- If a user is involved, is this expected behavior from the user, or exceptional?
- Is protected or sensitive data at risk of being compromised?
- How severe is the impact to your network if this behavior is allowed to continue?
- If there is communication with external entities, have these entities established connections with other entities on your network in the past?
- If this is a high priority alert, consider quarantining the entity from the internet, or otherwise closing its connections, before continuing your investigation.

## Snooze an Alert

1. On the Alerts Summary, In the Alerts table, check the checkbox next to the applicable alert.
2. From the Change Status drop-down list located in the upper right corner above the table, choose **Close**.
3. In the Close Alert dialog, specify a snooze period from the drop-down list and click **Submit**.

## Unsnnooze a Snoozed Alert

When you are ready to review a snoozed alert, you can unsnooze it. This sets the alert's status to Open.

1. On the Alerts Summary, In the Alerts table, check the checkbox next to the applicable alert.
2. In the Change Status drop-down list located in the upper right corner above the table, choose **Unsnnoozed**.

## Close an Alert

When you are finished investigating an alert, you can close it.

1. On the Alerts Summary, In the Alerts table, check the checkbox next to the applicable alert.
2. In the Change Status drop-down list located in the upper right corner above the table, choose **Close**.
3. On the Alerts Summary, in the Alerts Table, confirm that the alert is indeed closed.

## Reopen a Closed Alert

If you discover additional information related to a closed alert, or want to add more comments related to that alert, you can reopen it, changing the status to Open. You can then make changes as necessary to the alert, then close it again when your additional investigation is complete.

1. Filter the Alert list to display all closed alerts.
2. Search for and click the alert you need to reopen to view its details.
3. In the Change Status drop-down list located in the upper right corner above the table, choose **Open**.

## Update an Alert


Based on your initial triage, do one or more of the following:

- On the Alerts Summary, in the Actions field (located in the upper right corner above the table), add tags to the alert. This enables you to better categorize your alerts for future identification as well as helps to establish long-term patterns in your alerts.
- At the bottom of the Alert Details page in the Comments text box, enter a comment for the alert.

## Review an Alert

If you are reviewing an assigned alert, review the alert detail to understand why Secure Network Analytics generated an alert.

To do this, do one or both of the following:

- On the Observations Dashboard, click the  (**Arrow Right**) icon next to an observation type to view all logged observations of that type.
- On the Alerts Details page, view all logged observations for this alert's source entity.

Following are some suggestions for what to review:

- Review the supporting observations to understand what these observations mean for the source. View all observations for the source to understand its general behavior and patterns, and see if this activity may be part of a longer trend.
- Review the supporting observations. Understand what these observations mean for the source entity.
- View all of the observations for the applicable source to understand its general behavior and patterns, and see if this activity may be part of a longer trend.
- From the observations, view additional context surrounding the source, including other alerts and observations it may be involved in, information about the device itself, and what type of flow traffic it is transmitting. Determine if this behavior is indicative of malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet.
- From the observations, review the context for the entities with which the source established a connection. Examine the geolocation information, and determine if any of the geolocation data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior.

## Review Supporting Observations and Contextual Details

### Source Entities

Review the supporting observations to understand what these observations mean for the source entity. Determine if the source entity behavior indicates malicious behavior. If the source entity established connections with multiple external entities, determine if the external entities are somehow related, such as if they all have similar geolocation information, or their IP addresses are from the same subnet. View additional context surrounding the source entity, including other alerts and observations it may be involved in, information about the device itself, and the type of flow traffic it is transmitting.

From an observation, you have the following options:

---

From the Device drop-down list,

- Choose **Alerts** to view all alerts related to the entity.
- Choose **Observations** to view all observations related to the entity.
- Choose **Device** to view information about the device.
- Choose **Flow Analysis** to view flow traffic related to this entity.

From the IP address or hostname drop-down list,


- Click the  (**Copy**) icon to copy the IP address or hostname.

## External Entities

From the observations, examine information about other external entities. Examine the geolocation information, and determine if any of the geolocation data identifies a malicious entity. View the traffic generated by these entities. Check whether Talos, AbuseIPDB, or Google have any information on these entities. Find the IP address on multiple days and see what other types of connections the external entity established with entities on your network. If necessary, locate those internal entities and determine if there is any evidence of compromise or unintended behavior. Review the context for the entities with which the source entity established a connection:

From an observation, you have the following options:

From the IP address or hostname drop-down list,

- Choose the  (**Copy**) icon to copy the IP address or hostname.
- Choose **Find IP on multiple days** to see the amount of traffic sent to and from the corresponding entity and the number of connections it was involved in, for the previous day, today, and the next day. If you click a date in the Day column, you can view additional traffic-related information for the associated day for that entity.
- Choose **IP Traffic** to view recent traffic information for this entity.
- Choose **Flow Analysis** to view the flow search results for this entity.
- Choose **Add IP to watchlist** to add this entity to the watchlist.
- Choose **AbuseIPDB** to view information about this entity on AbuseIPDB's website.
- Choose **Cisco Umbrella** from the IP address or hostname drop-down to view information about this entity on Cisco Umbrella's website.
- Choose **Google Search** to search for this IP address on Google.
- Choose **Talos Intelligence** to view information about this information on Talos's website.



## Examine an Entity and Associated Users

Gather additional context on the source entity and any users that may have been involved with this alert.

