How To Integrate Nagios Network Analyzer 2026 Alerts With Nagios XI 2026 And Nagios Core

Purpose

This document describes how to integrate Nagios Network Analyzer 2026 alerts with Nagios XI and Nagios Core.

Overview

Nagios Network Analyzer 2026 can be integrated with Nagios XI and Nagios Core, extending the capabilities of Nagios Network Analyzer. The differences between integrating Nagios XI and Nagios Core are as follows:

Nagios XI

- Set up active Network Analyzer checks in Nagios XI with the Network Analyzer wizard.
- Configure Network Analyzer to send passive check results to Nagios XI using NRDP.
- Add Network Analyzer check data to regular Nagios XI Reports and Dashboards.

Nagios Core

- Configure Network Analyzer to send passive check results to Nagios Core using NRDP.

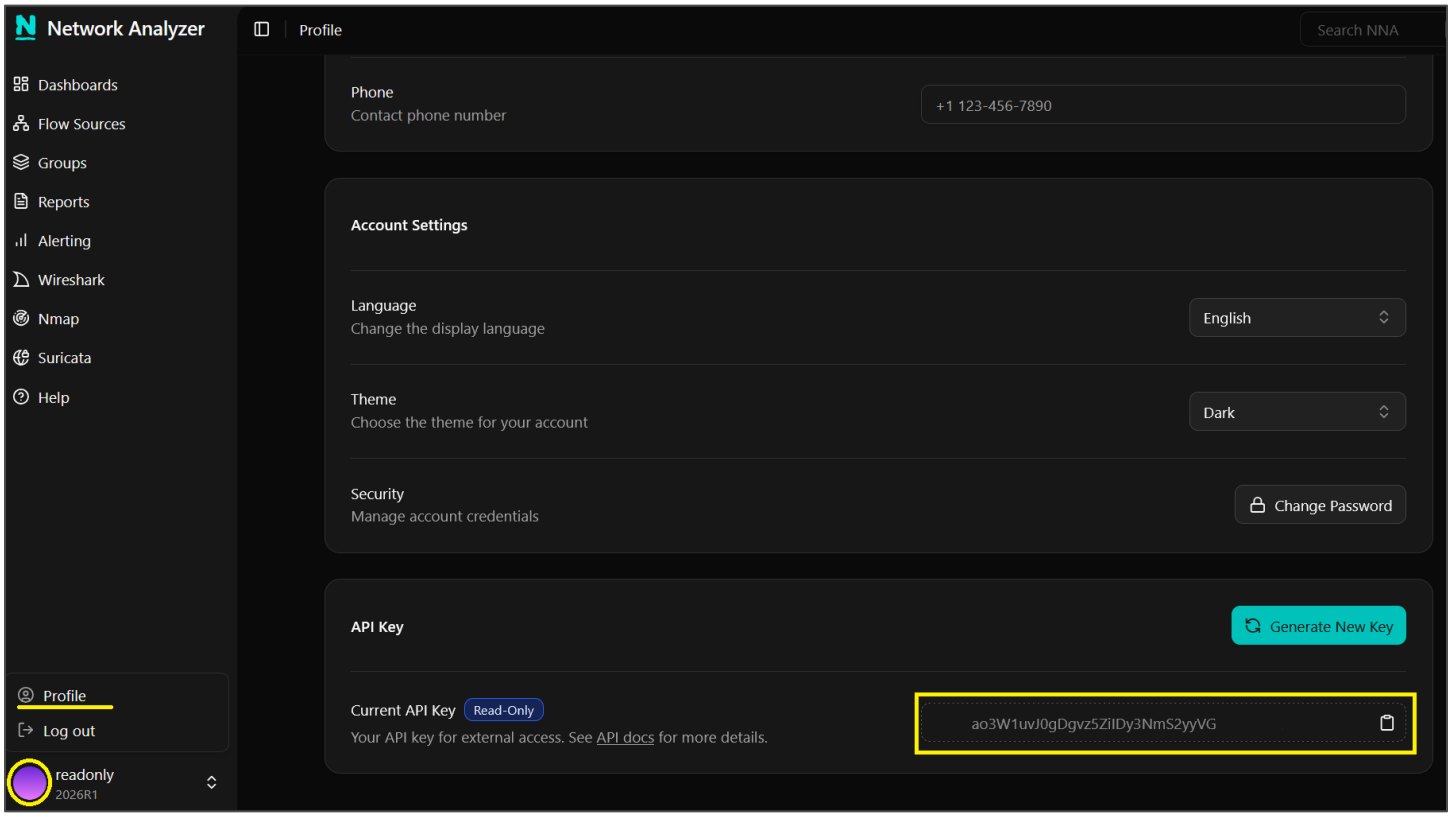
Nagios XI - Configure Integration

In Nagios XI configure the Nagios Network Analyzer Integration component with the details of your Nagios Network Analyzer server(s). Integration is achieved by using an API key that belongs to a Nagios Network Analyzer user's account that has been granted API access. The first step is to get the API key that is required when configuring the component.

Note: It is only necessary to configure the Network Analyzer component in XI if you wish to use the Network Analyzer configuration wizard to set up active checks. If you only want to use NRDP passive checks, you can skip ahead to the NRDP section.

In Network Analyzer

1. Login to **Nagios Network Analyzer** as a user with API access.
2. Click the **username** in the bottom-left corner of the screen, then click **Profile** and scroll to the bottom.



The screenshot above shows an example of a user's profile and API key. In this case, a dedicated user account has been created specifically for this purpose. This account has the default "User" Role which allows read only access, and API access has been granted.

A best practice is to use a dedicated account, as a new key can be easily generated on a rotational basis or regenerated if the existing key has been compromised.

If the user account's **Profile** page does not have an API Key and shows **No API Access**, the account will need to be altered.

