Cisco Secure Network Analytics

Endpoint License and NVM Configuration Guide 7.4.1

Table of Contents

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 allow:

- Storage of AnyConnect NVM fields
- Viewing the NVM fields
- Existing policy violation rules to trigger from NVM flows

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

Requirements

- Secure Network Analytics v7.4.x with Cisco Secure Network Analytics Endpoint license. For more information about Endpoint license, refer to the Smart Software Licensing Guide 7.4
- AnyConnect Secure Mobility Client v4.7 and later

Upgrading from 7.3.0 or 7.3.1 to 7.4.1

Remove Endpoint Concentrator

> ℹ 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 7.4.1, 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 (missing or bad snippet) in the **Actions** column for the Endpoint Concentrator.
   c. Select **Remove This Appliance**, then click **Yes**.
2. Configure flows from the NVM client to the Flow Collector using the Configure NVM profile on AnyConnect Secure Mobility Client section.
3. Update your cluster to v7.4.1 using the Secure Network Analytics Update Guide (v7.3.x to v7.4.1).
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 Stealthwatch 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.

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

Endpoint License 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

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

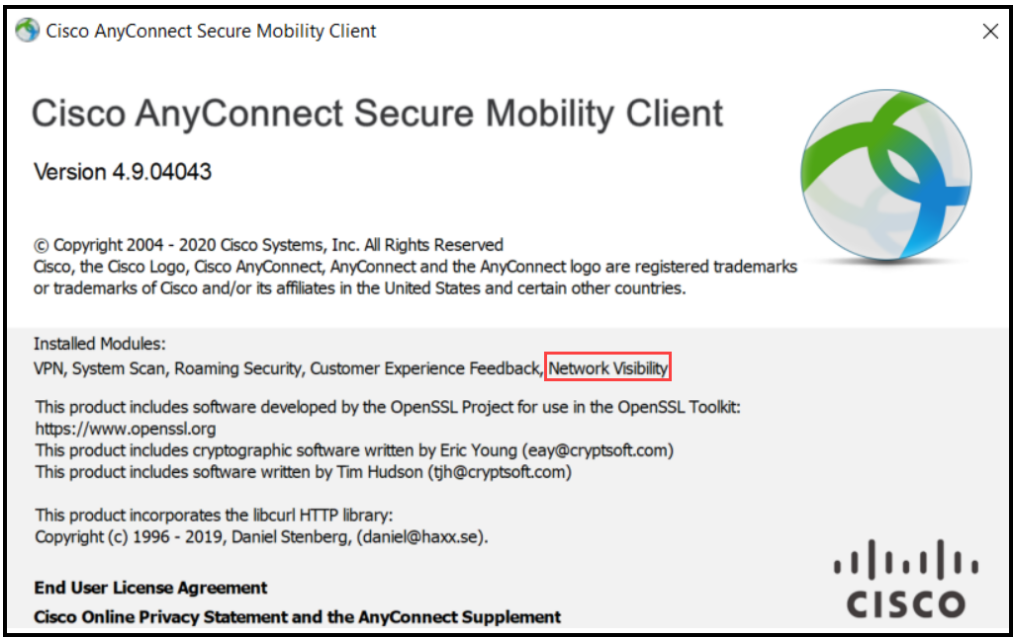
There are several factors that may affect your specific performance, such as number of hosts, average size of flows, and more. While we do our best to represent the data as fairly and accurately as possible, your environment may experience different limits.

