



# Cisco Secure Network Analytics

Endpoint License and NVM Configuration Guide 7.4.2



---

# Table of Contents


<b>Introduction</b> .....	<b>3</b>
Overview .....	3
Requirements .....	3
Upgrading from 7.3.0 or 7.3.1 to 7.4.2 .....	3
Remove Endpoint Concentrator .....	3
Report Builder .....	4
Endpoint License and Data Store Capabilities .....	5
<b>Configuration</b> .....	<b>6</b>
Configure NVM profile on AnyConnect .....	6
Configure the Flow Collector to Ingest NVM Traffic .....	8
Using First Time Setup (Data Store Only) .....	8
Using the Flow Collector Advanced Settings .....	12
Configure the Flow Collector for Off- Network Cached Flows (Optional) .....	14
<b>Verification</b> .....	<b>15</b>
Flow Search (Non Data Store Only) .....	15
Opening Report Builder (Data Store Only) .....	15
<b>Contacting Support</b> .....	<b>16</b>
<b>Change History</b> .....	<b>17</b>

# Introduction

## Overview

Use this guide to configure Cisco Secure Network Analytics (formerly Stealthwatch) and the Cisco AnyConnect Secure Mobility Client Network Visibility Module (NVM) to enable:

- Storing and viewing of NVM fields
- Existing policy violation rules to trigger from NVM flows
- NetFlow detections based on NVM traffic
- Creating Custom Security Events based on the endpoint connections


 Secure Network Analytics with NVM supports UDP, but it does not support DTLS.

## Requirements

- Secure Network Analytics v7.4.2 with Cisco Secure Network Analytics Endpoint license. For more information about Endpoint license, refer to the [Smart Software Licensing Guide 7.4](#)
- AnyConnect v4.7 and later

## Upgrading from 7.3.0 or 7.3.1 to 7.4.2

### Remove Endpoint Concentrator

 Starting in v7.3.2, the Endpoint Concentrator is not needed for the Endpoint License deployment, and the Flow Collector was enhanced to process Network Visibility Module (NVM) data on all Secure Network Analytics deployments, including Data Store.

If you are an existing Secure Network Analytics customer upgrading from 7.3.0 or 7.3.1 to 7.4.2, you will need to remove the Endpoint Concentrator and reconfigure your NVM deployment.

---

Remove your Endpoint Concentrator(s) and configure your Flow Collector using the following instructions:

1. Remove your Endpoint Concentrator(s) from your cluster using Central Management.
  - a. Open Central Management.
  - b. On the Appliance Manager page, click the **⋯ (Ellipsis)** icon in the **Actions** column for the Endpoint Concentrator.
  - c. Click **Remove This Appliance**, then click **Yes**.
2. Configure flows from the NVM client to the Flow Collector using the [Configure NVM profile on AnyConnect](#) section.
3. Update your cluster to v7.4.2 using the [Secure Network Analytics Update Guide](#).
4. Add the NVM processing port to your Flow Collector Advanced Settings using the [Configure the Flow Collector](#) section.
5. Verify NVM data is processed using Report Builder or Flow Search using the [Verification](#) section.

 For assistance, please contact [Cisco Support](#).

## Report Builder

We moved Report Builder from a separate app to the core Secure Network Analytics in v7.4.x. If you have a previous version of the app installed, your app will be removed automatically as part of the update to Secure Network Analytics v7.4.x. Make sure you follow the instructions in the [Update Guide](#).



Do not uninstall your existing Report Builder app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted.

## Endpoint License and Data Store Capabilities

Endpoint license is now supported for Cisco Secure Network Analytics Data Store and provides:

- Full visibility to the endpoint, including on- network and off- network data
- Visibility to any NVM fields from the Endpoint Traffic (NVM) report in the Report Builder app
- A minimum of 30 days of storage of NVM data
- Improved processing and query performance
- NetFlow detections based on NVM traffic
- Creating Custom Security Events based on the endpoint connections

The following table provides performance estimates for a standard enterprise traffic profile (most customers):

Flows per second (FPS)		Number of FC 4210s	Number of DS 6200s/ 31 Days Storage
NetFlow	NVM		
300,000	150,000	1	3



There are several factors that may affect your specific performance, such as number of hosts, average size of flows, and more. While we do our best to represent the data as fairly and accurately as possible, your environment may experience different limits.