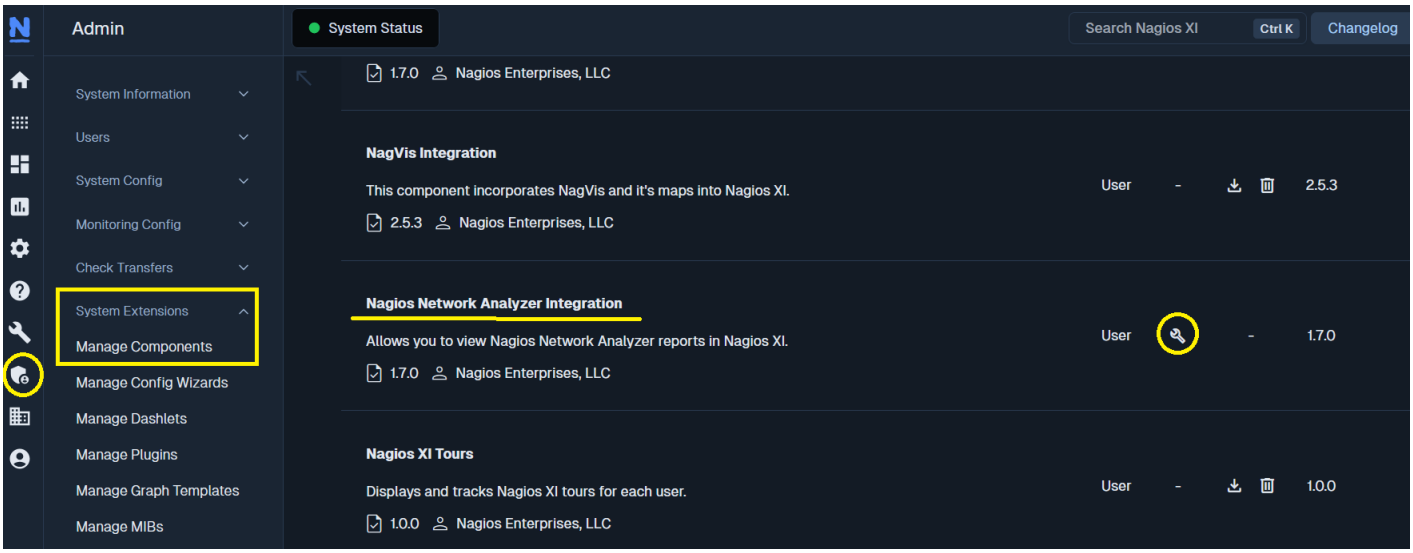
- Login as an admin user and navigate to **Administration** > **User Management**
- Edit the user and change **API Access** to **Yes**.

You can learn more about managing Users and Roles here:

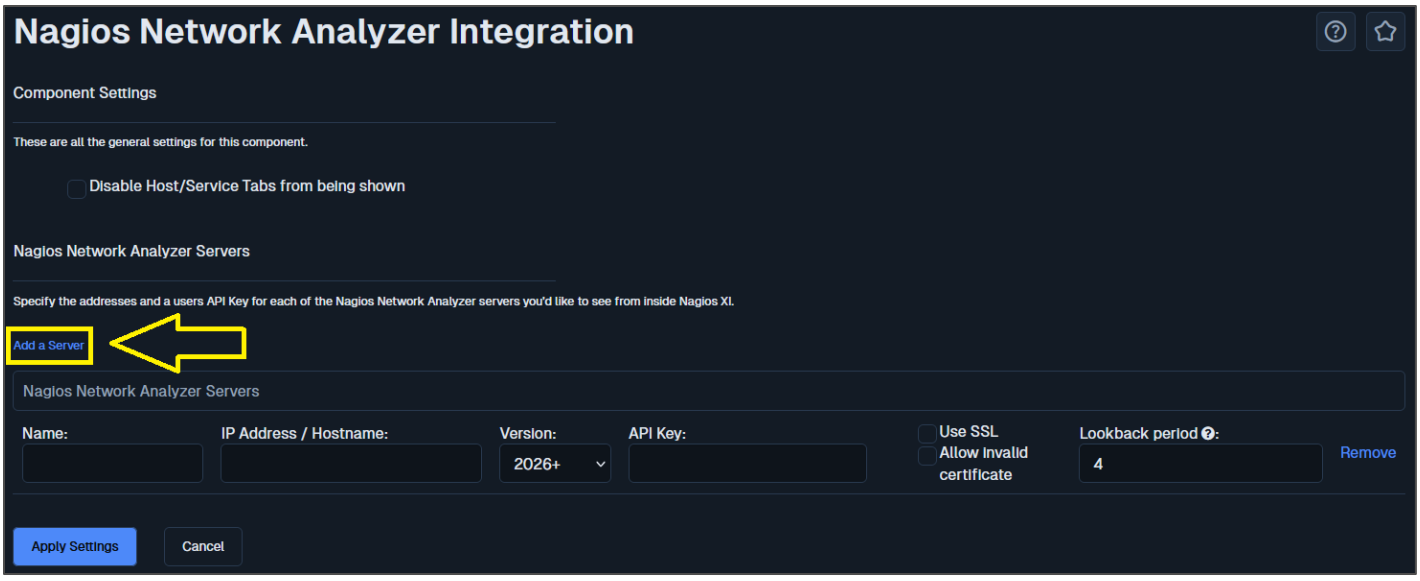
[Managing Users in Network Analyzer 2026]

In Nagios XI

3. **Login** and navigate to **Admin** > **System Extensions** > **Manage Components**.
4. Locate the **Nagios Network Analyzer Integration** component and click the **settings** icon.



5. Click the **Add a Server** link to display the fields for adding a Nagios Network Analyzer server.



a. The following fields will be populated:
    i. **Name** - This is the name that you will see in the Network Analyzer Server dropdowns throughout Nagios XI. For example, in the Nagios Network Analyzer configuration wizard.
    ii. **IP Address / Hostname** - The network address that Nagios XI uses to communicate with Nagios Network Analyzer.
    iii. **Version** – whether the Network Analyzer server is Legacy (2024) or 2026+. Choose **2026+**.
    iv. **API Key** - This is used for authentication with Nagios Network Analyzer as explained earlier.
    v. **Use SSL** - Required if your Nagios Network Analyzer server is configured with SSL/TLS certificates.
    vi. **Allow Invalid Certificate** – choose whether to allow an invalid Network Analyzer server certificate.
    vii. **Lookback Period** – How much data you want the component to show by default, in hours.

