

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

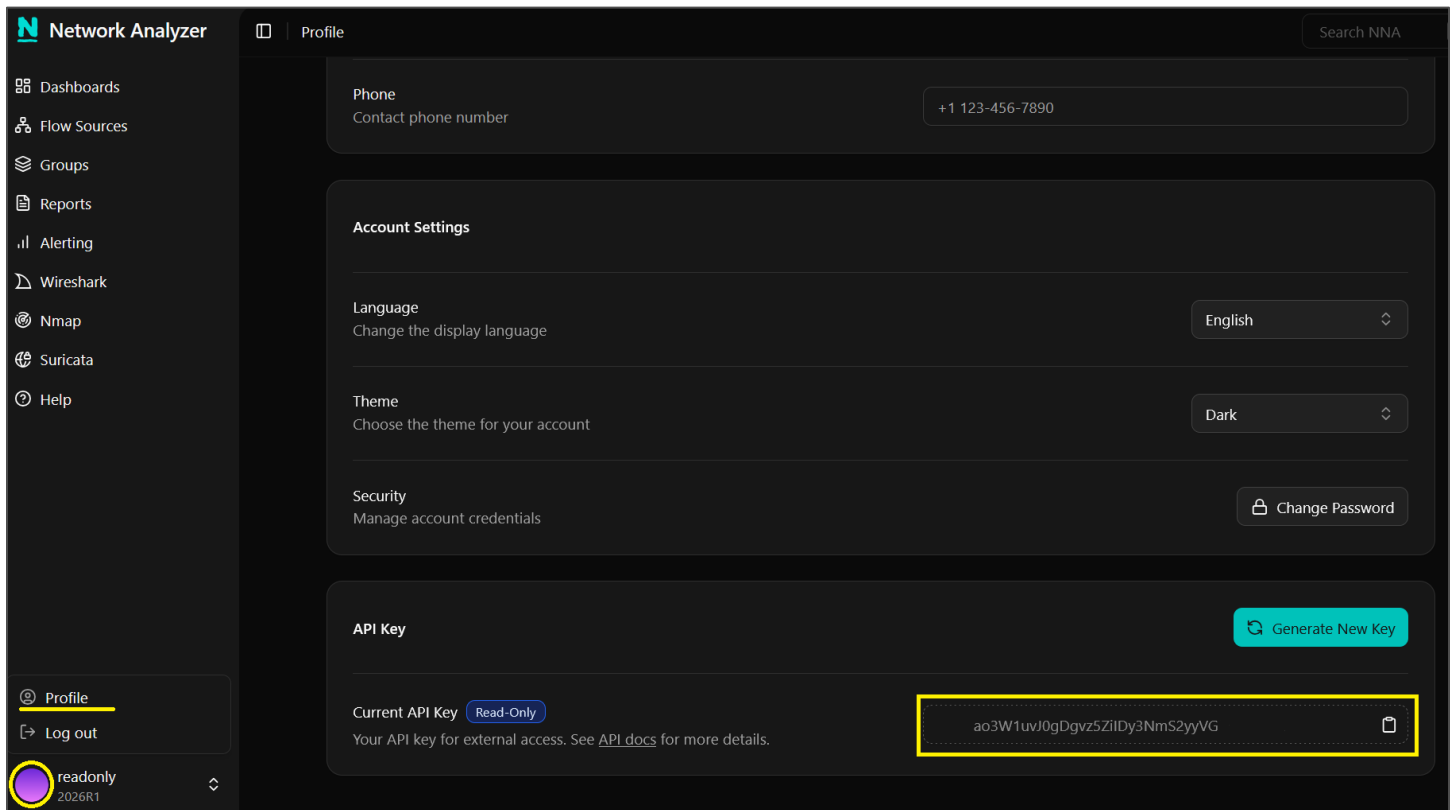
In Nagios XI configure the Nagios Network Analyzer Integration component with the details of your Nagios Network Analyzer server(s). Integration is achieved by using an API key that belongs to a Nagios Network Analyzer user's account that has been granted API access. The first step is to get the API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

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



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**.

