



Cisco Secure Cloud Analytics

On-Premises Device, Hostname, and IP Mapping



Table of Contents

Introduction	3
Overview	3
Hostname Resolution in Secure Cloud Analytics	3
Overlapping Subnets	4
Definitions	4
On-Premises Device and Hostname Mapping	5
Environments with No Available Hostname Information	5
Environments with Hostname Information	5
Note on Hostname Matching	6
Environments with NVM	6
Environments with ISE	7
Environments with Cisco Meraki	7
Cisco Meraki Integration using Secure Cloud Analytics	7
Cisco Meraki Integration using Cisco XDR	7
FAQ	8
Additional Resources	9
Contacting Support	10
Change History	11

Introduction

Overview

Secure Cloud Analytics tracks a logical device's behavior over time, known as a Device, and uses various techniques to correlate network traffic to these logical devices over time. However, particularly in an on-premises environment, there are limits to how well Secure Cloud Analytics can associate traffic to a Device. This document describes the behavior, consequences, and limits of on-premises Device, hostname, and IP address mapping in Secure Cloud Analytics.



This document only describes Device behavior and hostname resolution in Secure Cloud Analytics. This information does not apply to Cisco XDR Devices.

Hostname Resolution in Secure Cloud Analytics

Secure Cloud Analytics primarily gathers telemetry for on-premises environments through NetFlow using the Secure Cloud Analytics sensor, Cisco Telemetry Broker (CTB), or the Cisco Meraki integration with Cisco XDR. Secondly, Secure Cloud Analytics can get hostname resolution through:

- active hostname resolution using reverse DNS lookups and optional SMB queries using the Secure Cloud Analytics sensor.
- Cisco Identity Services Engine (ISE) integration using the Secure Cloud Analytics sensor.
- the Secure Cloud Analytics Meraki integration.
- the Network Visibility Module (NVM), with additional caveats.

NetFlow has IP addresses without hostname information. Without hostname information, it assumes each [internal IP address](#) seen is a Device as it has no further information to make a more intelligent Device association.

In a case where hostname collection is configured, Secure Cloud Analytics will use hostnames, when seen, to tie it to an internal representation of a Device. This allows Secure Cloud Analytics to group multiple IP addresses over time to one Device.

NVM telemetry can be optionally configured as part of Cisco XDR. This telemetry source provides a NetFlow-like data feed, but also provides endpoint information with unique identifiers. The way Secure Cloud Analytics leverages this information has the net effect of Device tracking behaving similarly to the case where hostname collection is enabled on the Secure Cloud Analytics sensor.

All of these setups have limitations based on the available telemetry.



Secure Cloud Analytics assumes the nature of IP address and hostname mappings is a many-to-one relationship (many IPs can map to one hostname). One logical device can have multiple IPs simultaneously (for example, two physical interfaces or IPv4 and IPv6). Due to the nature of the monitoring, Secure Cloud Analytics cannot assume to have all relationships of the actual network at any given moment in time.

Overlapping Subnets

If a single Secure Cloud Analytics portal is monitoring multiple on-premises subnets simultaneously, Secure Cloud Analytics cannot distinguish between the same IP seen in each of them and will over-correlate IPs to Devices. Hostname availability will not improve this situation. To avoid this, we suggest configuring multiple Secure Cloud Analytics portals with one monitoring each subnet. Another option is to configure the Cisco Meraki Integration using Cisco XDR to use the [namespace](#) isolation feature provided with this integration.

Definitions

Internal IP address: Secure Cloud Analytics considers IP addresses either internal or external, and this is configurable using the subnet settings. Subnets for on-premises default to the RFC internal subnets (RFC1918 and RFC4193), but subnets can be added or removed. For more information, see the Secure Cloud Analytics [Subnet Configuration Guide](#).

Namespace: Additional information that is used to label NetFlow and Devices seen from different observation points, allowing [Overlapping Subnets](#) without overlapping IP issues.

On-Premises Device and Hostname Mapping

Environments with No Available Hostname Information

As a side effect of the limited telemetry information, the system can come to an incorrect understanding of a Device's history. One scenario is when IPs are dynamically assigned, Secure Cloud Analytics does not have a way to know that the underlying logical device has changed. For example, a laptop on WiFi leaves, and the IP is assigned to a new laptop. In the absence of hostname or other identifying information, the system will associate the activities of multiple logical devices to one Device. This can lead to confusing device profile information.

```
Actual situation
#   t0   t1   t2   t3
# ip1 d1---- d2---
```

As seen by Secure Cloud Analytics

```
#   t0   t1   t2   t3
# ip1 d1-----
```

On the flip side, in cases where one logical device has more than one IP address (for example, two physical interfaces or IPv4 and IPv6), there is no information with which we can reliably tie these to the same Device, so Secure Cloud Analytics shows them as two separate Devices.

```
Actual situation
#   t0   t1   t2   t3
# ip1 d1-----
# ip2 d1-----
```

As seen by Secure Cloud Analytics

```
#   t0   t1   t2   t3
# ip1 d1-----
# ip2 d2-----
```

Environments with Hostname Information

Where Secure Cloud Analytics can see hostname information, the system has the ability to associate more than one IP address with one Device. However, there are still limits to what the system can reliably determine. This can lead to over-correlation of IPs to Devices in the system.