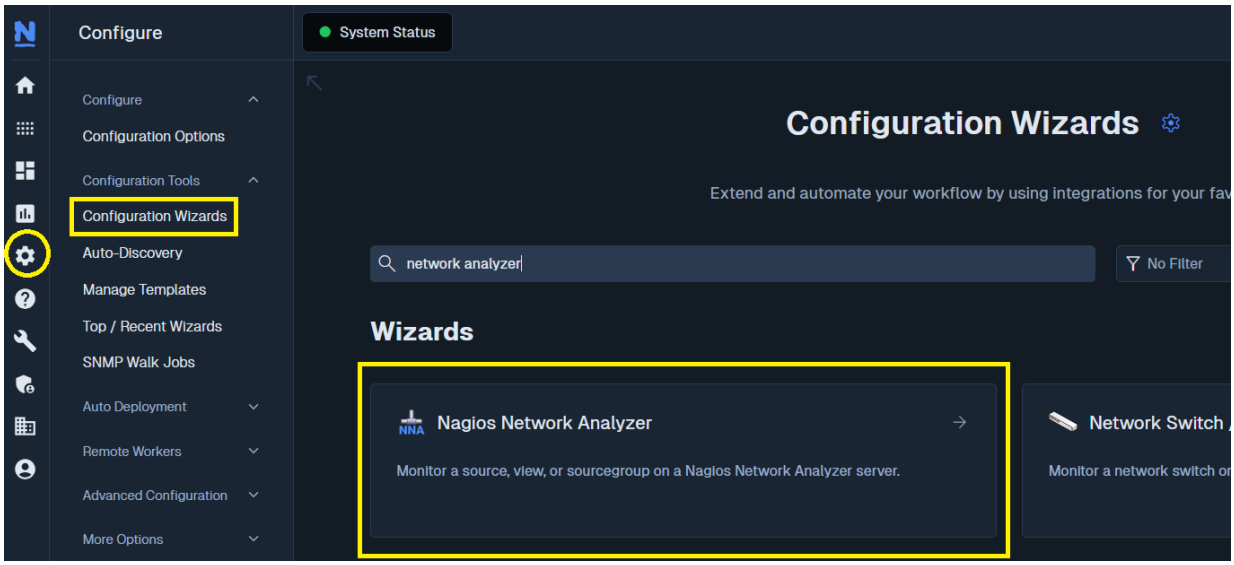
6. When finished, click the **Apply Settings** button. Additional Network Analyzer servers can be added by clicking on the **Add a Server** link.
7. Servers can be removed by clicking on the server's **Remove** link.
8. To remove the **Network Traffic Analysis** tabs from the **Hosts and Services** details screens in Nagios XI, check the **Disable Host/Service Tabs from being shown** checkbox.

   Note that at launch, Network Analyzer 2026 integration is limited to the Network Analyzer wizard, so this setting will only apply to linked Network Analyzer 2024 servers initially.

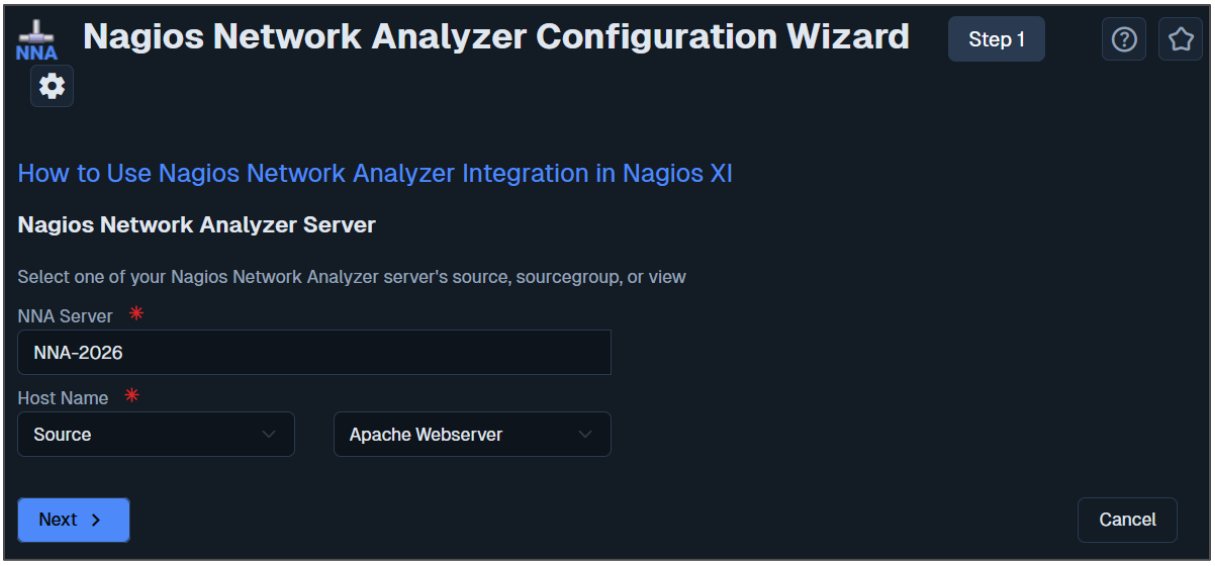
This completes the initial steps for integrating Nagios Network Analyzer with Nagios XI.

Nagios XI - Configuration Wizard

To begin using the Nagios Network Analyzer wizard navigate via the top menu bar to **Configure** > **Configuration Wizards** and select the **Nagios Network Analyzer** wizard. The search field allows you to quickly find the wizard.