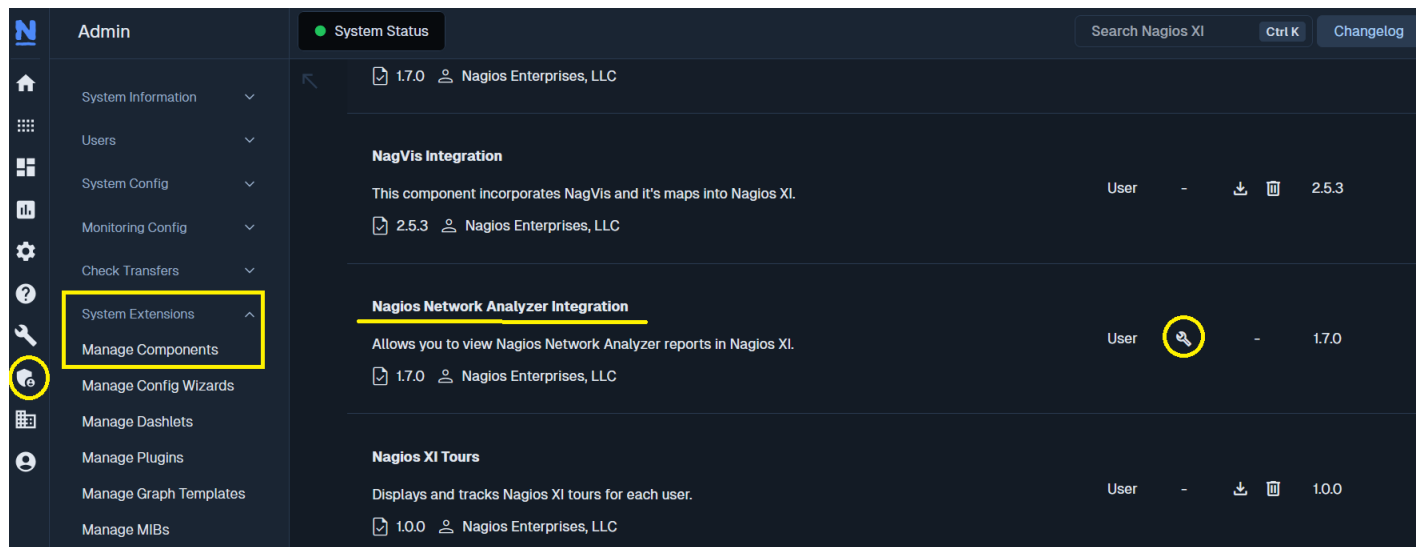
You can learn more about managing Users and Roles here:

[Managing Users in Network Analyzer 2026](#)

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

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 screenshot of the 'Nagios Network Analyzer Integration' settings page. The page has a title bar with a question mark and a star icon. Below the title, there's a 'Component Settings' section with a toggle for 'Disable Host/Service Tabs from being shown'. The main section is 'Nagios Network Analyzer Servers', which includes a description and an 'Add a Server' link highlighted with a yellow box and a yellow arrow. Below this is a table for adding servers with columns for Name, IP Address / Hostname, Version (with a dropdown set to '2026+'), API Key, Use SSL, Allow invalid certificate, Lookback period (set to '4'), and a Remove button. At the bottom are 'Apply Settings' and 'Cancel' buttons.

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

- 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.