# Configuration

## Configure NVM profile on AnyConnect



The AnyConnect Profile Editor is available through Cisco Adaptive Security Device Manager (ASDM) or as a standalone offering. For more information about how to use the AnyConnect Profile Editor, refer to the [AnyConnect Administrator Guide](#).

1. Verify you have installed the Network Visibility Module.



2. Open the Network Visibility Module Profile Editor.
3. In the **Collector Configuration** section, enter the **IP Address** and **Port** of your Flow Collector.



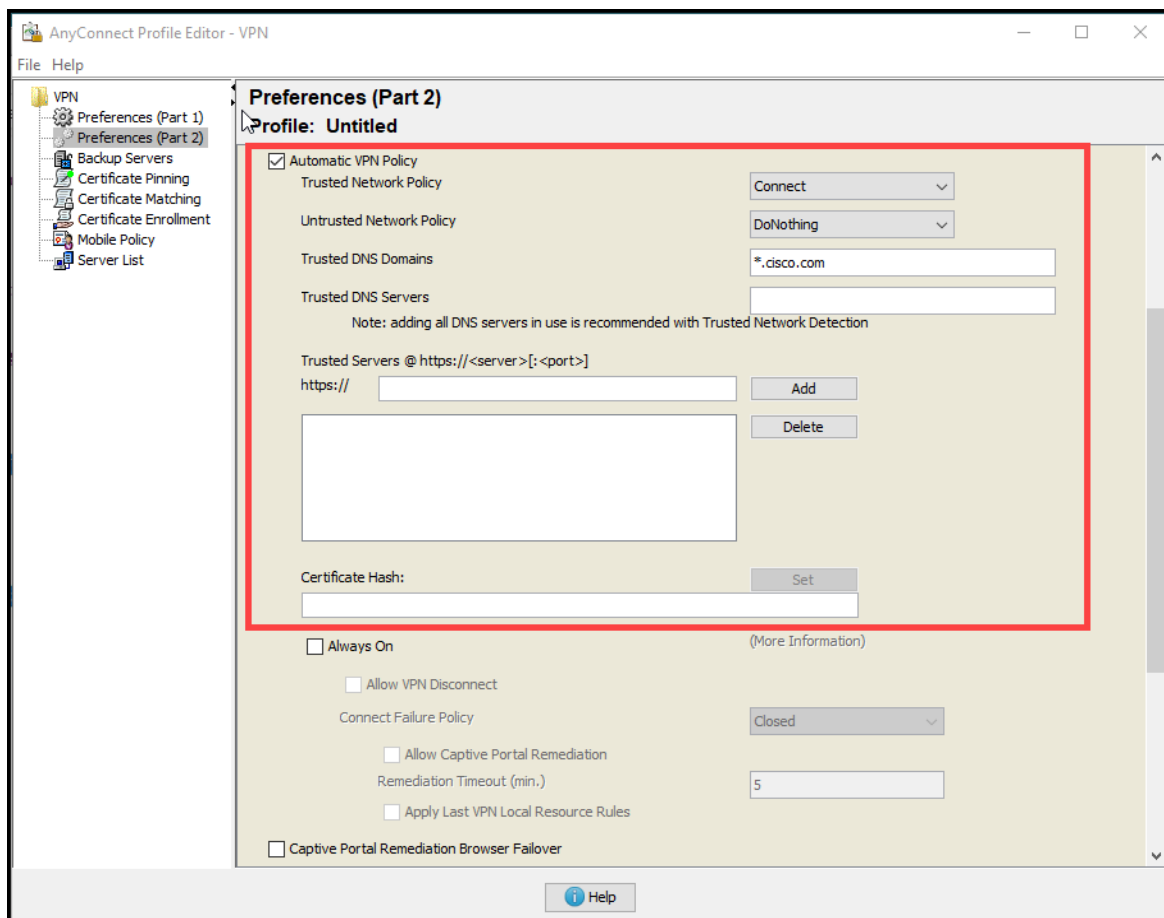
We recommend you use port 2030 rather than the default port, 2055. If port 2030 is already in use, you may use any non-reserved port. You will use this port in the [Configure the Flow Collector](#) section.