- Locate the log files for this entity. If it is a physical entity on your network, access the device to review the log information, and see if there is any information as to what caused this behavior. If it is a virtual entity, or stored in the cloud, access the logs and search for entries related to this entity. Examine the logs for further information on unauthorized logins, unapproved configuration changes, and the like.
- Examine the entity. Determine if you can identify malware or a vulnerability on the entity itself. See if there has been some malicious change, including if there are physical changes to a device, such as a USB stick that is not approved by your organization.
- Determine if a user on your network, or from outside your network, was involved. Ask the user what they were doing if possible. If the user is unavailable, determine if they were supposed to have access, and if a situation occurred that prompted this behavior, such as a terminated employee uploading files to an external server before leaving the company.
- Enter comments about what you find. To do this, scroll to the bottom of the Alert Details page and enter it in the Comment text box. When finished, click **Comment**.

## Remediate an Issue

If malicious behavior caused the alert, remediate the malicious behavior.

- If a malicious entity or user attempted to log in from outside your network, update your firewall rules to prevent the entity or user from accessing your network.
- If you identify a vulnerability or exploit, update or patch the affected entity to remove the vulnerability, or update your firewall settings to prevent unauthorized access. Determine if other entities on your network may similarly be affected, and apply the same update or patch to those entities. If the vulnerability or exploit currently does not have a fix, contact the appropriate vendor to let them know.
- If you identify malware, quarantine the entity and remove the malware. Determine if other entities on your network are at risk, and update the entities or your security solution to prevent this malware from spreading. Update your security intelligence with information about this malware, or the entities that caused this malware. Alert vendors as necessary.
- If malicious behavior resulted in data exfiltration, determine the nature of the data sent to an unauthorized source. Follow your organization's protocols for unauthorized data exfiltration.

- Enter comments about what you find. To do this, scroll to the bottom of the Alert Details page and enter it in the Comment text box. When finished, click **Comment**.

## Fine-Tune Your Secure Network Analytics Settings

Based on the alert and remediation, update your Secure Network Analytics settings to help identify this behavior in the future.

- Add external entities to a watchlist if they caused malicious behavior.
- Add countries to the country watchlist if multiple entities from a country caused malicious behavior.
- Update your subnet sensitivity if a particular subnet is targeted.
- Update your alert type priority settings if a specific alert becomes a concern.
- Add any known good scanners to the default Network Scanners Host Group (ID 48).

## Alert Details

 For more information on how to use this page, see [Investigating Alerts](#)

The Alert details presents an overview of the alerts reported by the system. You can search for specific text, or filter by status, tags, or assignee. You can also see all observations generated for the affected entity as well as view related device information.

The following information is displayed in the Alert Type Details section.

### Open Alert Details

On the Alerts Summary, click an alert.

*The Alert Details page for that alert opens.*

### View Alert Type Details

Field	Description
Description	A description of the alert.
Next Steps	The next steps you should take in investigating the alert.
MITRE Tactics	The MITRE tactics associated with the alert. To access the MITRE page for this tactic, either click the MITRE Tactic entry or hover your cursor over the entry and, in the pop-up window that opens, click the "See Full Details at" link.

MITRE Techniques	The MITRE techniques associated with the alert. To access the MITRE page for this technique, either click the MITRE Technique entry or hover your cursor over the entry and, in the pop-up window that opens, click the "See Full Details at" link.
Alert Type Priority	The alert priority: Low, Normal, High.

## View Alert Rule Details

In the Alert Rule Details section, you can view additional information related to the alert. The following information is displayed in the Alert Rule Details section.

Field	Description
Status	The alert status: Open, Closed, Snoozed.
ID	The alert ID number.
Updated	The time that the alert was last updated. When an existing alert accumulates new observations, the system updates this field.
Created	The time the alert was created.
Assignee	The user assigned to the alert.
Tags	A tag is any type of label or text that you add to an alert so that it can be filtered by that label or text.
Close Alert	To close the alert, click <b>Close Alert</b> .

## View descriptions for the Supporting Observations table

An alert's details display a list of observations that led to this alert being generated. You can review these for more information about the network behavior that led to this alert.



The fields displayed in this table vary depending on the alert the table is associated with.

Option Name	Description
Affected Resource	The affected resource.
Affected Resource Type	The affected resource type.
Anomaly	The type of anomaly detected.
Bytes In	Amount of traffic (in bytes) that has been received by the device for a specific point in time.
Bytes Out	Amount of traffic (in bytes) that has been sent from the device for a specific point in time.
CIDR Range	The approximate CIDR notation scanning range (the actual range may be smaller).
Connected Device	The device to which the endpoint or source established a connection.
Connected IP	The IP with which this source communicated.
Connected Ports	The port with which this port communicated.
Corresponding Ports	The ports that were used in the communication.
Data Sink IP	The IP address of the external device to which data was uploaded.
Data Sink Profile	The Local profile of the observation source (this device) when uploading to the data sink.
Data Source	The internal device from which the data was downloaded.
Data Source IP	The IP address of the internal device from which the data was downloaded.

Option Name	Description
Data Source Profile	The local profile of the observation source (this device) when downloading from the data source.
Device	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see Flow Search Results: Overview.</li> </ul>
Domain/URL	The domain/URL based on NGFW connection events or passive DNS.
Download Sec	The length of time required for the download to complete.
Download Speed bps	The download speed in bps.
Download Start	The time the download began for the external data sink.