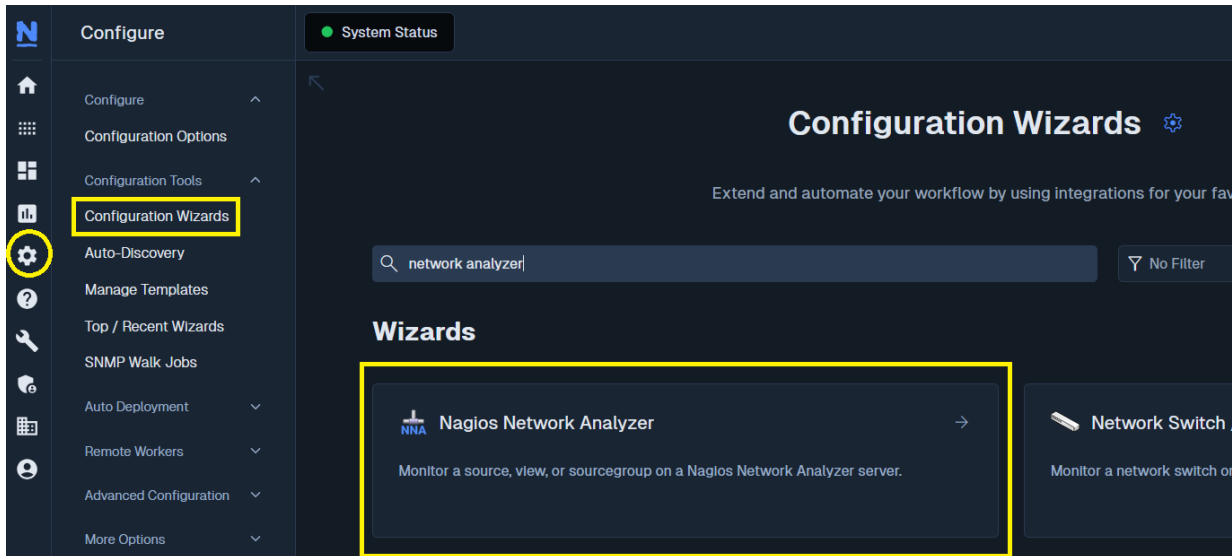
Note that at launch, Network Analyzer 2026 integration is limited to the Network Analyzer wizard, so this setting will only apply to linked Network Analyzer 2024 servers initially.

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

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

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**.

Nagios Network Analyzer Configuration Wizard Step 1

How to Use Nagios Network Analyzer Integration in Nagios XI

Nagios Network Analyzer Server

Select one of your Nagios Network Analyzer server's source, sourcegroup, or view

NNA Server *
NNA-2026

Host Name *
Source Apache Webserver

Next > Cancel

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

- 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.

Nagios Network Analyzer Configuration Wizard Step 2

Nagios Network Analyzer Server

NNA Server
NNA-2026 (192.168.145.57)

Host Name *
NNA Source - Apache Webserver

Select What to Monitor

Select what you would like to monitor.
The graph on the right is provided to help with estimating the warning and critical thresholds.

Default values are created by the following:
Warning Threshold: **20% above max value**,
Critical Threshold: **40% above max value**

<input checked="" type="checkbox"/> Bytes ⓘ	⚠ 8875938 /sec	🔴 10355261 /sec
<input checked="" type="checkbox"/> Flows ⓘ	⚠ 7173 /sec	🔴 8369 /sec
<input checked="" type="checkbox"/> Packets ⓘ	⚠ 34439 /sec	🔴 40179 /sec