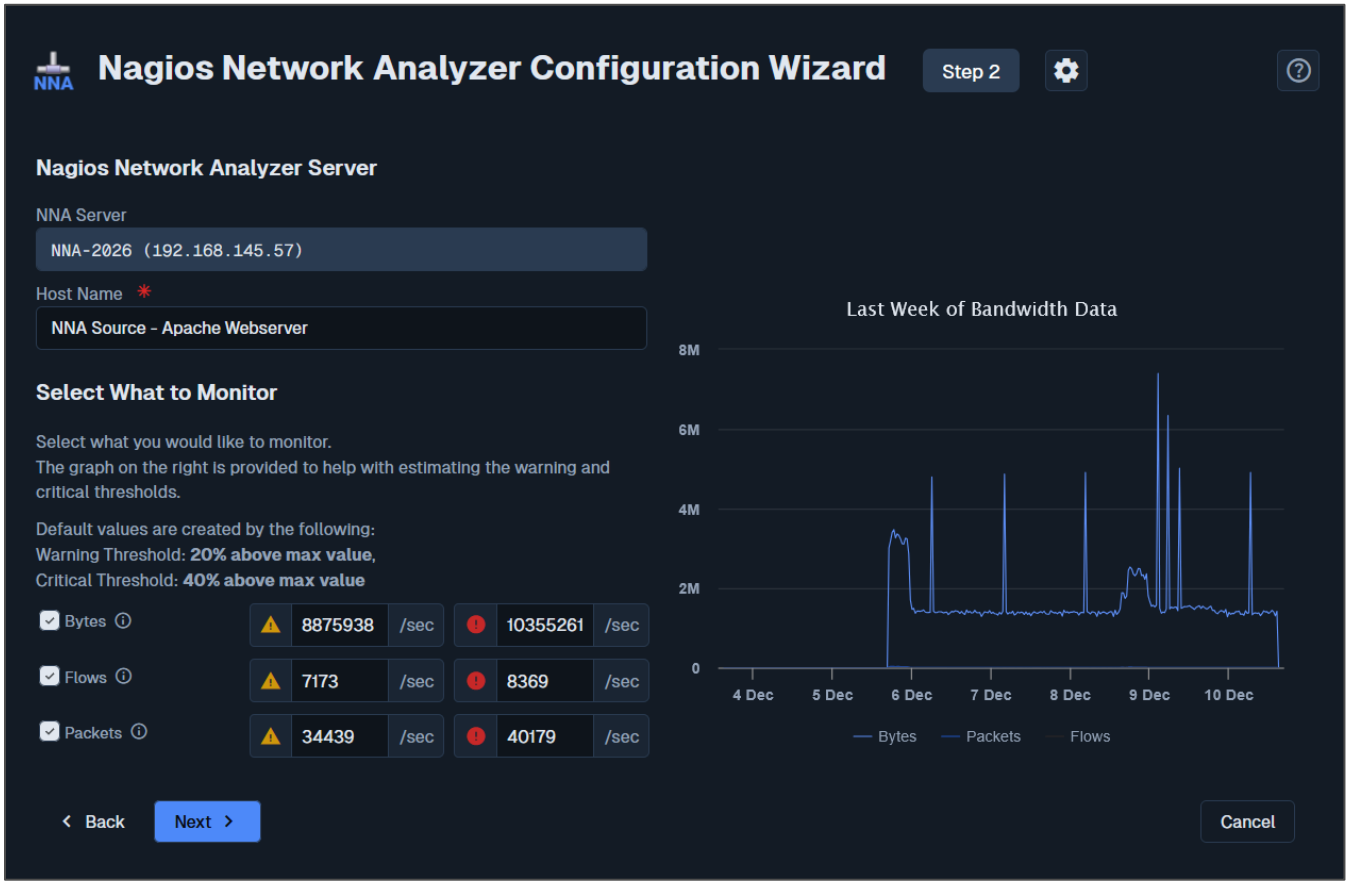
- In **Step 1** select the NNA Server and **Source** or **Sourcegroup** for the wizard to use in **Step 2**.
- Click **Next** to progress to **Step 2**.



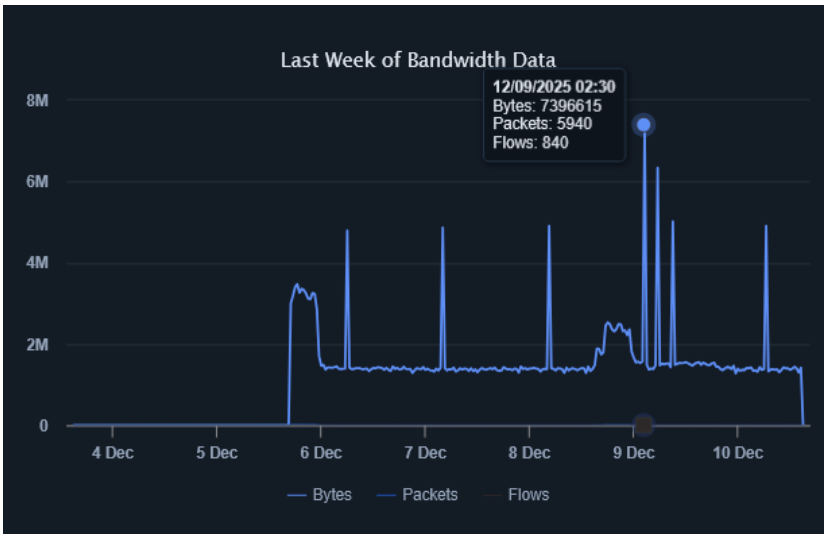
- Make sure the configuration has a valid **Host Name**. The default format is:

```
NNA Source/Sourcegroup - <Selected Source/Sourcegroup Name>
```

- Select what to monitor.
- **Bytes**, **Flows** and **Packets** all require warning and critical thresholds. Data queried from the source will be used to suggest warning and critical threshold values.



- The graph on the right-hand side of **Step 2** shows data from the last week. Hovering the mouse over the chart will display the historical data of each point on the graph. This data can be used to help you determine meaningful thresholds.

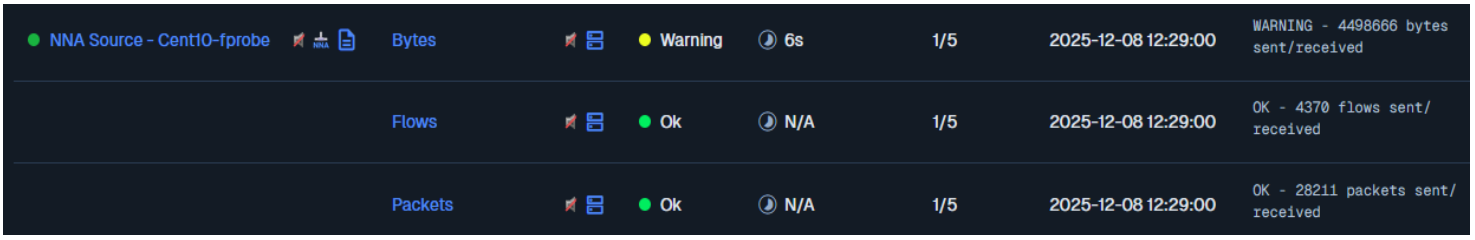


- Use the check boxes to deselect unnecessary/unwanted service checks.
- Click **Next** and then complete the wizard by choosing the required options in **Step 3** – **Step 5**. You can learn more about the various settings here:

  Understanding and Using Configuration Wizards in Nagios XI

- Click **Finish** in the final step of the wizard.