Option Name	Description
External IP	The external IP address.
Failed Attempts	The number of times an entity has attempted to establish a connection to a device.
Heartbeat period (Seconds)	The time between heartbeats.
History Length (Days)	The number of days of history that was used to calculate the normal set.
Internal Port Set	The type of port set. For example, "connected internal" is the set of connected ports used for internal connections.
Last Active	The time that an observation was last active.
Local Device	The local device involved in the communication.
Local Port	The port over which the endpoint or source connected to the device.
Lookback Days	The number of days of history that was used to calculate the normal set.
Lost Port Sets	Ports that are no longer used on this date.
Matching Watchlists	If the watchlist is domain-based, the matching domain names are listed here.
Metric	The metric for this outlier. For example, an outlier for internal "Bytes In" indicates that the internal network traffic (where there is no internet) to the device has spiked.
New Connections	New connections on this date that weren't in the lookback period.
New Port Set	Ports that were used on this date that weren't used in the

Option Name	Description
	lookback period.
New Profile	A new device profile that differs from previous behavior.
Normal Connection Set	The connections found in the lookback period.
Normal Ports Set	The ports that were used in the lookback period.
Number of Heartbeats	The number of times the server was connected during this observed event.
Packets In	The packets received by the source.
Packets Out	The packets sent from the source.
Port	The source port used in the observed event.
Port Ranges	The device-scanned ports included in this range, and possibly others. Common targets may include web server targets.
Probability	The probability that you would see this outlier.
Profile	The role(s) associated with the endpoint or source to which the device connected.
Public Facing IP	A public IP address that was discovered on a watchlist.
Remote Device	<p>The device this source communicated with.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source.</li> </ul> <p>For information about the Device page, see <a href="#">Device Report</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Alerts</b> to access the Alerts Summary that</li> </ul>

Option Name	Description
	<p>contains a list of all the alerts related to that source.</p> <p>For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source.</li> </ul> <p>For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source.</li> </ul> <p>For information about the Flow Search Results page, see Flow Search Results: Overview.</p>
Remote IP	The IP address with which this source communicated.
Remote Port	The port with which this source communicated.
Resource	The affected resource.
Sample Size	The number of historical samples used in this calculation.
Scanned Device	The IP address or host name of the device that was scanned.
Scanned Ports	The device-scanned ports included in this range, and possibly others.
Scanner Device	The IP address or host name of the device that performed the scan.
Severity	The severity of the reported event.
Source	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p>



Option Name	Description
	<ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see Flow Search Results: Overview.</li> </ul>
Source IP	The IP of the source at the time of the observed event.
Source Port	The port of the source at the time of the observed event.
Suspect Connections	New connections to unusual external sources or that are on unusual ports.
Time	The time the observation occurred.
Time Window	The length of time during which the event was shared.
Transfer Size	The number of bytes transferred.
Upload Start	The start time of the upload to the external data sink.
Upload Sec	The duration of the upload.

Option Name	Description
Upload Speed bps	The upload speed in bps.
User	The user account associated with the observed event.
Violating Port	The port used by the source.
Violating Protocol	The network protocol used by the source (for example, TCP).
Violating Type	The type of violation.

## Other Pages You Can Access from the Alert Details Page

### Alert Priorities Configuration

To access the Alerts Priorities Configuration page, click the **"Go to Alert Priorities page"** link at the bottom of the Alert Type Details section.

*The Alert Priorities Configuration page opens.*

### Flow Search Results

To access the Flow Search results page for a particular time displayed in the Supporting Observations table, click the applicable entry in the Time column.

OR

From the Supporting Observations table, click the drop-down list for the applicable device, and from the menu that is displayed, choose **Flow Analysis**.

*The Flow Search Results page opens.*

For information about the Flow Search Results page, see Flow Search Results: Overview.

### Device Report

To access the Device Report for a particular device displayed in the Supporting Observations table, click the drop-down list for the applicable device, and from the menu that is displayed, choose **Device**.

*The Device Report opens.*

For information about the Device page, see [Device Report](#).

## Alerts Summary

To access the Alerts Summary that contains a list of all the alerts related to a particular device displayed in the Supporting Observations table, click the drop-down list for the applicable device, and from the menu that is displayed, choose **Alerts**.

*The Alerts Summary opens, filtered by that device.*

For information about the Alerts Summary, see [Alerts Summary](#).

## Observations by Device

To access the Observations by Device page that contains a list of all observations related to a particular device displayed in the Supporting Observations table, click the drop-down list for the applicable device, and from the menu that is displayed, choose **Observations**.

*The Observations by Device page opens, filtered by that device.*

For information about the Observations by Device page, see [Observations by Device](#).

## Enter Comments for an Alert

1. In the Comments text box at the bottom of the page, enter any applicable comments.
2. Click **Comment**.

## Device Report

The Device Report provides behavioral information about an entity within your network.

- To view additional context about an alert, access the Device Report from the Alert Details page.
- To view additional context about an observation, access this report from one of the Observation pages listed in the next section.

## Open Device Report

On any of the following pages, click the drop-down list for the desired device displayed in the applicable table, and from the menu that is displayed, choose **Device**.

- Alert Details
- Observation Highlights
- Observations by Device
- Selected Observations


*The Device Report opens.*

---

## Device Report Overview

Refer to the following sections to learn what you can view on this page.

### Device Outline

In this section on the left side of the page, you can view general information about the device, such as data for the current day and Cisco Secure Cloud Analytics generated data. Click the  (**Copy**) icon beside an entry to copy it to the clipboard.