< Back Next >

Cancel

Last Week of Bandwidth Data

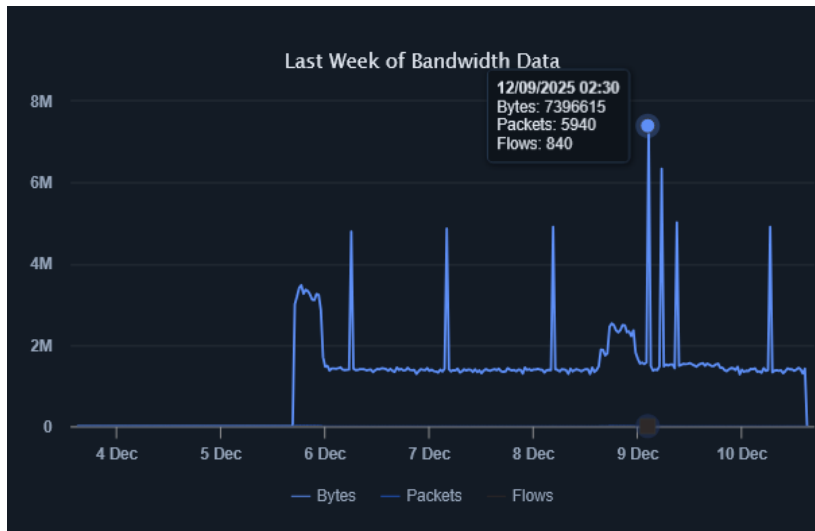
8M
6M
4M
2M
0

4 Dec 5 Dec 6 Dec 7 Dec 8 Dec 9 Dec 10 Dec

— Bytes — Packets — Flows

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

- 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.

● NNA Source - Cent10-fprobe	📄 📄	Bytes	🔊 📄	● Warning	🕒 6s	1/5	2025-12-08 12:29:00	WARNING - 4498666 bytes sent/received
		Flows	🔊 📄	● Ok	🕒 N/A	1/5	2025-12-08 12:29:00	OK - 4370 flows sent/received
		Packets	🔊 📄	● Ok	🕒 N/A	1/5	2025-12-08 12:29:00	OK - 28211 packets sent/received