The wizard will create new hosts and services for XI to begin monitoring. Once the wizard applies the configuration, click the **View status details for xxxxx** link to see the new host and services that were created.



NRDP Passive Checks

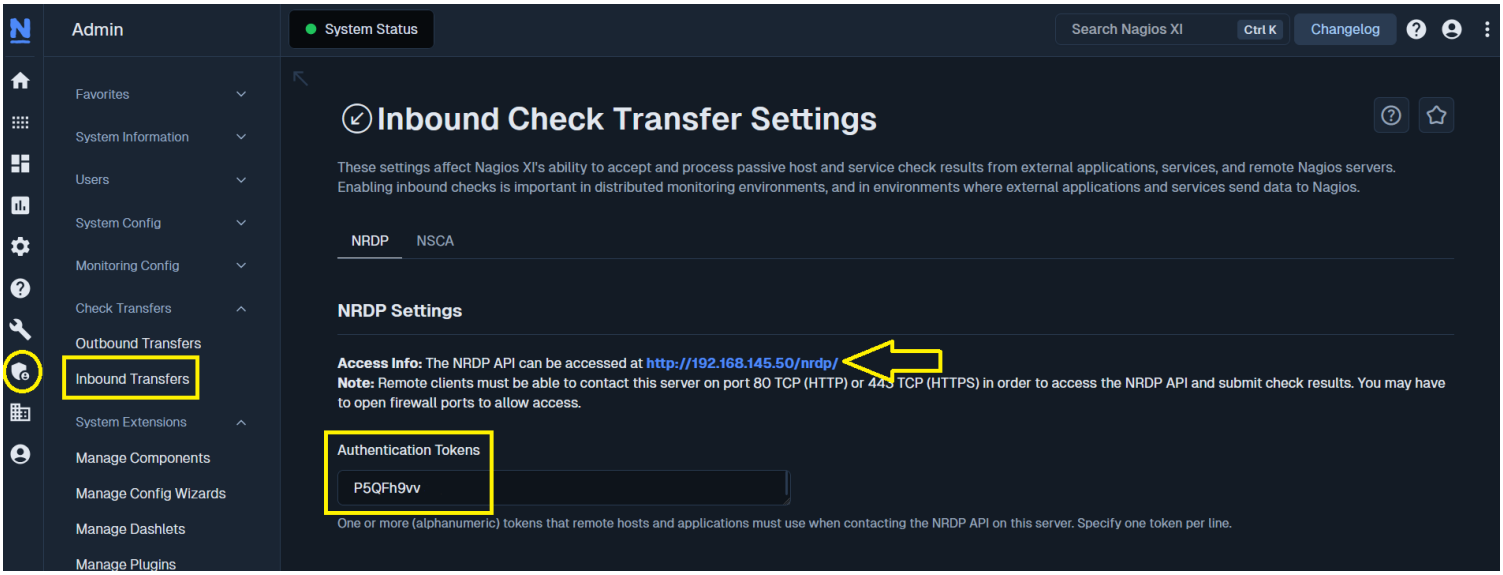
NRDP Setup in Nagios XI and Nagios Core

To be able to send alerts to a Nagios server using NRDP you will need to do the following:

- **Nagios XI**
  - The Inbound Transfers settings on your Nagios XI server, found in the **Admin > Check Transfers > Inbound Transfers > NRDP Tab** menu.
- **Nagios Core**
  - Install and configure NRDP

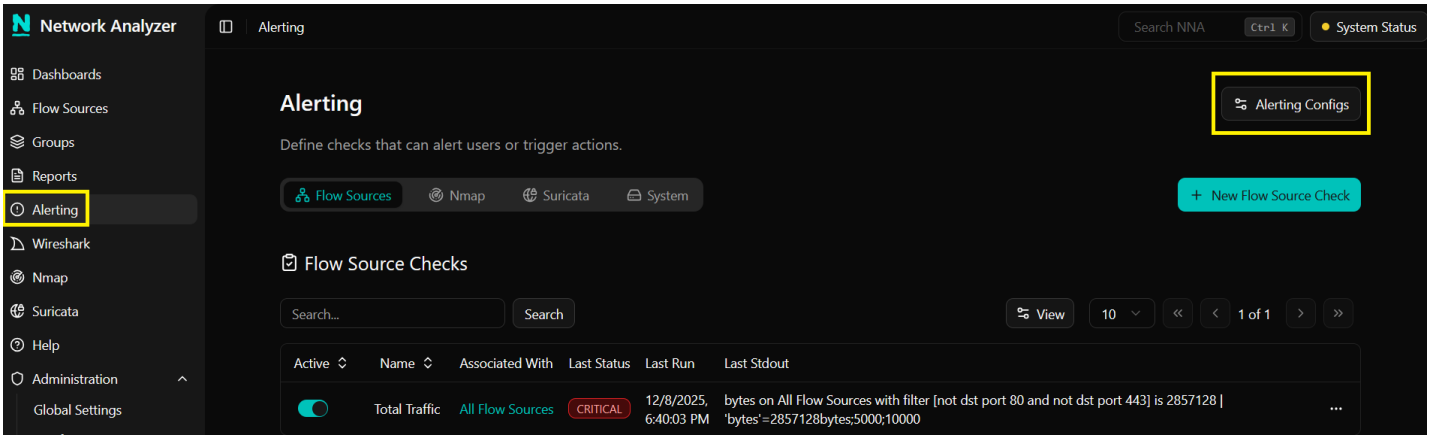
    You can refer to the following documentation to learn how to perform these tasks in Nagios Core: NRDP Overview

Please take note of the **Authentication Token** and **Access Info** found in XI's **Inbound Transfers** menu. The NRDP token and URL will be needed in the following steps.