### Alerts

In the Alerts section in the upper right section of the page, you can see at a glance the number of open alerts, closed alerts, observations, total connections, and total traffic.

- If you click the Open or Closed number, the [Alerts Summary](#) opens, displaying all open alerts or all closed alerts (depending on which number you clicked) associated with this device.
- If you click the Observations number, the [Observations by Device](#) page opens, listing the observations associated with this device.

### History

The History line graph displays the amount of traffic sent to and from an entity and the number of connections it was involved in, per 1-day intervals. Hover your cursor over points in the graph to view details about the entity's traffic for that day.

### Edit Time Range

By default, the Summary, Traffic, Traffic Connections Visualization, Profiling, and IPs tabs display information for the current day. However, you can also choose to view information for a day in the past. To do this, complete the following steps.

1. From the **Selected Date** dropdown list located immediately under the History graph, use the left and right arrows to navigate to the desired month.
2. Click the desired date.
3. Click **Select Date**.
4. Click **Apply**, which is located on the right side of the Selected Date section.

### Summary

The Summary tab displays an overview of the entity's model that is stored by the system. Refer to the following table for descriptions of the fields displayed on the Summary tab.

#### Entity Summary Fields


Field	Description
<b>Attendance</b>	
Normally Active	The time period during which this entity is normally active.
IP Addresses	The IP addresses associated with the entity.
<b>Connectivity</b>	
Connections	The number of connections this entity was involved in.
Internal Connections	The number of connections with internal entities this entity was involved in.
External Connections	The number of connections with external entities this entity was involved in.
<b>Top Internal Connections</b>	
Top Internal Connections	Up to the top 5 internal entities with which the entity established connections, based on total traffic transmitted.
<b>Top External Connections</b>	
Top External Connections	Up to the top 5 external entities with which the entity established connections, based on total traffic transmitted.
<b>Traffic</b>	
Bytes In	The amount of traffic that the entity received.
Bytes Out	The amount of traffic that the entity sent.
Bytes Total	The amount of traffic that the entity transmitted in total.
<b>Traffic Internal</b>	
Bytes In	The amount of traffic that the entity received from internal entities.

Bytes Out	The amount of traffic that the entity sent to internal entities.
<b>Traffic External</b>	
Bytes In	The amount of traffic that the entity received from external entities.
Bytes Out	The amount of traffic that the entity sent to external entities .
<b>DNS Names</b>	
DNS Names	DNS domain names associated with the entity.
<b>Roles</b>	
Roles	The roles associated with this entity.
<b>Profiles</b>	
Profiles	The percentage of time that the entity acted corresponding to the listed profile.

## Traffic

The Traffic line graph displays the amount of traffic sent to and from an entity and the number of connections it was involved in, per 10-minute intervals. You can also view information about the connections with which the entity was involved.

- Hover your pointer over areas on the various lines in the Traffic graph to view details on the entity's traffic for that 10-minute interval.
- To filter the graph, you have the following options:
  - Click **All** to view information about all entities with which this entity established a connection.
  - Click **Internal** to view information about internal entities with which this entity established a connection.
  - Click **External** to view information about external entities with which this entity established a connection.

To export the results on the Traffic tab to a CSV file, click the  **(Download CSV)** icon, located above the following table in the upper right corner.

Refer to the following table for descriptions of the fields displayed on the Traffic tab.

### Entity Traffic Fields

Field	Description
Connected IP	The IP address that this entity established a connection with.
Hostname/PDNS Record	The hostname for this IP address, if available.
Bytes In	The bytes received by the entity from the connected entity.
Bytes Out	The bytes sent by the entity to the connected entity.
Bytes Total	The total bytes transmitted by the entity in this connection.
First Connection	The time of the first connection with the connected IP on this day.
Last Connection	The time of the last connection with the connected IP on this day.
See Conversation in Flow Analysis (Ellipsis icon)	In the last column, click the <b>⋮ (Ellipsis)</b> icon > <b>See Conversation in Flow Analysis</b> to access the associated flow search results.

## IPs

The IPs tab displays a list of the IPs associated with the device for each associated date as well as a consolidated list of all IPs associated with the device for the last 30 days. It also provides the date that each of these IPs was last active in association with the device.

Field	Description
IPs	The IP associated with the device.
Last Active	The date that the IP was last active in association with the device.

# Roles

Use this page to view a list of all roles (in the Active Roles table), along with at least one associated device for each role, that were active on your system for a specific time frame. The entries that are displayed in the Active Roles table depend on the telemetry types your system is ingesting. You can also view a list of all roles that are currently inactive on your system (the Inactive Roles table). The default time frame for both tables is the last 7 days, though you can set the time frame to a maximum of 90 days.



- You can see the Roles page only if you've enabled Analytics.
- The following roles will always be inactive in Cisco Secure Network Analytics (and therefore will always be listed in the Inactive Roles table):
  - AWS
  - Azure
  - GCP
  - Any other Cloud telemetry-related roles

## Open the Roles page

From the main menu, choose **Investigate > ASSETS Roles**.