Do not use ports 2055, 514, or 8514.

4. Select **File > Save** to save your NVM Profile.
5. Close the NVM Profile Editor.
6. Open the VPN Profile Editor.
7. Click on **Preferences (Part 2)**.
8. Check the **Automatic VPN Policy** check box.
9. For **Trusted Network Policy**, select **Connect** from the drop down.
10. For **Untrusted Network Policy**, select **DoNothing** from the drop down.
11. Enter your **Trusted DNS Domains**, **Trusted Servers**, and **Certificate Hash**.



- The Trusted DNS Domain should be the same domain that the Flow Collector is running on. Wildcards (\*) are supported for DNS suffixes.
- The Trusted Servers should be the IP addresses of the DNS servers on the network.



12. Select **File > Save** to save your preferences.
13. Close the AnyConnect Profile Editor.

## Configure the Flow Collector to Ingest NVM Traffic

### Using First Time Setup (Data Store Only)

To enable ingest of NVM traffic on a new Flow Collector with Data Store, complete the following steps:

1. Follow the instructions in the applicable [appliance installation guide](#) for your Flow Collector. Then, use the [System Configuration Guide](#) for more detailed instructions on appliance configuration of multiple telemetry types.
2. Access the virtual machine console. Allow the virtual appliance to finish booting up.
3. Log in through the console.



- **Login:** root
  - **Default Password:** lan1cope
  - You will change the default password when you configure the system.
4. At the command prompt, type `SystemConfig`. Press Enter.
  5. Review the failed login attempts information. Select **OK** to continue.

```
Login information:
The user root has no failed login attempts.
Last login information:
root pts/0 10.0.7.10 Wed Nov 24 16:43 still logged in
root pts/0 10.0.7.10 Wed Nov 24 16:08 - 16:10 (00:02)
```

< OK >

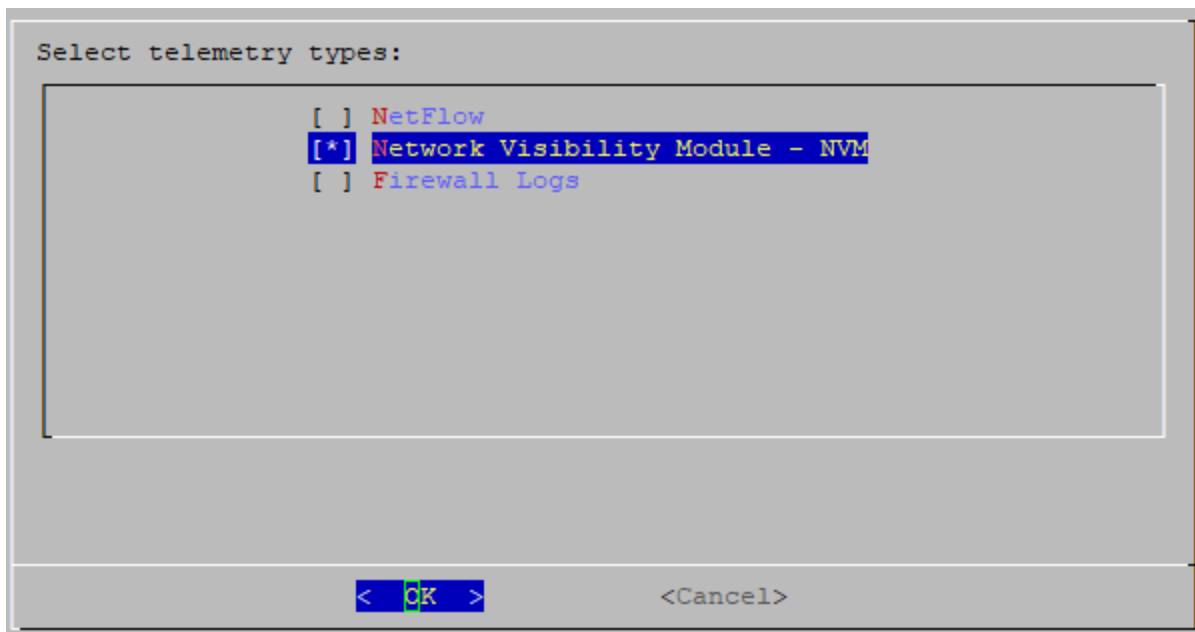
6. Review the First Time Setup introduction. Select **OK** to continue.

```
Welcome to First Time Setup. The First Time Setup wizard helps you
configure your appliance. First Time Setup takes approximately 5-10
minutes to complete, depending on your appliance model and
configuration options. Select OK to continue.
```

< OK >

7. Select Network Visibility Module - NVM from the telemetry types list. Select **Yes** to continue.

 All telemetry types are selected by default.