Configuration

Configure NVM profile on AnyConnect Secure Mobility Client

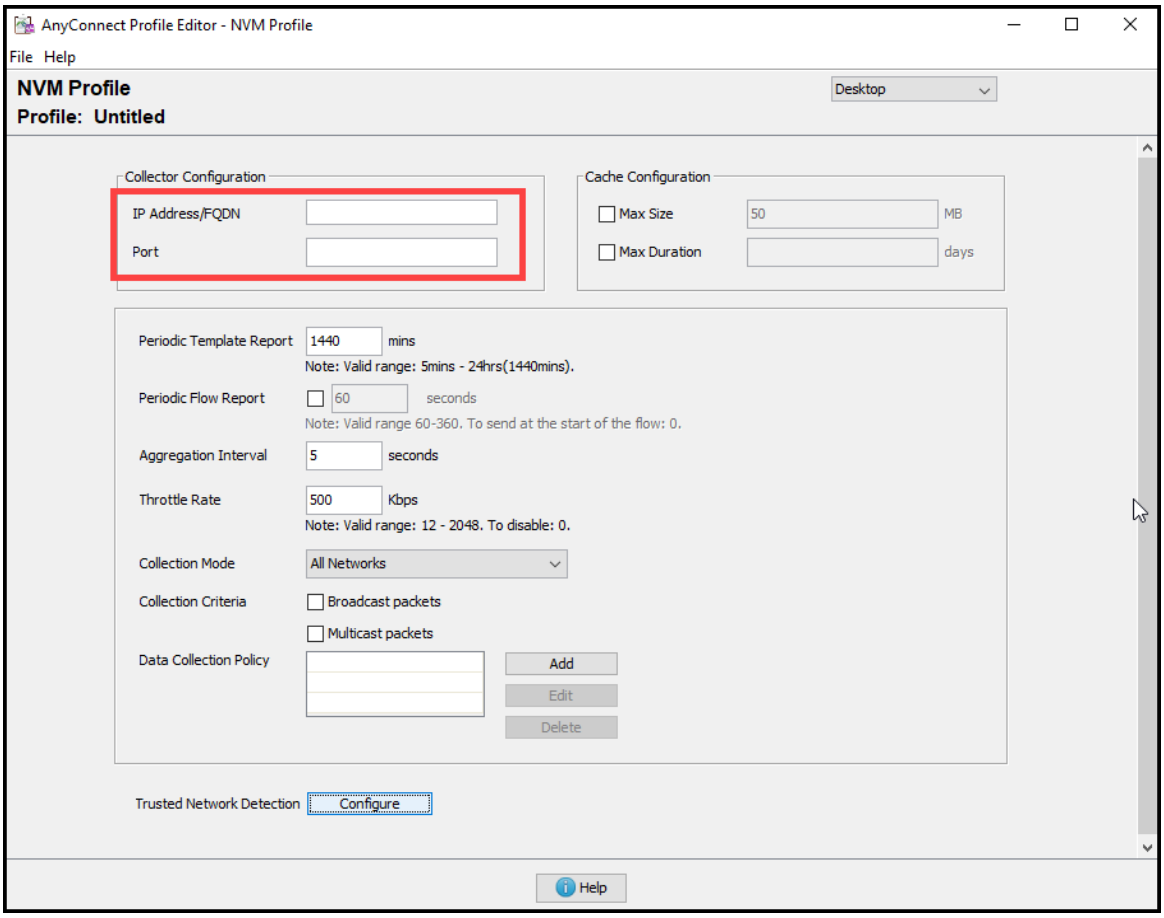
> The AnyConnect Profile Editor is available through Cisco Adaptive Security Device Manager (ASDM) or as a standalone offering. For more information about how to use the AnyConnect Profile Editor, refer to the Cisco AnyConnect Administrator Guide.