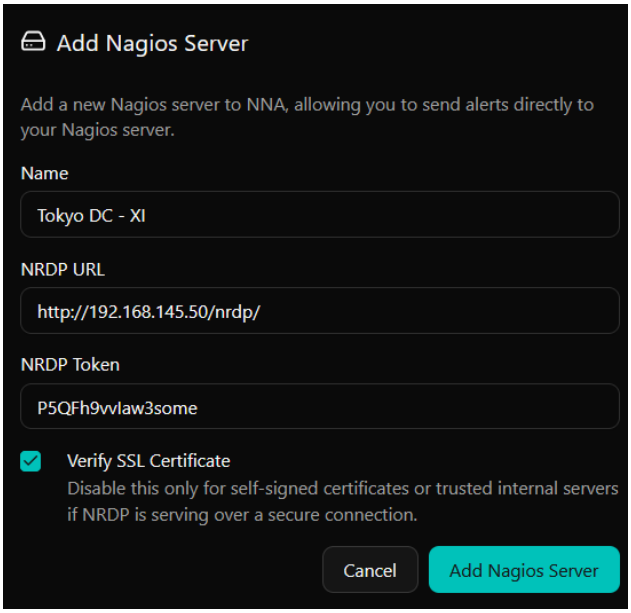


NRDP Setup in Network Analyzer

1. In Nagios Network Analyzer navigate to **Alerting** and then click the **Alerting Configs** button.
2. Click the **New Nagios Server** button in the **Nagios Setup** tab.

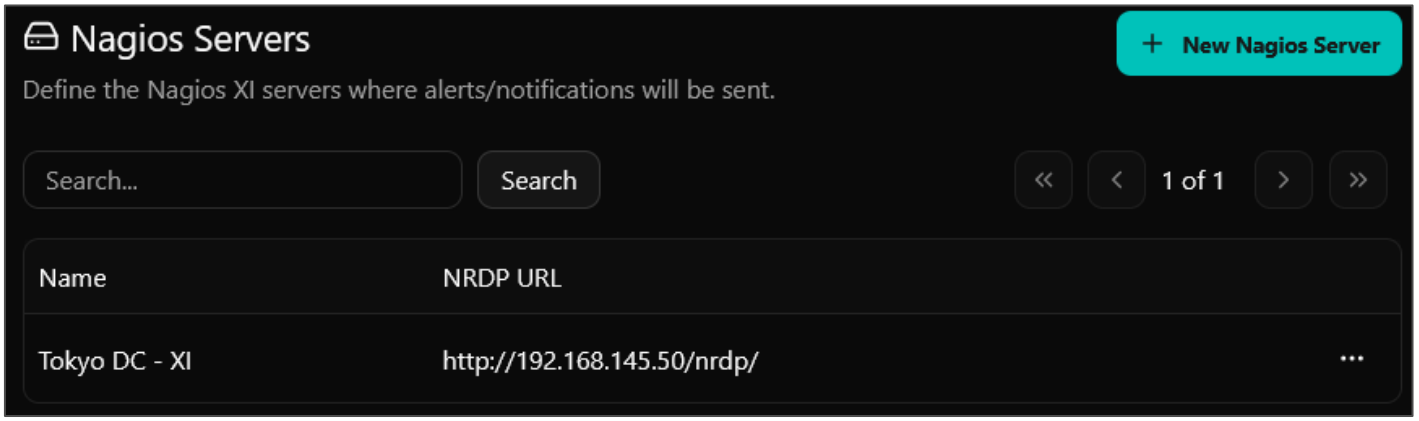


3. Provide the details of the Nagios XI or Core server.
    a. **Name** - The Nagios server's human-readable name which will be used for alerts.
    b. **NRDP URL** - The address where the NRDP results will be sent. Be sure to include the **http://** or **https://**.
    c. **NRDP Token** - The token that Network Analyzer will use when connecting to the NRDP server.
    d. **Verify SSL Certificate** – Disable this option only for self-signed certificates, or when using trusted internal servers if NRDP is server over a secure connection.



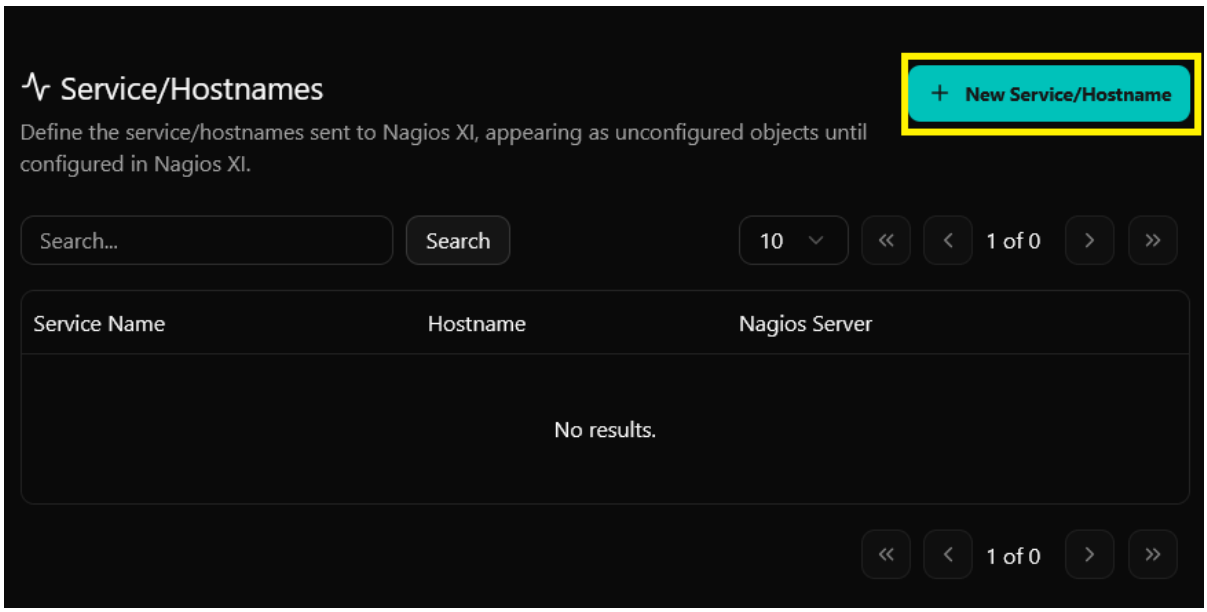
Network Analyzer validates the NRDP server settings by attempting to connect to the NRDP server. If Network Analyzer cannot connect to the server or the token is invalid, it will display a warning.