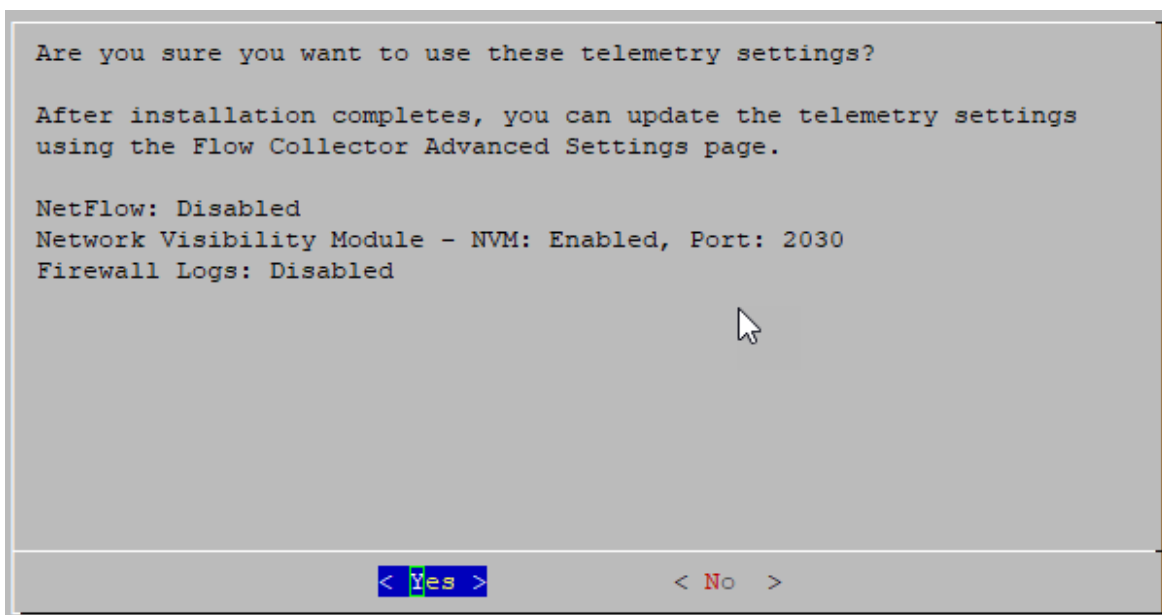
8. Enter the UDP port for Network Visibility Module - NVM. Select **OK**.

Set the value to the port specified in step 2 of the [Configure NVM profile on AnyConnect](#) section. Port 2030 is the default port. Do not use ports 2055, 514, or 8514.



Make sure your telemetry ports are unique. If you configure duplicate telemetry ports, the ports will be reset to their internal defaults to avoid loss of flow data. For example, if NetFlow and NVM are exported to the same telemetry port, each device exporting NVM data will create an exporter on the Flow Collector and exhaust the exporter resources in the Flow Collector engine, resulting in loss of flow data.

9. Confirm your settings. Select **Yes** to continue.




10. Follow the on- screen prompts to finish the virtual environment and restart the appliance.

## Using the Flow Collector Advanced Settings


-  Make sure to install the [latest Flow Collector NetFlow rollup patch](#) before you begin this procedure.

