



Cisco Secure Network Analytics

Endpoint License and NVM Configuration Guide 7.4.0



Table of Contents

Introduction	3
Overview	3
Requirements	3
Updating to v7.4.0	3
Endpoint License Capabilities	4
Configuration	5
Configure NVM profile on AnyConnect Secure Mobility Client	5
Configure the Flow Collector	7
Configure the Flow Collector for Off-Network Cached Flows (optional)	8
Verification	10
Flow Search	10
Opening Report Builder (Data Store only)	10
Contacting Support	11

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

Updating to v7.4.0

We moved Report Builder from a separate app to the core Secure Network Analytics in v7.4.0. 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 v7.4.0. 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.

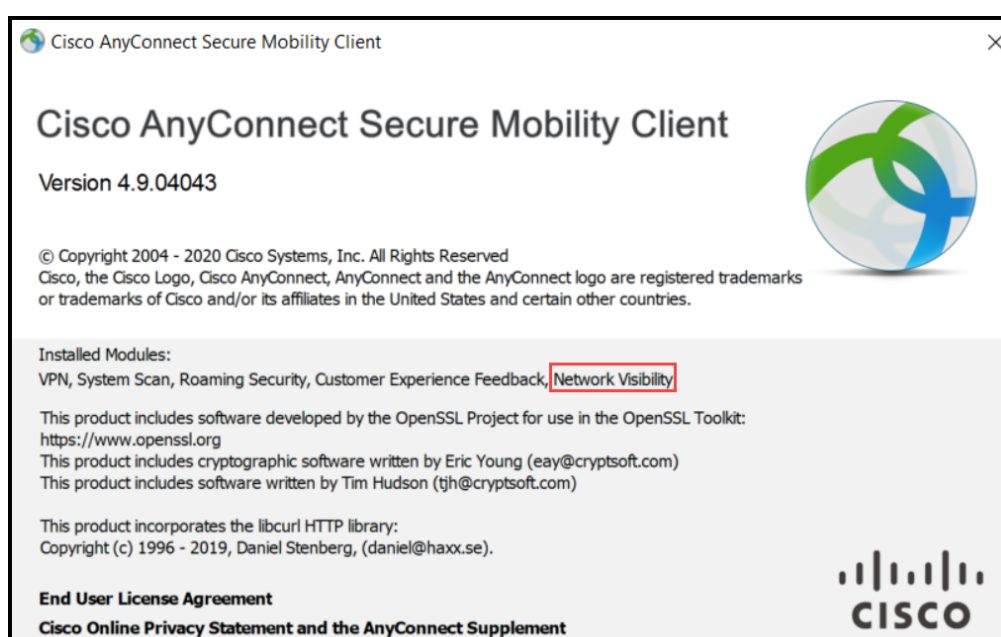
Configuration

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.



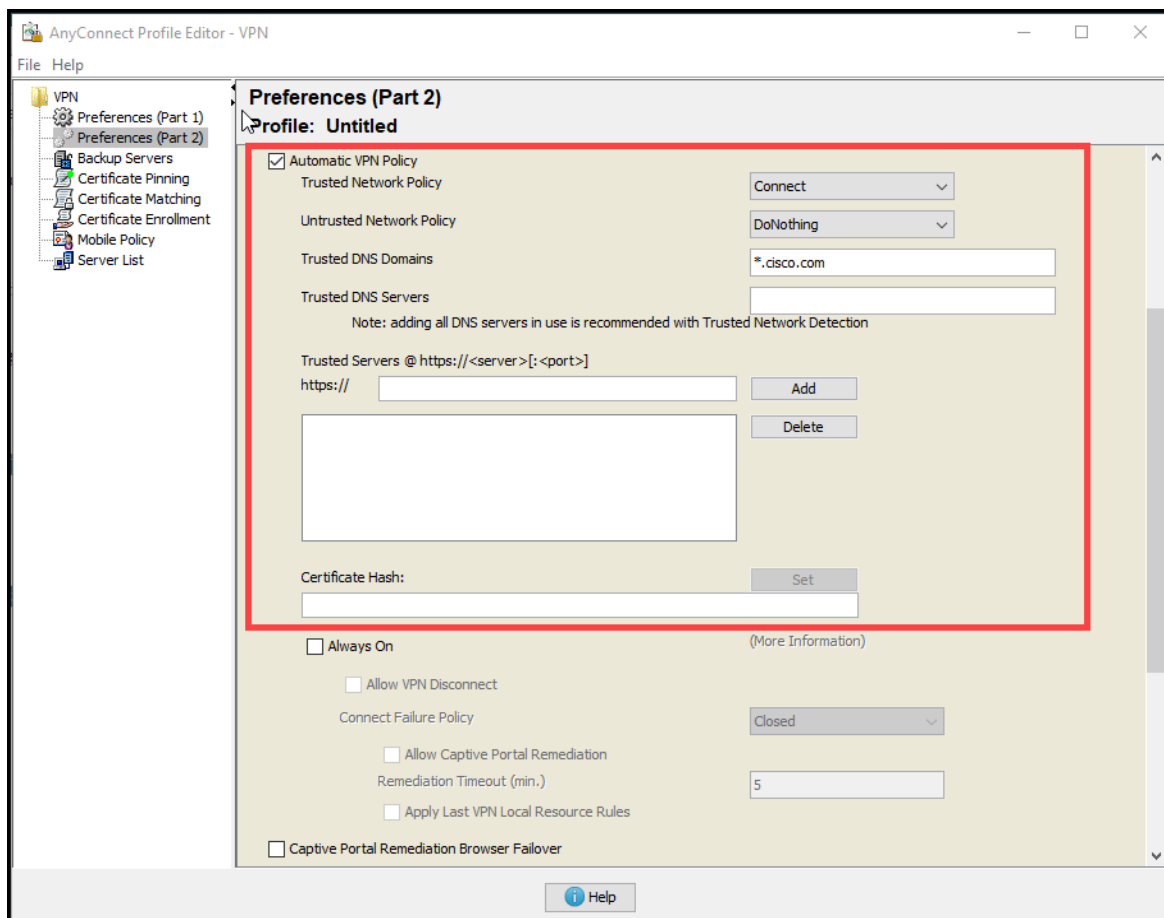
We recommend you use port 2030 rather than the default port, 2055. If port 2030 is already in use, you may use any non-reserved port. You will use this port in step 5 of the [Configure the Flow Collector](#) section.

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

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 **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.

max_service_bandwidth_pool	166	<input type="checkbox"/>
max_templates_pool	4	<input type="checkbox"/>
max_threshold_pool	172	<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"/>
nvm_age_limit_days	0	<input type="checkbox"/>
nvm_netflow_port	2030	<input type="checkbox"/>
process_old_nvm_flows	0	<input type="checkbox"/>
quiet_long_flow_duration	32400	<input type="checkbox"/>
quiet_long_flow_max	300000	<input type="checkbox"/>
restart_hour	4	<input type="checkbox"/>

- Click **Apply**.
- When the confirmation message is shown, click **OK**.
- 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 Administrator 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)

The Endpoint Traffic (NVM) report is only available in Secure Network Analytics with a Data Store.

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.



To access the Help for Report Builder, click the  (**Help**) icon. The Help includes instructions and details about the Endpoint Traffic (NVM) report.

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

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)