*The Roles page opens.*

## Set the time frame

The time frame for the results defaults to the last 7 days. To configure a different time frame, complete the following steps:

1. In the Active Dates section located above the Active Roles table, click either one of the text boxes.

*The From Date/Time and To Date/Time calendars open.*

2. Click the desired date in each calendar. The days between those two dates will be highlighted in light blue. Alternatively, you can click one of the time range options located on the left side of the dialog.
3. You can change the times by using the scrolling lists located above each of the two calendars.
4. When finished, click **Select range**. If you need to cancel without saving, click anywhere outside the Calendars dialog.



## View the results

To view the matching devices for a role, click the row in which the role name is listed in the Active Roles table. The + (**Add**) icon beside that role name switches to the ✕ (**Large X**) icon, the row becomes highlighted in blue, and the matching sources and role names for this role are added to a table that opens to the right.


Each time you click a role name to view its matching sources and role names, the matching sources and role names for previous selections continue to be displayed. To remove matching resources and role names for a role, click the row in which the role name is listed in the Active Roles table. The **Large X** icon beside that role name switches back to the **Add** icon.

To view details about a matching source, hover your cursor over the 🔴 (**Alert**) icon or the 👁 (**Eye**) icon that is beside the applicable source. (If the source is associated with a minimum of one open alert, the **Alert** icon is displayed. If the source is not associated with an open alert, the **Eye** icon is displayed.)

If you click the menu to the right of a matching source IP address, you can choose from several options to access the following pages:

Choose...	To access this page...
Device	Device Report. In the Roles section you will see the roles associated with the device, and in the Profiles section you will see the processes or protocols associated with the roles.
Alerts	Alerts Summary
Observations	Observations by Device
Flow Analysis	Flow Search Results

## Export results

To export the results on this page to a CSV file, click the  (**Download CSV**) icon, located in the upper right corner of the page.

# Observations Dashboard



- For information about the Observation Types page, see [Observation Types](#).
- For information about the Observations by Device page, see [Observations by Device](#).
- For information about the Selected Observations page, see [Selected Observations](#).

## Open Observations Dashboard

From the main menu, choose **Monitor > Observations**.

*The Observations Dashboard opens.*

## Observations Highlights Overview

Observations are facts about an entity's behavior on the network, such as a heartbeat connection with an external IP address, an interaction with an entity on a watchlist, or a remote access session established with another entity. Observations on their own do not carry meaning beyond the fact of what they represent. A typical customer may have many thousands of observations and a few alerts.

Alerts are generated from combinations of observations; observations in isolation do not necessarily constitute malicious behavior. The recent observations, by themselves, do not necessarily mean there is malicious behavior on your network. Review your alerts for a better picture of the potential malicious behavior.

As the system inspects your traffic, it logs observations, or facts, about the entities on your network. Because observations are logged per entity, your network may generate more observations than can be reasonably reviewed. The system presents a subset of the most notable observations logged for your network. You can review and filter these to gain a better understanding of the types of behavior that may result in alerts being generated.




A high number of observations does not necessarily correspond with a high number of alerts, or even any alerts. For example, an entity with many observations may be passing a large amount of varied traffic, but Dynamic Entity Modeling may have identified this behavior as normal and expected for this entity. Similarly, a low number of observations does not necessarily correspond with a lack of alerts. For example, if the only activity detected for an entity is a continual attempt to log into a server with improper credentials, this may




generate a relatively small number of observations, and an alert noting the multiple failed login attempts.

## View Observations Highlights

You can drill down and view all observations of that type. If you drill down, the system opens a new tab on this page that displays those observations. If you select a different observation type to drill down into, the system updates that new tab with these observations.

- To view all observations of a specific type, click the  (**Arrow Right**) icon next to the applicable observation type.

*The Selected Observations page opens, which by default displays a table that contains all observations of the type you selected that have occurred within the last 24 hours. For more information about the Selected Observations page, see [Selected Observations](#).*

- To download a .csv file containing all observations for a specific type, click the  (**Download CSV**) icon located at the top right corner of the associated table.

## View Descriptions for the Observations Highlights tables



The fields displayed in these tables vary depending on the observation each table is associated with.

Option Name	Description
Affected Resource	The affected resource.
Affected Resource Type	The affected resource type.
Anomaly	The type of anomaly detected.
Bytes In	Amount of traffic (in bytes) that has been received by the device for a specific point in time.
Bytes Out	Amount of traffic (in bytes) that has been sent from the

Option Name	Description
	device for a specific point in time.
CIDR Range	The approximate CIDR notation scanning range (the actual range may be smaller).
Connected Device	The device to which the endpoint or source established a connection.
Connected IP	The IP with which this source communicated.
Connected Ports	The port with which this port communicated.
Corresponding Ports	The ports that were used in the communication.
Data Sink IP	The IP address of the external device to which data was uploaded.
Data Sink Profile	The Local profile of the observation source (this device) when uploading to the data sink.
Data Source	The internal device from which the data was downloaded.
Data Source IP	The IP address of the internal device from which the data was downloaded.
Data Source Profile	The local profile of the observation source (this device) when downloading from the data source.
Device	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source.</li> </ul> <p>For information about the Device page, see <a href="#">Device Report</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Alerts</b> to access the Alerts Summary that</li> </ul>

Option Name	Description
	<p>contains a list of all the alerts related to that source.</p> <p>For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source.</li> </ul> <p>For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</p> <ul style="list-style-type: none"> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source.</li> </ul> <p>For information about the Flow Search Results page, see Flow Search Results: Overview.</p>
Domain/URL	The domain/URL based on NGFW connection events or passive DNS.
Download Sec	The length of time required for the download to complete.
Download Speed bps	The download speed in bps.
Download Start	The time the download began for the external data sink.
External IP	The external IP address.
Failed Attempts	The number of times an entity has attempted to establish a connection to a device.
Heartbeat period (Seconds)	The time between heartbeats.
History Length (Days)	The number of days of history that was used to calculate the normal set.