To enable ingest of NVM traffic on a Flow Collector that has already been configured, complete the following steps:

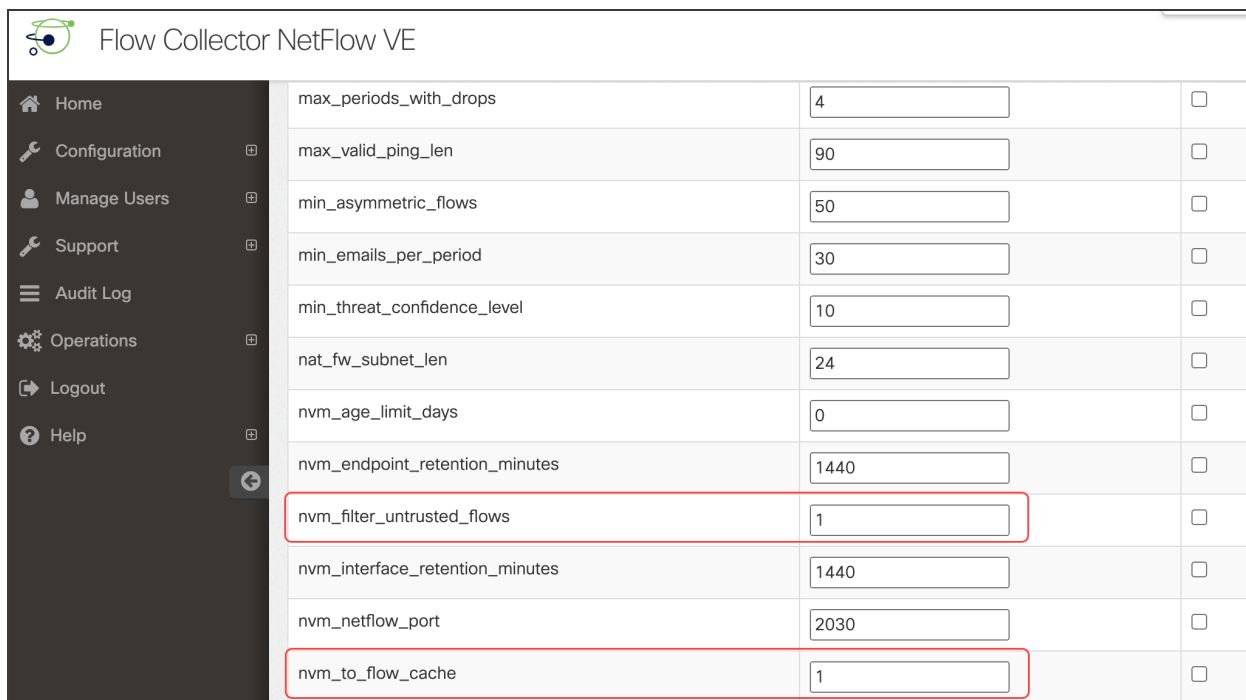
1. Log in to your Manager.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. On the Inventory page, click the **⋮ (Ellipsis)** icon for your Flow Collector, then select **View Appliance Statistics**. The Flow Collector Admin interface opens.
4. Select **Support > Advanced Settings**.

-  If a field is not shown, scroll to the bottom of the page. Click the **Add New Option** field. For more information about editing advanced settings on the Flow Collector, refer to the *Advanced Settings* Help topic.

5. In the **enable\_nvm** field, set the value to **1**. This field defaults to **0**.
6. In the **nvm\_netflow\_port** field, set the value to the port specified in step 2 of the [Configure NVM profile on AnyConnect](#) section. For example, port **2030**.

-  Make sure your telemetry ports are unique. If you configure duplicate telemetry ports, the ports will be reset to their internal defaults to avoid loss of flow data. For example, if NetFlow and NVM are exported to the same telemetry port, each device exporting NVM data will create an exporter on the Flow Collector and exhaust the exporter resources in the Flow Collector engine, resulting in loss of flow data.

7. In the **nvm\_to\_flow\_cache** field, set the value to **1** to capture network-based detections of NVM ingest flows. This field defaults to **0**.
8. In the **nvm\_filter\_untrusted\_flows** field, set the value to **1**. When you activate this field, it filters out untrusted traffic from network-based detections and averts possible issues such as conflicting IP addresses. This field defaults to **0**.