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

NRDP Passive Checks

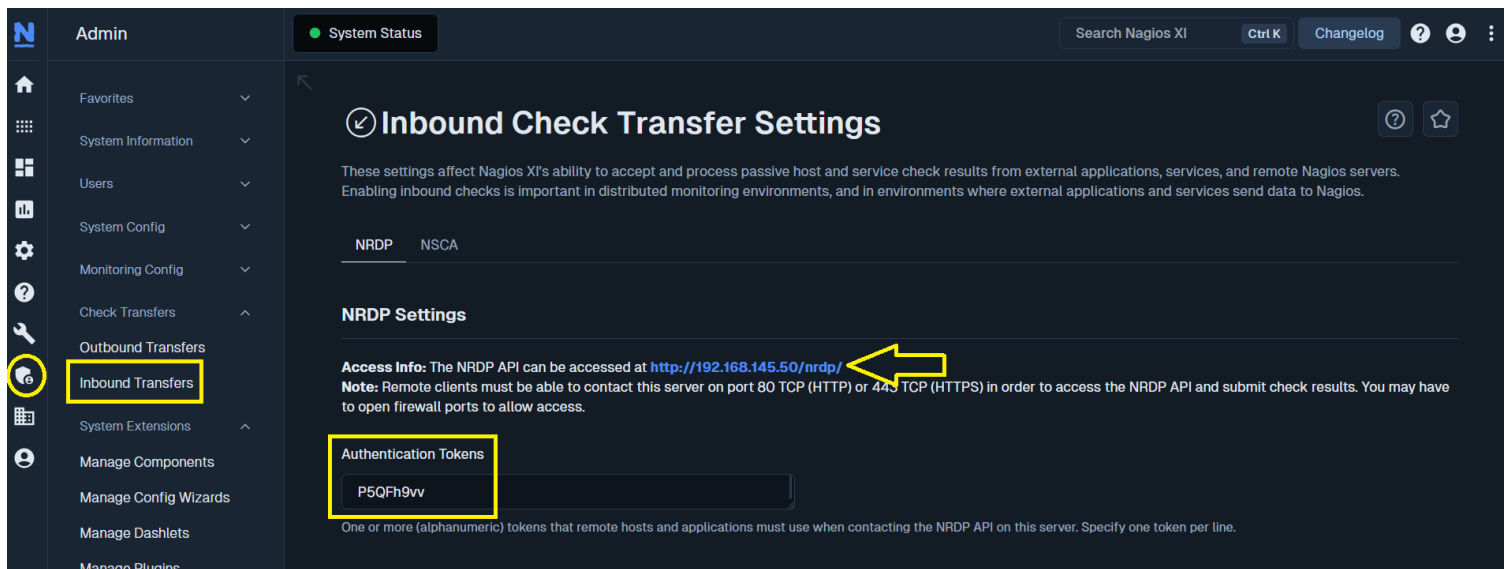
NRDP Setup in Nagios XI and Nagios Core

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.

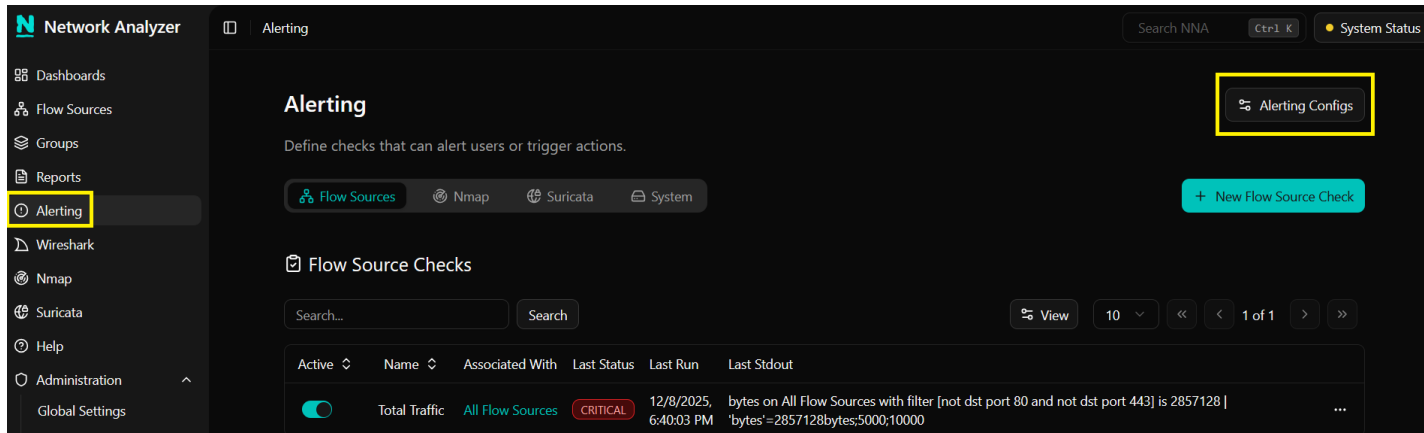


The screenshot shows the Nagios XI Admin interface. On the left sidebar, the 'Inbound Transfers' menu item is highlighted with a yellow box. The main content area is titled 'Inbound Check Transfer Settings'. It features two tabs: 'NRDP' (selected) and 'NSCA'. Under the 'NRDP Settings' section, there is an 'Access Info' field showing the URL 'http://192.168.145.50/nrdp/' with a yellow arrow pointing to it. Below this, there is an 'Authentication Tokens' section with a text input field containing the token 'P5QFh9vv', which is also highlighted with a yellow box. A note at the bottom states: 'One or more (alphanumeric) tokens that remote hosts and applications must use when contacting the NRDP API on this server. Specify one token per line.'

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

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.