If a Device has an IP to hostname association in Secure Cloud Analytics, and then the logical device changes IP address, the telemetry will eventually reflect the new IP to

hostname mapping. However, because of the potential for this to be a many-to-one relationship, Secure Cloud Analytics cannot safely assume the previously seen IP is no longer associated with the hostname (and thus the Device). It could, for example, be a separate physical interface to the same logical device. So Secure Cloud Analytics will keep both the previously seen IPs, along with the most recently seen IP, until telemetry is seen that positively maps the IP address to a different hostname. At this point we will 'expire' the mapping, and it will just be listed as a previous IP address. There is no way to tell the system to break an association 'early'.

Actual situation, where t3 is when ip1 gets used by a new hostname

```
#   t0   t1   t2   t3   t4
# ip1 d1----- d2----
# ip2           d1-----
```

As seen by Secure Cloud Analytics

```
#   t0   t1   t2   t3   t4
# ip1 d1-----d2----
# ip2           d1-----
```

Note on Hostname Matching

In order to try to better handle cases where a tenant may have the same hostname configured in multiple domains, Secure Cloud Analytics employs 'flexible' matching and will treat the following as matching hostnames when looking to match an existing Device (for example, in the case of a matching IP):

```
foo
foo.com
foo.net
foo.obsrvbl.com
foo.bar.obsrvbl.com
foo.example.com
```

Secure Cloud Analytics considers just the hostname while ignoring the rest of the domain name.

Environments with NVM

This setup behaves very similar to the [Environments with Hostname Information](#) section, but there are a couple differences.

The NVM data feed provides the added benefits of being able to provide some unique endpoint identifiers to the user. These IDs potentially allow us to track a physical device that undergoes a change of hostname, which is not possible to track otherwise, and Secure Cloud Analytics would create two different Devices.

While we will make Devices based on the endpoint data feed (with unique endpoint IDs), there will be no hostname or IPs associated with these Devices until an observation is made about that endpoint based on the flow data.

Environments with ISE

The benefits of the ISE integration to Device tracking end up being identical to the [Environments with Hostname Information](#) section. ISE data is used to associate hostname information to IP addresses, but Secure Cloud Analytics will not create a new Device or track IPs that have not been seen in NetFlow.

Environments with Cisco Meraki

Cisco Meraki Integration using Secure Cloud Analytics

The Meraki integration using Secure Cloud Analytics proactively gathers hostname information from Meraki devices, and maps those hostnames to IPs as usual for on-premises Devices (the “default namespace”). This process will create Devices if they do not already exist. It will not augment Device or IP information gathered from the Cisco Meraki integration using Cisco XDR due to namespace differences. This causes this configuration to behave like [Environments with hostname information](#).

Cisco Meraki Integration using Cisco XDR

The Cisco Meraki Integration using Cisco XDR gets NetFlow from Meraki networking equipment through Cisco XDR into the standard Secure Cloud Analytics NetFlow path. As such, it will create Devices like any other NetFlow, and it does not contain hostname information. In effect, this configuration behaves like [environments with no available hostname information](#), with one major exception.

This integration leverages the information sent to label the NetFlow from different Meraki equipment into different namespaces. This avoids the usual [Overlapping Subnets](#) issues, but it can introduce new difficulties if more than one integration is configured. Most obviously, if both Secure Cloud Analytics and Cisco XDR Meraki integrations are configured, they will not use the same namespaces, and they will create non-overlapping Devices even in cases where the information represents the same physical device. That is, you will have 2 Devices, one in the default namespace with a hostname and no traffic, and another with traffic in a specific Meraki namespace and no hostname. Similar ‘splits’ can occur with other integrations if simultaneously enabled.

FAQ

Q: Why am I seeing IPs on an Secure Cloud Analytics Device that are no longer associated with that logical device on my network?

A: Unfortunately, there is nothing we can do about this. Secure Cloud Analytics cannot know if the old association is invalid or the result of, for example, an additional physical network interface.

Q: I don't have any hostname information being sent to Secure Cloud Analytics, why does my Device that is using both IPv4 and IPv6 addresses show as 2 distinct Devices?

A: Without hostname information, we cannot know different IPs are associated with the same logical device on your network.

Q: Why do I see multiple logical devices from different subnets appearing in the same Secure Cloud Analytics device?

A: Secure Cloud Analytics currently has no way to distinguish what subnet telemetry comes from, so the same IP will always be grouped into one Device.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

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
- 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

Revision	Revision Date	Description
1.0	August 15, 2025	Initial Version

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)