1. Verify you have installed the Network Visibility Module.



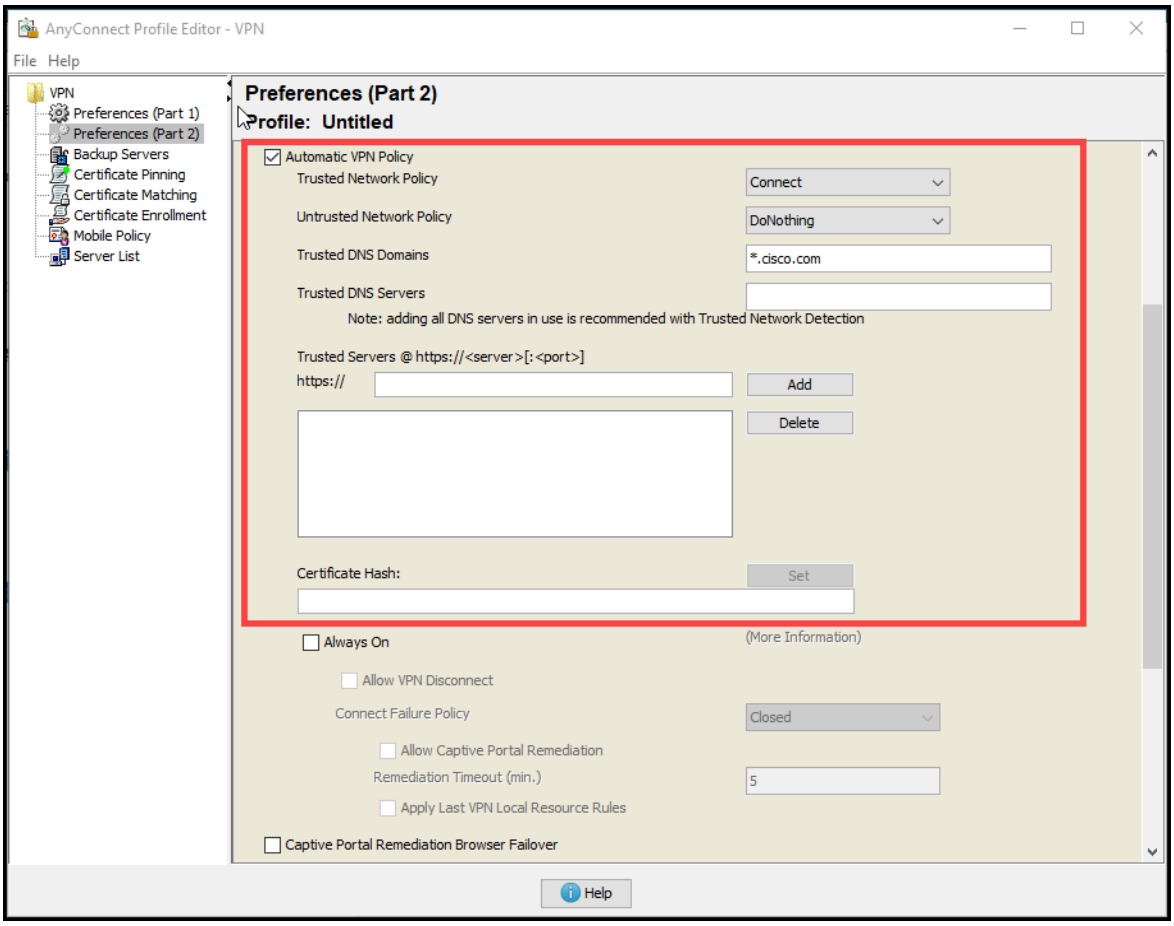
2. Open the Network Visibility Module Profile Editor.
3. In the **Collector Configuration** section, enter the **IP Address** and **Port** of your Flow Collector.

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

Configure the Flow Collector

Using First Time Setup (Data Store Only)

To enable ingest of NVM flows on a new Flow Collector, complete the following steps:

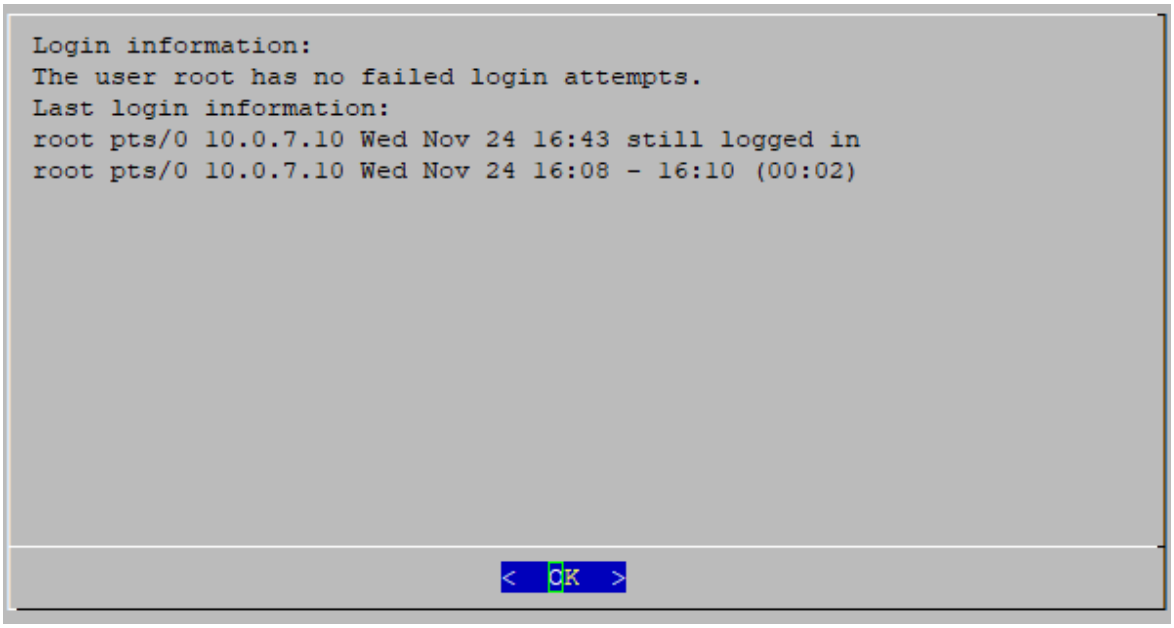
1. Use the applicable Data Store appliance installation guide for your Flow Collector. Follow the instructions to get to the Configuring your Environment using First Time Setup section.

   For more detailed instructions on appliance installation and configuration of multiple telemetry types, use the Data Store appliance installation guide.

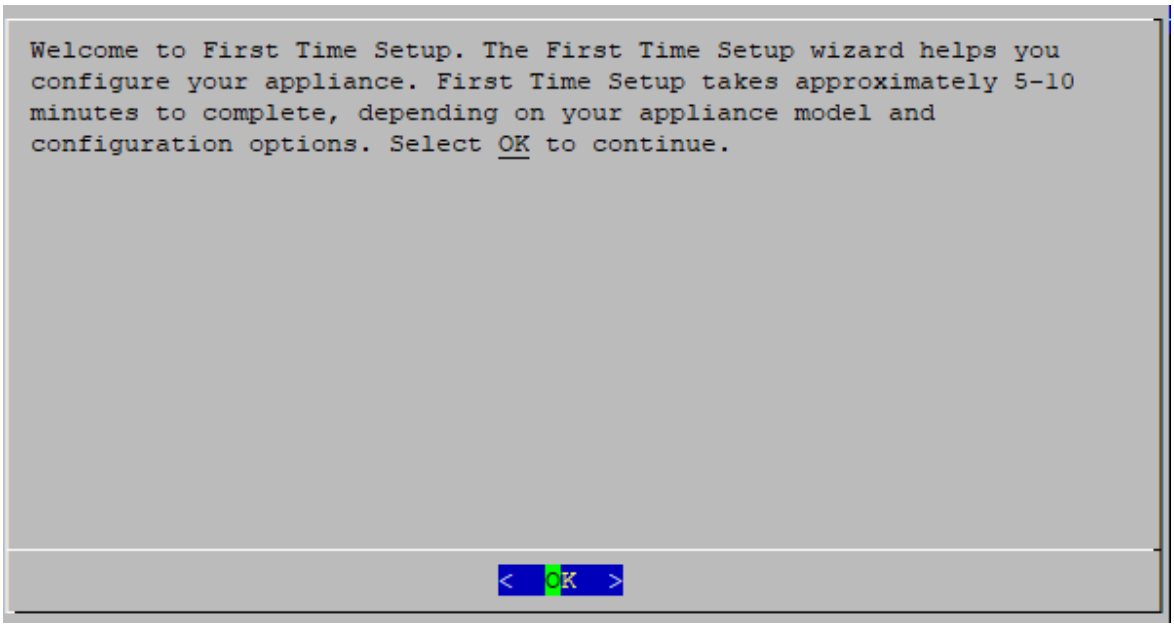
2. Access the virtual machine console. Allow the virtual appliance to finish booting up.
3. Log in through the console.