Once the server has been added successfully, the screen will be updated to include the new server.

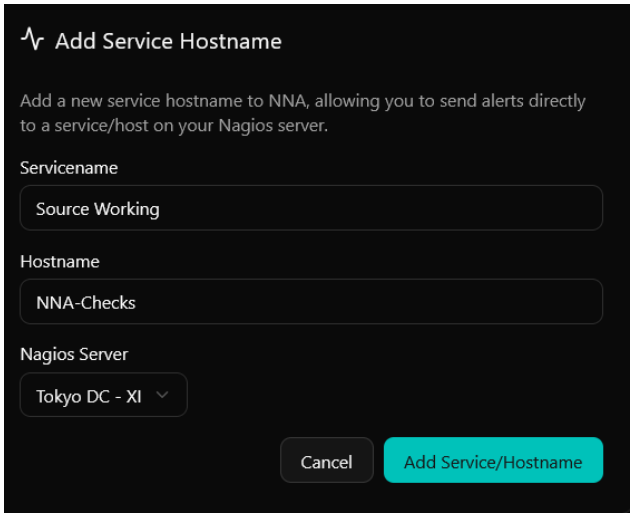


Now that the Nagios Server has been defined a Service/Hostname needs to be defined for NRDP to use to send passive checks to the Nagios Server.

4. Click the **+ New Service/Hostname** button in **Alerting Configs > Service/Hostnames**

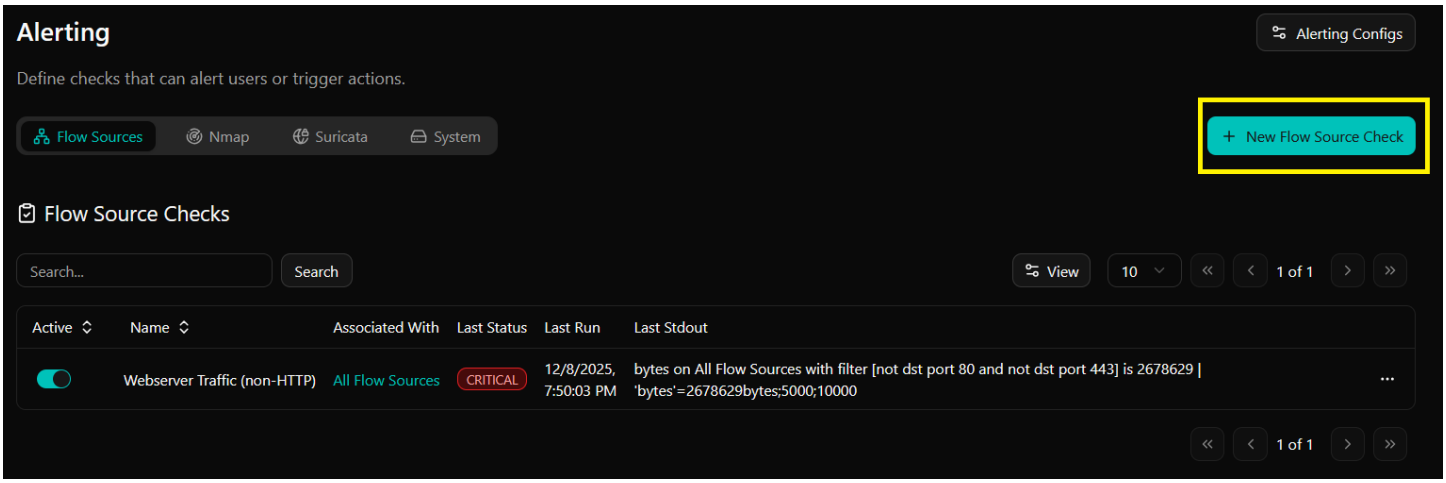


a. **Servicename -** The name of the service that the alert will be sent to in Nagios XI or Core.
b. **Hostname -** The name of the host object that you want the service to be assigned to in Nagios XI or Core.
c. **Server -** The Nagios XI or Core server receiving the alert. Click the **Finish & Save** button to create the Service/Hostname object. The screen will update as shown:



Creating a Check in Network Analyzer

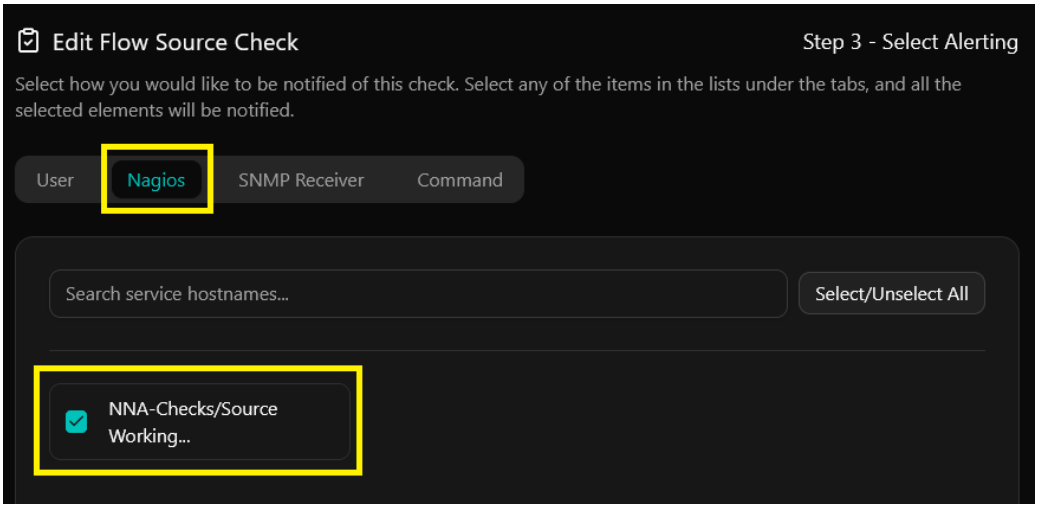
The next step is to create a check in Network Analyzer so Nagios XI or Nagios Core will receive passive check results.