Option Name	Description
Internal Port Set	The type of port set. For example, "connected internal" is the set of connected ports used for internal connections.
Last Active	The time that an observation was last active.
Local Device	The local device involved in the communication.
Local Port	The port over which the endpoint or source connected to the device.
Lookback Days	The number of days of history that was used to calculate the normal set.
Lost Port Sets	Ports that are no longer used on this date.
Matching Watchlists	If the watchlist is domain-based, the matching domain names are listed here.
Metric	The metric for this outlier. For example, an outlier for internal "Bytes In" indicates that the internal network traffic (where there is no internet) to the device has spiked.
New Connections	New connections on this date that weren't in the lookback period.
New Port Set	Ports that were used on this date that weren't used in the lookback period.
New Profile	A new device profile that differs from previous behavior.
Normal Connection Set	The connections found in the lookback period.
Normal Ports Set	The ports that were used in the lookback period.
Number of Heartbeats	The number of times the server was connected during this observed event.

Option Name	Description
Packets In	The packets received by the source.
Packets Out	The packets sent from the source.
Port	The source port used in the observed event.
Port Ranges	The device-scanned ports included in this range, and possibly others. Common targets may include web server targets.
Probability	The probability that you would see this outlier.
Profile	The role(s) associated with the endpoint or source to which the device connected.
Public Facing IP	A public IP address that was discovered on a watchlist.
Remote Device	<p>The device this source communicated with.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source.</li> </ul>

Option Name	Description
	For information about the Flow Search Results page, see Flow Search Results: Overview.
Remote IP	The IP address with which this source communicated.
Remote Port	The port with which this source communicated.
Resource	The affected resource.
Sample Size	The number of historical samples used in this calculation.
Scanned Device	The IP address or host name of the device that was scanned.
Scanned Ports	The device-scanned ports included in this range, and possibly others.
Scanner Device	The IP address or host name of the device that performed the scan.
Severity	The severity of the reported event.
Source	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source.</li> </ul>



Option Name	Description
	<p>For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</p> <ul style="list-style-type: none"><li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source.</li></ul> <p>For information about the Flow Search Results page, see Flow Search Results: Overview.</p>
Source IP	The IP of the source at the time of the observed event.
Source Port	The port of the source at the time of the observed event.
Suspect Connections	New connections to unusual external sources or that are on unusual ports.
Time	The time the observation occurred.
Time Window	The length of time during which the event was shared.
Transfer Size	The number of bytes transferred.
Upload Start	The start time of the upload to the external data sink.
Upload Sec	The duration of the upload.
Upload Speed bps	The upload speed in bps.
User	The user account associated with the observed event.
Violating Port	The port used by the source.
Violating Protocol	The network protocol used by the source (for example, TCP).
Violating Type	The type of violation.

# Observation Types


## Open Observation Types

1. From the main menu, choose **Monitor > Observations**.
2. On the Observations dashboard, choose **Types** from the Observations side menu.

*The Observation Types page opens.*

## View Observation Types

To read an observation type description, do the following:

Click the  (**Arrow Right**) icon next to the observation type you want to view.

*The Selected Observations page opens, which by default displays a table that contains all observations of the type you selected that have occurred within the last 24 hours. For more information about the Selected Observations page, see [Selected Observations](#).*

The Observation Types lists all of the types of observations that the system can log, along with a description, and a count of how many of that observation it has logged.

You can drill down and view all observations of that type. If you drill down, the system opens a new tab on this page that displays those observations. If you select a different observation type to drill down into, the system updates that new tab with these observations.

# Observations by Device

## Open Observations by Device

1. From the main menu, choose **Monitor > Observations**.
2. On the Observations dashboard, choose **By Device** from the Observations side menu.

OR

In the Supporting Observations table on the Alert Details page, from the drop-down list for the desired device, choose **Observations**.

*The Observations by Device page opens with a list of all observations related to that device.*

## View Observations by Device

You can use this page to view the devices that have the most observations associated with them.

Field	Description
Device	<p>The endpoint or source associated with the observation.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"><li>• Choose <b>Device (Network)</b> to access the Device Report filtered by the source.</li></ul> <p>For information about the Device page, see <a href="#">Device Report</a>.</p> <ul style="list-style-type: none"><li>• Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source.</li></ul> <p>For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</p> <ul style="list-style-type: none"><li>• Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source.</li></ul> <p>For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</p> <ul style="list-style-type: none"><li>• Choose <b>Flow Analysis</b> to access the Flow Search</li></ul>

---

	<p>Results page that contains flow information related to the source.</p> <p>For information about the Flow Search Results page, see <a href="#">Flow Search Results: Overview</a>.</p>
Count	The number of observations that have occurred for the associated device.
Time	The time at which the system last logged an observation for the associated device.

# Selected Observations

## Open Selected Observations

1. From the main menu, choose **Monitor > Observations**.
2. On the Observations dashboard, choose **Selected Observation** from the Observations side menu.

*The Selected Observations page opens.*

## View Selected Observations

You can view all observations of a given type from the Selected Observation window. This allows you to review the observations that Secure Network Analytics is logging based on your network traffic. All observations that have occurred within the last 24 hours are displayed (though you can change this time range using the Time field).