- **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.

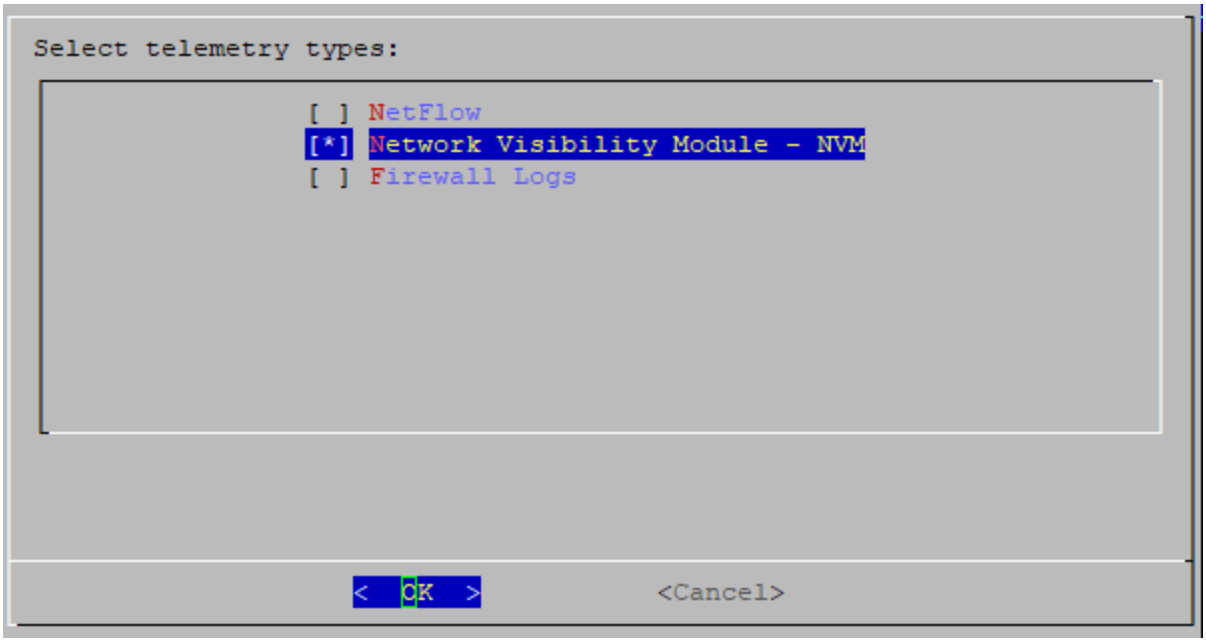


6. Review the First Time Setup introduction. Select **OK** to continue.



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