Flow Collector NetFlow VE

max_periods_with_drops	4	<input type="checkbox"/>
max_valid_ping_len	90	<input type="checkbox"/>
min_asymmetric_flows	50	<input type="checkbox"/>
min_emails_per_period	30	<input type="checkbox"/>
min_threat_confidence_level	10	<input type="checkbox"/>
nat_fw_subnet_len	24	<input type="checkbox"/>
nvm_age_limit_days	0	<input type="checkbox"/>
nvm_endpoint_retention_minutes	1440	<input type="checkbox"/>
nvm_filter_untrusted_flows	1	<input type="checkbox"/>
nvm_interface_retention_minutes	1440	<input type="checkbox"/>
nvm_netflow_port	2030	<input type="checkbox"/>
nvm_to_flow_cache	1	<input type="checkbox"/>



If you have Data Store and set the **nvm\_filter\_untrusted\_flows** field value to **1**, untrusted traffic is filtered out but remains stored in the NVM tables used to build the Endpoint Traffic (NVM) report. If you don't have Data Store, the untrusted traffic is not retained.

9. Click **Apply**.
10. When the confirmation message displays, click **OK**.

## Configure the Flow Collector for Off- Network Cached Flows (Optional)

Use the following instructions to configure cache flow processing for collecting off-network NVM traffic.

Collecting off- network NVM traffic impacts system performance. Do not enable this configuration if you do not need to collect or analyze this data.



If you enable the configuration and your system performance is impacted, adjust the throttle rate (refer to the [AnyConnect Administrator Guide](#)) and/or decrease the `nvm_age_limit_days` (refer to the instructions in this section).

Before you start this procedure, make sure you finish the previous procedures. You will continue this configuration on the Flow Collector Advanced Settings page. If the Flow Collector is closed, log in to it directly, or:

1. Log in to your Manager.
2. From the main menu, select **Configure > GLOBAL Central Management**.
3. On the Inventory page, click the **⋮ (Ellipsis)** icon for your Flow Collector, then select **View Appliance Statistics**. The Flow Collector Admin interface opens.
4. Select **Support > Advanced Settings**.
5. Update the following fields:
  - **process\_old\_nvm\_flows:** Enter 1 to enable cached flows to be processed by the Flow Collector.
  - **nvm\_age\_limit\_days:** Enter the maximum age (number of days) to collect cached flows by the Flow Collector. For example, if you enter 7, cached flows up to 7 days old will be processed. If you enter 0 (zero), then **all** cached flows will be processed. For best performance, set a limited number of days.



If a field is not shown, scroll to the bottom of the page. Enter the information into the **Add New Option** field. For more information about editing advanced settings on the Flow Collector, refer to the *Advanced Settings* Help topic.

6. Click **Apply**.
7. When the confirmation message is shown, click **OK**.

---

# Verification

Depending on your Secure Network Analytics deployment, you will see NVM data in a Flow Search or Report Builder.

## Flow Search (Non Data Store Only)


1. Log in to your Manager.
2. From the main menu, select **Investigate > Flow Search**.
3. Run a Flow Search.
4. On the Flow Search Results, filter the table by the **Subject Process Name** to verify you are getting NVM flows.

## Opening Report Builder (Data Store Only)

Report Builder provides three NVM- related reports for Secure Network Analytics with a Data Store:

- **NVM Database Ingest Trend**, provides a notification when your data has successfully reached the database ingest
- **NVM Collection Trend**, shows flow rate arrival at the Flow Collector from NVM
- **Endpoint Traffic (NVM)**, displays the most recent 300 records based on the end time



For more information about these reports, click the  (**Help**) icon to access the Help for Report Builder.

For example, to view the Endpoint Traffic (NVM) report:

1. Log in to your Manager.
2. From the main menu, select **Report > Report Builder**.
3. Click **Create New Report** and select **Endpoint Traffic (NVM)**.
4. Click **Run**.
5. Verify the report is showing NVM traffic.

# 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
1_0	March 1, 2023	Initial Version.
1_1	March 27, 2023	Updated the <i>Flow Collector for Off- Network Cached Flows (Optional)</i> section.
2_0	May 26, 2023	Updated the <i>Using the Flow Collector Advanced Settings</i> section to include information related to the <b>nvm_to_flow_cache</b> and <b>nvm_filter_untrusted_flows</b> fields.
2_1	January 12, 2024	Updated the <i>Verification</i> section.

---

# 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)