To view selected observations, do the following:

1. Click the ► (**Triangle-Right**) icon to expand the Filters pane at the top of the page.
2. From the Observation Type drop-down list, select an **Observation Type**.
3. Enter a filter value in the **Search** field.
4. To set the time range, click the **Time** drop-down arrow. Time is displayed according to your browser's time zone.

*The Calendar dialog displays.*

If you want to use a pre-defined time range, choose the applicable option from the menu in the left panel.

If you want to define a custom time range, you can do one of the following:

- a. In the From Date/Time section, use the spin list to choose a desired start date.
- b. In the To Data/Time section, use the spin list to choose a desired end date. The days between those two dates will be highlighted in gray.
- c. Click **Select range** to save your changes.



The fields displayed in this table vary depending on the observation the table is associated with.

## View descriptions for the Selected Observations table

Option Name	Description
Affected Resource	The affected resource.
Affected Resource Type	The affected resource type.
Anomaly	The type of anomaly detected.
Bytes In	Amount of traffic (in bytes) that has been received by the device for a specific point in time.
Bytes Out	Amount of traffic (in bytes) that has been sent from the device for a specific point in time.
CIDR Range	The approximate CIDR notation scanning range (the actual range may be smaller).
Connected Device	The device to which the endpoint or source established a connection.
Connected IP	The IP with which this source communicated.
Connected Ports	The port with which this port communicated.
Corresponding Ports	The ports that were used in the communication.
Data Sink IP	The IP address of the external device to which data was uploaded.
Data Sink Profile	The Local profile of the observation source (this device) when uploading to the data sink.
Data Source	The internal device from which the data was downloaded.
Data Source IP	The IP address of the internal device from which the data

Option Name	Description
	was downloaded.
Data Source Profile	The local profile of the observation source (this device) when downloading from the data source.
Device	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see Flow Search Results: Overview.</li> </ul>
Domain/URL	The domain/URL based on NGFW connection events or passive DNS.
Download Sec	The length of time required for the download to complete.
Download Speed bps	The download speed in bps.

Option Name	Description
Download Start	The time the download began for the external data sink.
External IP	The external IP address.
Failed Attempts	The number of times an entity has attempted to establish a connection to a device.
Heartbeat period (Seconds)	The time between heartbeats.
History Length (Days)	The number of days of history that was used to calculate the normal set.
Internal Port Set	The type of port set. For example, "connected internal" is the set of connected ports used for internal connections.
Last Active	The time that an observation was last active.
Local Device	The local device involved in the communication.
Local Port	The port over which the endpoint or source connected to the device.
Lookback Days	The number of days of history that was used to calculate the normal set.
Lost Port Sets	Ports that are no longer used on this date.
Matching Watchlists	If the watchlist is domain-based, the matching domain names are listed here.
Metric	The metric for this outlier. For example, an outlier for internal "Bytes In" indicates that the internal network traffic (where there is no internet) to the device has spiked.
New Connections	New connections on this date that weren't in the lookback period.



Option Name	Description
New Port Set	Ports that were used on this date that weren't used in the lookback period.
New Profile	A new device profile that differs from previous behavior.
Normal Connection Set	The connections found in the lookback period.
Normal Ports Set	The ports that were used in the lookback period.
Number of Heartbeats	The number of times the server was connected during this observed event.
Packets In	The packets received by the source.
Packets Out	The packets sent from the source.
Port	The source port used in the observed event.
Port Ranges	The device-scanned ports included in this range, and possibly others. Common targets may include web server targets.
Probability	The probability that you would see this outlier.
Profile	The role(s) associated with the endpoint or source to which the device connected.
Public Facing IP	A public IP address that was discovered on a watchlist.
Remote Device	<p>The device this source communicated with.</p> <p>Click the drop-down list to access the following options:</p> <ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source.</li> </ul> <p>For information about the Device page, see <a href="#">Device Report</a>.</p>

Option Name	Description
	<ul style="list-style-type: none"> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see Flow Search Results: Overview.</li> </ul>
Remote IP	The IP address with which this source communicated.
Remote Port	The port with which this source communicated.
Resource	The affected resource.
Sample Size	The number of historical samples used in this calculation.
Scanned Device	The IP address or host name of the device that was scanned.
Scanned Ports	The device-scanned ports included in this range, and possibly others.
Scanner Device	The IP address or host name of the device that performed the scan.
Severity	The severity of the reported event.
Source	<p>The associated endpoint or source.</p> <p>Click the drop-down list to access the following options:</p>

Option Name	Description
	<ul style="list-style-type: none"> <li>Choose <b>Device (Network)</b> to access the Device Report filtered by the source. For information about the Device page, see <a href="#">Device Report</a>.</li> <li>Choose <b>Alerts</b> to access the Alerts Summary that contains a list of all the alerts related to that source. For information about the Alerts Summary, see <a href="#">Alerts Summary</a>.</li> <li>Choose <b>Observations</b> to access the Observations by Device page that contains a list of all observations related to the source. For information about the Observations by Device page, see <a href="#">Observations by Device</a>.</li> <li>Choose <b>Flow Analysis</b> to access the Flow Search Results page that contains flow information related to the source. For information about the Flow Search Results page, see Flow Search Results: Overview.</li> </ul>
Source IP	The IP of the source at the time of the observed event.
Source Port	The port of the source at the time of the observed event.
Suspect Connections	New connections to unusual external sources or that are on unusual ports.
Time	The time the observation occurred.
Time Window	The length of time during which the event was shared.
Transfer Size	The number of bytes transferred.
Upload Start	The start time of the upload to the external data sink.
Upload Sec	The duration of the upload.