You can learn how to compose checks starting on **page 7** of this guide:

Understanding Alerting in Network Analyzer 2026

Important: In **Step 3** of the check creation dialog, be sure to select the Hostname and Servicename you wish the check to appear as when it reaches your Nagios server:

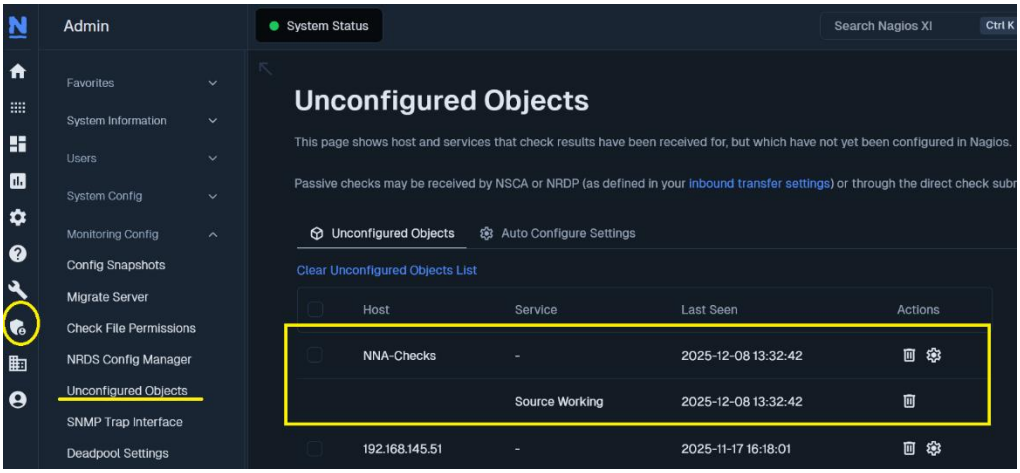


Once created, your Network Analyzer checks run every five minutes. It is important to understand that every five minutes the check will fire off a notification to Nagios XI or Nagios Core. Based on the WARNING and CRITICAL thresholds defined on the check, Nagios will receive the check results with the appropriate state.

Configuring Checks in Nagios XI

Once your check is configured in Network Analyzer, passive results received by Nagios XI from Nagios Network Analyzer via NRDP will appear in the following menu:

Admin > Monitoring Config > Unconfigured Objects



You can learn more about monitoring unconfigured objects here:

Monitoring Unconfigured Objects in Nagios XI

Configuring Checks in Nagios Core

Create passive services to accept the check results. This is outside the scope of this documentation; however, here is a simple example:

```
define service {
        service_description       Source Working
        host_name                 10.25.14.3
        use                       generic-service
        active_checks_enabled           0
        passive_checks_enabled          1
        flap_detection_enabled          0
        check_period              24x7
        max_check_attempts        1
        check_interval             5
        retry_interval            1
        check_freshness           0
        contact_groups            admins
        notification_interval           60
        notification_period       24x7
        notification_options      w,u,c,r
    }
```

Leveraging The Network Analyzer API

Check results can also be queried directly from the Network Analyzer API to retrieve a JSON response. You can use the following command from the Linux command line, replacing `{your-server}` with the IP/FQDN or your Network Analyzer server, `{check ID}` with the `id` of the check you wish to query, and `{your_API_key}` with your API key:

```
curl -X GET "http://{your-server}/api/v1/checks/{check id}" \
-H "Authorization: Bearer {your_API_key}" \
-H "Accept: application/json"
```

Here is an example response:


```
  {
    "id": 1,
    "active": 1,
    "name": "Webserver Traffic (non-HTTP)",
    "object_type": "sourcegroup",
    "object_id": 1,
    "metric": "bytes",
    "warning": "5000",
    "critical": "10000",
    "raw_query": "not dst port 80 and not dst port 443",
    "last_val": null,
    "last_run": "2025-12-09 13:05:05",
    "last_code": 2,
    "last_stdout": "bytes on All Flow Sources with filter [not dst port 80 and not dst port 443] is
758042 | 'bytes'=758042bytes;5000;10000",
    "created_at": null,
    "updated_at": null,
    "check_type": "flow_source",
    "alerting_associations": [
      {
        "id": 1,
        "check_id": 1,
        "association_type": "nagios",
        "association_id": 1,
        "created_at": null,
        "updated_at": null
      }
```


To determine the id numbers of your checks, poll the `/checks` endpoint without specifying an `id`:

```
curl -X GET "http://{your-server}/api/v1/checks" \
-H "Authorization: Bearer {your_API_key}" \
-H "Accept: application/json"
```

To nicely format the response, you can append your command with `| jq`, like this:

```
curl -X GET "http://your-server/api/v1/checks/{check id}" \
-H "Authorization: Bearer {YOUR_API_KEY}" \
-H "Accept: application/json" | jq
```

When used in a script the data in the JSON object can be manipulated as needed.

Nagios Threshold Values

Nagios Thresholds can be complicated to initially understand, however once grasped they can be very powerful. Documentation on Nagios thresholds:

https://nagios-plugins.org/doc/guidelines.html#THRESHOLDFORMAT

The Nagios Threshold standards were designed with many different use cases, for example negative numbers are valid values. However, in the case of Nagios Network Analyzer, the alert value being tested will always be 0 or greater (no negative numbers are involved).

Network Ports

The following network ports are used for communication between Nagios Network Analyzer and Nagios XI or Nagios Core:

- Nagios XI Integration communicates with the Nagios Network Analyzer server on TCP 80 or 443.
- Nagios Network Analyzer when using NRDP for sending passive check to Nagios XI or Nagios Core occurs on TCP 80 or 443.

Finishing Up

This completes the documentation on how to integrate Nagios Network Analyzer with Nagios XI or Nagios Core. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library