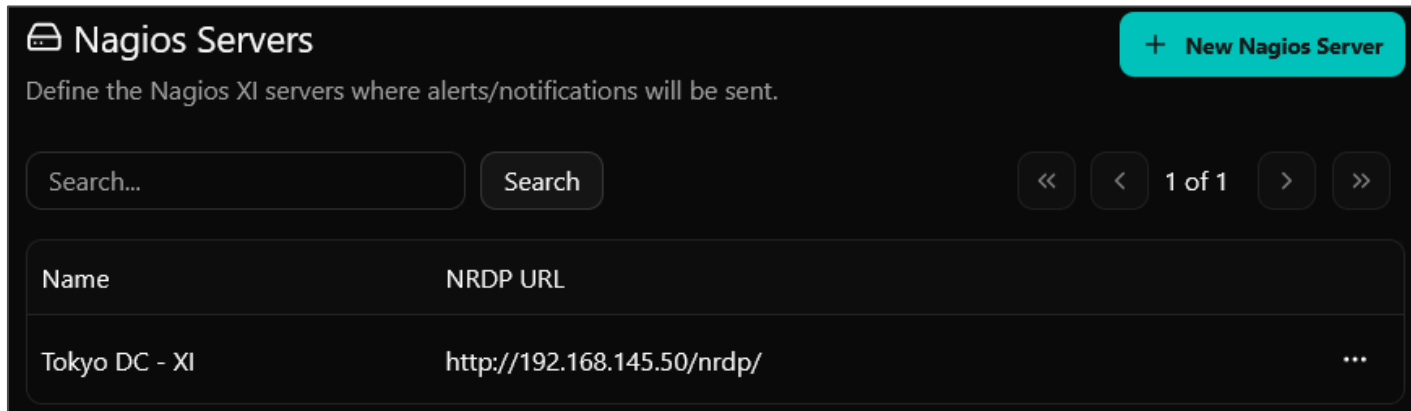
3. Provide the details of the Nagios XI or Core server.
 - a. **Name** - The Nagios server's human-readable name which will be used for alerts.
 - b. **NRDP URL** - The address where the NRDP results will be sent. Be sure to include the **http://** or **https://**.
 - c. **NRDP Token** - The token that 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.

The screenshot shows the 'Add Nagios Server' form in the Nagios Network Analyzer. The form has a title 'Add Nagios Server' and a description: 'Add a new Nagios server to NNA, allowing you to send alerts directly to your Nagios server.' It contains four input fields: 'Name' (filled with 'Tokyo DC - XI'), 'NRDP URL' (filled with 'http://192.168.145.50/nrdp/'), and 'NRDP Token' (filled with 'P5QFh9vvlaw3some'). There is a checkbox labeled 'Verify SSL Certificate' which is checked. Below the checkbox is a note: 'Disable this only for self-signed certificates or trusted internal servers if NRDP is serving over a secure connection.' At the bottom right are two buttons: 'Cancel' and 'Add Nagios Server'.

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.