---

Option Name	Description
Upload Speed bps	The upload speed in bps.
User	The user account associated with the observed event.
Violating Port	The port used by the source.
Violating Protocol	The network protocol used by the source (for example, TCP).
Violating Type	The type of violation.

# Configuring Priorities



- For information about the Alerts Expiration Configuration page, see [Configuring Expiration](#).
- For information about the Alerts Country Watchlist Configuration page, see [Configuring Country Watchlist](#).

For information about alert statuses, see [Alerts FAQs](#).

## Open Alerts Priorities Configuration

From the main menu, choose **Configure > DETECTION Alerts**.

OR

On the Alert Details page, at the bottom of the Alert Types Details section, click the **"Go to Alert Priorities page"** link.


*The Alert Priorities Configuration page opens.*



## Configure Alert Priorities

Refer to the following table for descriptions of the fields that appear on this page.



For more information about alerts, see [Alerts FAQs](#).

Field	Description
Alert Type	Click the  ( <b>Filter</b> ) icon and choose one of these options by which you want to filter the alerts: Contains, Starts with, Ends with.
History	The number of days of data collection required to generate the alert type (also known as "soak time").
Priority	Alerts default to Low or Normal. The alert priority is determined by alert type. From the Priority drop-down list, you can configure any alert type to be Low, Normal, or High. You can also filter the Alert Settings page by priority using the <b>Filter</b> icon in the Priority column header. If no activity occurs for that

	<p>alert after 14 days, the alert automatically closes.</p> <p>Changing the priority does not affect whether or not an alert is published or unpublished. For more information about unpublished alerts, see the "Filter the Alerts Table" section in <a href="#">Alerts Summary</a>.</p>
Enabled	<p>To enable an alert, click the  (<b>Toggle</b>) icon so that the bar displays in blue (.</p>
Telemetry	<p>The Telemetry column shows the telemetry sources for your alerts. Some may have one or more telemetry sources, which are a union of telemetry sources from the observations, roles, etc. The alert fires only if your environment has integrated and is consuming that telemetry source.</p>
MITRE ATT&CK Tactics	<p>The MITRE tactics associated with the alert. To access the MITRE page for this tactic, either click the MITRE Tactic entry or hover your cursor over the entry and, in the pop-up window that opens, click the "See Full Details at" link.</p>
MITRE ATT&CK Techniques	<p>The MITRE techniques associated with the alert. To access the MITRE page for this technique, either click the MITRE Technique entry or hover your cursor over the entry and, in the pop-up window that opens, click the "See Full Details at" link.</p>

# Configuring Expiration

## Open Alerts Expiration Configuration

1. From the main menu, choose **Configure > DETECTION Alerts**.

*The Alert Priorities Configuration page opens.*

2. On the Alert Priorities Configuration page, choose **Expiration** from the Settings side menu.

*The Alerts Expiration Configuration page opens.*

## Configure Alert Expiration Days

Use the **Days before alerts expire** drop-down list to specify the number of days an alert remains in any given table before it is tagged as expired.

# Configuring Country Watchlist

## Open Alerts Country Watchlist Configuration

1. From the main menu, choose **Configure > DETECTION Alerts**.



*The Alert Priorities Configuration page opens.*

2. On the Alert Priorities Configuration page, choose **Country Watchlist** from the Settings side menu.

*The Alerts Country Watchlist Configuration page opens.*

## View Watched Countries

Use the Country Watchlist to trigger alerts for any countries that are listed on this page.

For each country that you want to add to the Country Watchlist, click its  (**Toggle**) icon so that the bar displays a blue bar ().

To revert to the default settings for all priorities, click **Reset All to Default** located in the upper right corner of the page.



# Troubleshooting

Use the following troubleshooting information as needed.

## Analytics jobs are lagging

In both of the following instances, the "Analytics performance has degraded" system alarm will be triggered.

### The secondary Manager has been promoted to primary Manager

When you change the role of the primary Manager to that of the secondary Manager, and more than 5 hours has passed before the original primary Manager has been recovered and re-assigned to the primary role, the "Analytics performance has degraded" system alarm will be triggered. Analytics will recover and run the jobs that occurred during the last 6 hours, while the original primary Manager was down. Job performance will continue to lag until your system has processed all jobs from the last 6 hours and begins to process jobs in real time.

### An appliance went down due to degradation

If your system is experiencing degradation (which is usually due to insufficient resources such as CPU or memory), jobs will begin to lag. If this lag exceeds 5 hours, then the "Analytics performance has degraded" system alarm will be triggered. At this point, results will be incomplete and unreliable.

A possible cause for this failure is that you have increased the flows per second beyond what is supported in your setup. To resolve this, either reduce the flows per second or increase the resources on the Manager, the Data Store, or both. If you cannot resolve the issue, contact [Customer Support](#).

# Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: [tac@cisco.com](mailto:tac@cisco.com)
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:  
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

## Change History

Document Version	Published Date	Description
2_1	Feb 2023	Initial version.
2_2	May 2023	Further clarified who can enable and disable Analytics. Removed the "ISE Session Started" observation as an available observation.

---

# Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)