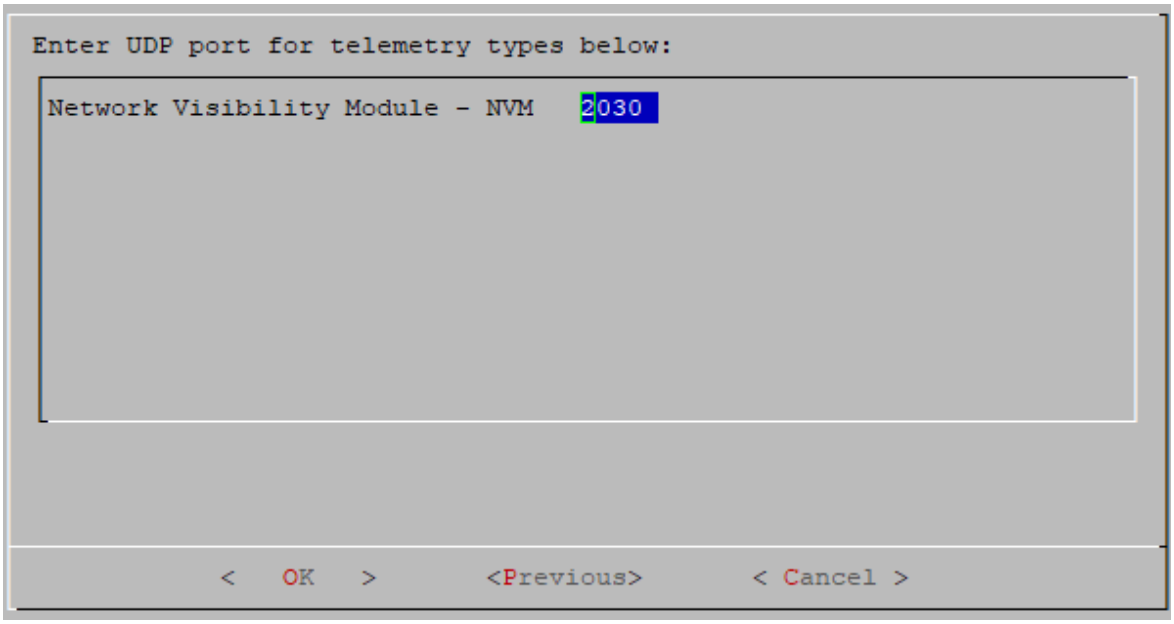
> All telemetry types are selected by default.



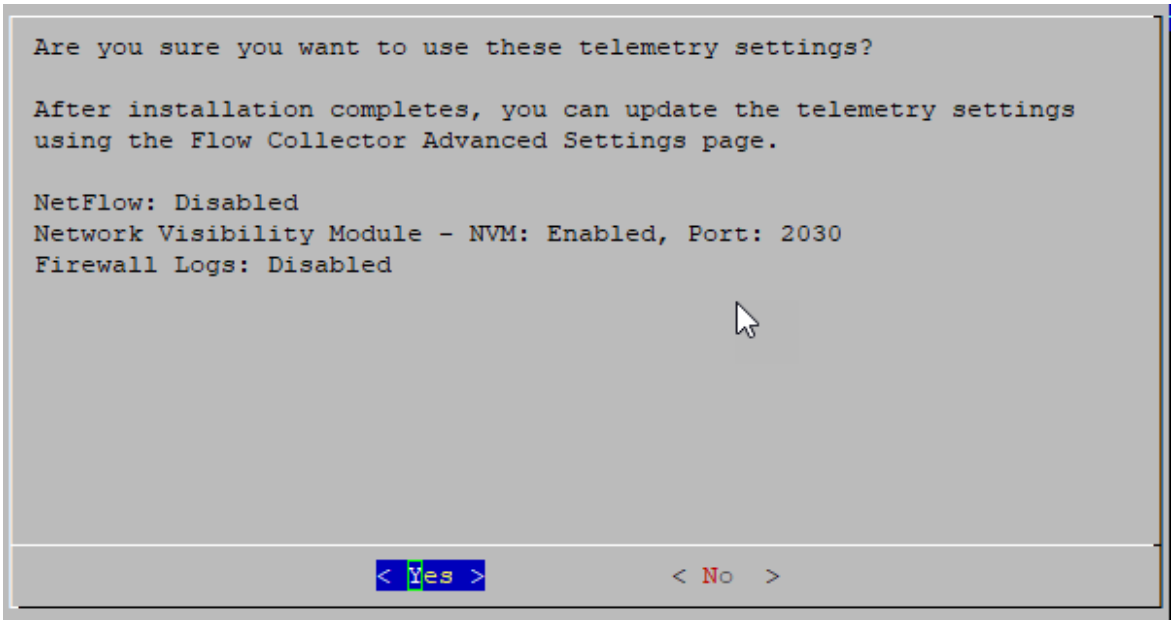
8. Enter the UDP port for Network Visibility Module – NVM. Select **OK**.