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

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

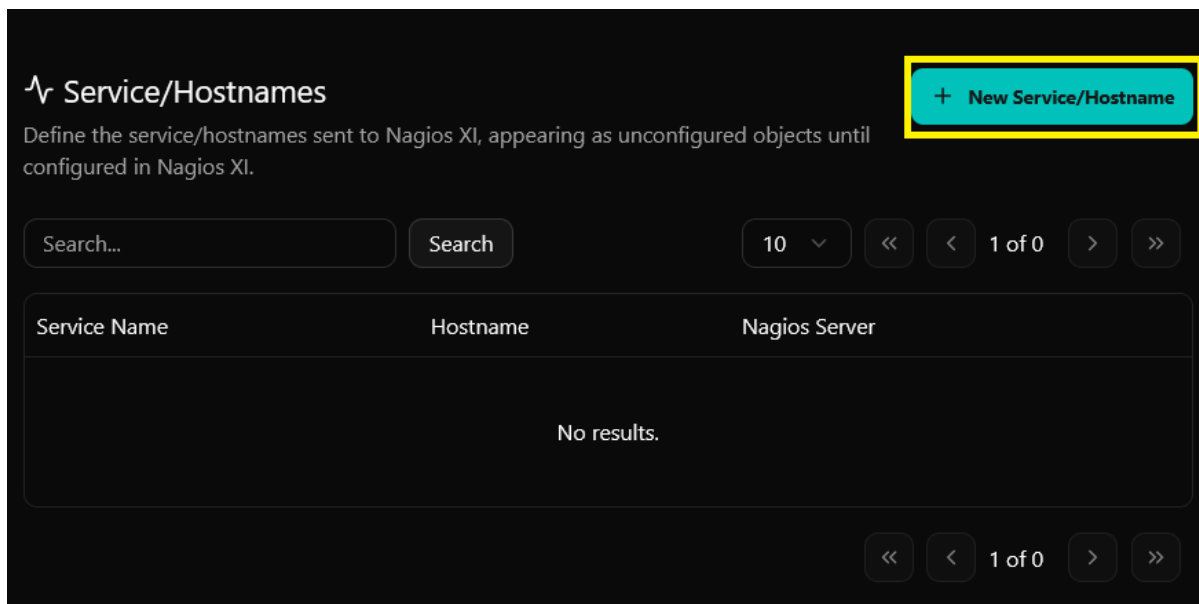


The screenshot shows the 'Nagios Servers' configuration page. At the top, there's a header 'Nagios Servers' with a sub-header 'Define the Nagios XI servers where alerts/notifications will be sent.' and a '+ New Nagios Server' button. Below the header is a search bar with 'Search...' and a 'Search' button. To the right of the search bar are navigation buttons: '<<', '<', '1 of 1', '>', and '>>'. The main content area is a table with two columns: 'Name' and 'NRDP URL'. There is one row with the data: 'Tokyo DC - XI' and 'http://192.168.145.50/nrdp/'. A three-dot menu icon is visible at the end of the row.

Name	NRDP URL
Tokyo DC - XI	http://192.168.145.50/nrdp/

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**

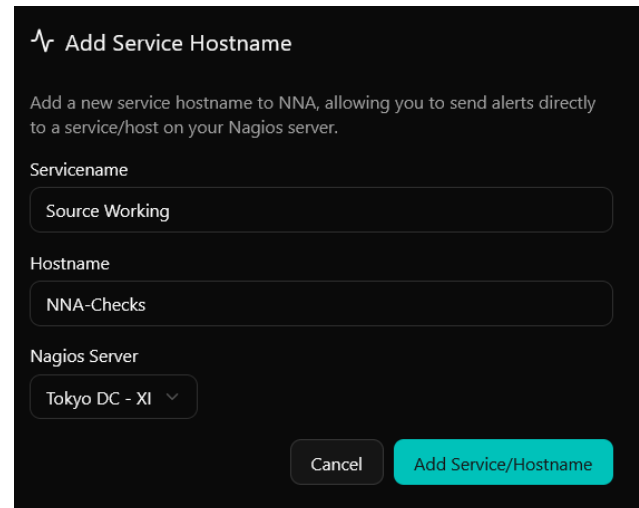


The screenshot shows the 'Service/Hostnames' configuration page. At the top, there's a header 'Service/Hostnames' with a sub-header 'Define the service/hostnames sent to Nagios XI, appearing as unconfigured objects until configured in Nagios XI.' and a '+ New Service/Hostname' button highlighted with a yellow box. Below the header is a search bar with 'Search...' and a 'Search' button. To the right of the search bar are navigation buttons: '10' with a dropdown arrow, '<<', '<', '1 of 0', '>', and '>>'. The main content area is a table with three columns: 'Service Name', 'Hostname', and 'Nagios Server'. The table is empty, and the text 'No results.' is displayed in the center. At the bottom right, there are navigation buttons: '<<', '<', '1 of 0', '>', and '>>'. The table structure is as follows:

Service Name	Hostname	Nagios Server
No results.		

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

- Servicename** - The name of the service that the alert will be sent to in Nagios XI or Core.
- Hostname** - The name of the host object that you want the service to be assigned to in Nagios XI or Core.
- 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:



Add Service Hostname

Add a new service hostname to NNA, allowing you to send alerts directly to a service/host on your Nagios server.