> Set the value to the port specified in step 2 of the Configure NVM profile on AnyConnect Secure Mobility Client section. Port 2030 is the default port.

> Do not use ports 2055, 514, or 8514.



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

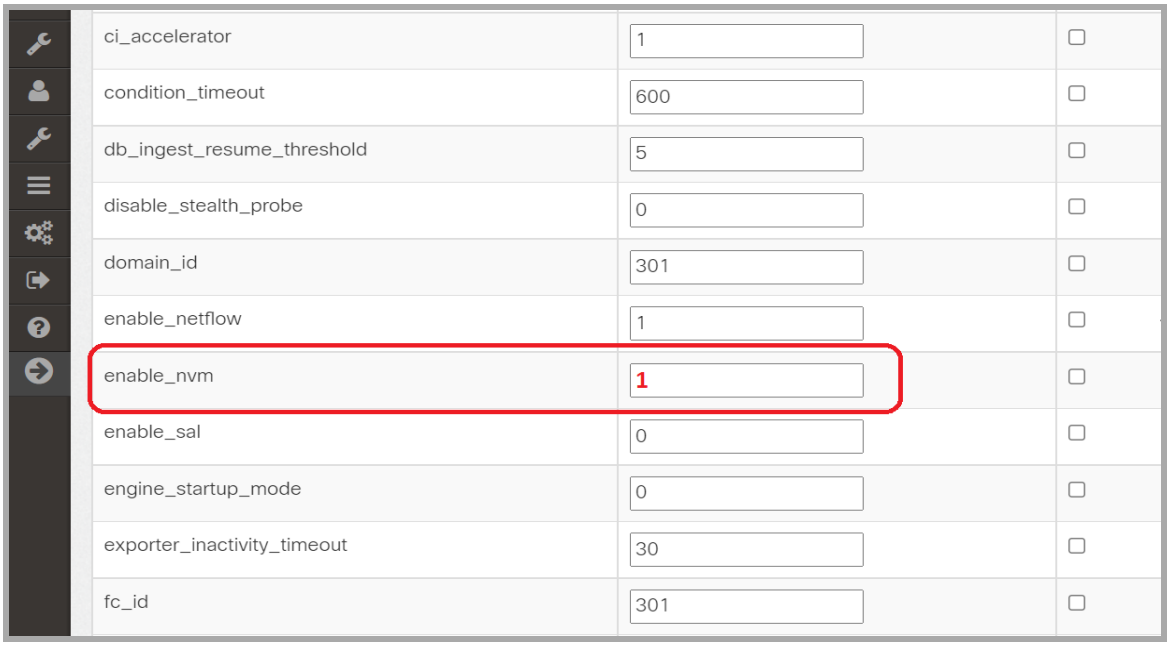


10. Follow the on-screen prompts to finish the virtual environment and restart the appliance.

Using the Flow Collector Advanced Settings

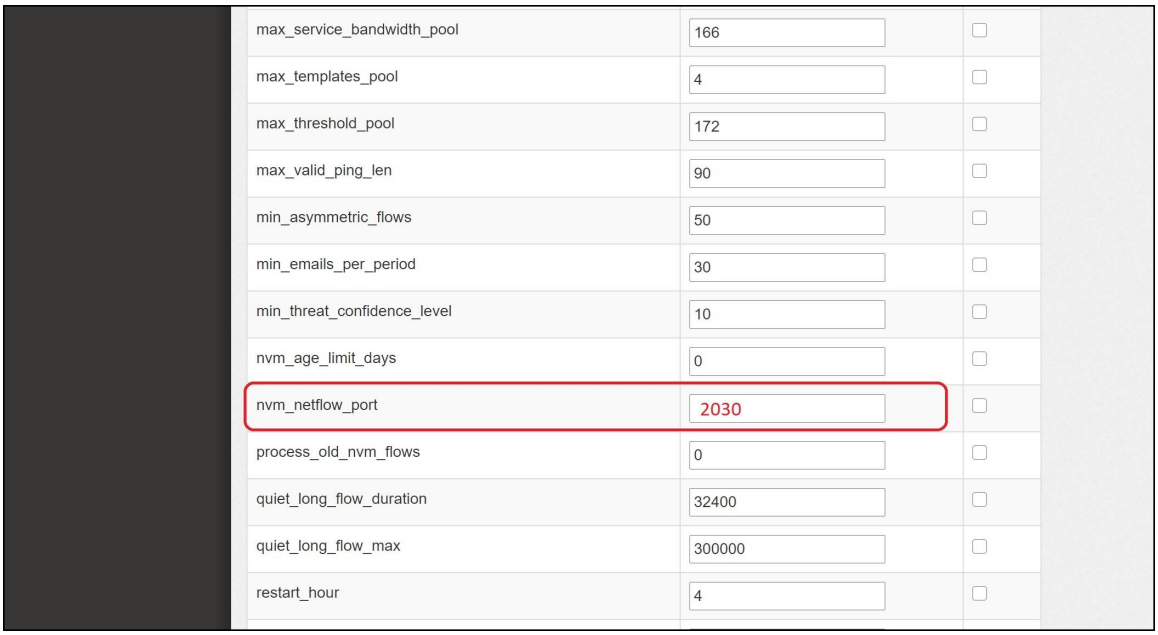
To enable ingest of NVM flows on a Flow Collector that has already been configured, complete the following steps:

1. Log in to your Manager.
2. From the navigation menu, click the ⚙ (**Global Settings**) icon and select **Central Management**.
3. Click the ••• (**Ellipsis**) icon for your Flow Collector, then click **View Appliance Statistics**. The Flow Collector Admin interface opens.
4. Click **Support > Advanced Settings**.
5. In the **enable_nvm** field, set the value to 1.



6. In the **nvm_netflow_port** field, set the value to the port specified in step 2 of the Configure NVM profile on AnyConnect Secure Mobility Client section. For example, port 2030.

> 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.



7. Click **Apply**.
8. When the confirmation message is shown, click **OK**.
9. To configure the Flow Collector for Offline Data Collection, continue to the next section. Do not close the Flow Collector.

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

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

> Collecting off-network NVM data 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 Administator Guide) and/or decrease the nvm_age_limit_days (refer to the instructions in this section).

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

- Log in to your Manager.
- From the navigation menu, click the ⚙ (**Global Settings**) icon and select **Central Management**.
- Click the ••• (**Ellipsis**) icon for your Flow Collector, then click **View Appliance Statistics**. The Flow Collector Admin interface opens.
- Click **Support > Advanced Settings**.

2. Update the following fields:

   - **process_old_nvm_flows:** Enter 1 to enable cached flows.
   - **nvm_age_limit_days:** Enter the maximum number of days to collect cached flows.
     For example, if you enter 7, it collects the last 7 days. If you enter 0 (zero), there is no limit. For best performance, set a limited number of days.

> 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.

3. Click **Apply**.
4. When the confirmation message is shown, click **OK**.

Verification

Flow Search

1. Log in to your Manager.
2. Click **Analyze > 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. Select the **Dashboards** menu.
3. Select **Report Builder**.
4. Click **Create New Report** and select **Endpoint Traffic (NVM)**.
5. Click **Run**.
6. Verify the report is showing NVM fields.

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

Copyright Information