Servicename
Source Working

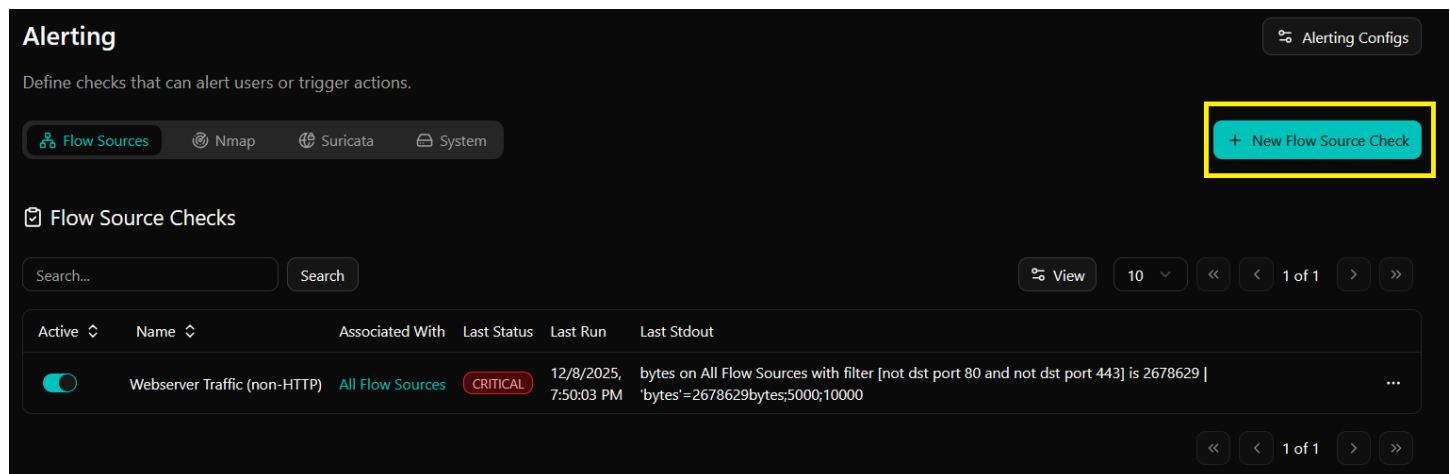
Hostname
NNA-Checks

Nagios Server
Tokyo DC - XI

Cancel Add Service/Hostname

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.



Alerting

Define checks that can alert users or trigger actions.

Flow Sources Nmap Suricata System

+ New Flow Source Check

Flow Source Checks

Search... Search View 10 1 of 1

Active	Name	Associated With	Last Status	Last Run	Last Stdout
<input checked="" type="checkbox"/>	Webserver Traffic (non-HTTP)	All Flow Sources	CRITICAL	12/8/2025, 7:50:03 PM	bytes on All Flow Sources with filter [not dst port 80 and not dst port 443] is 2678629 bytes=2678629bytes:5000;10000

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

[Understanding Alerting in Network Analyzer 2026](#)

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

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:

Edit Flow Source Check Step 3 - Select Alerting

Select how you would like to be notified of this check. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

User **Nagios** SNMP Receiver Command

Search service hostnames... Select/Unselect All

☒ NNA-Checks/Source Working...

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

Unconfigured Objects

This page shows host and services that check results have been received for, but which have not yet been configured in Nagios.

Passive checks may be received by NSCA or NRDP (as defined in your [inbound transfer settings](#)) or through the direct check sub...

☒ Unconfigured Objects ☐ Auto Configure Settings

[Clear Unconfigured Objects List](#)

<input type="checkbox"/>	Host	Service	Last Seen	Actions
<input type="checkbox"/>	NNA-Checks	-	2025-12-08 13:32:42	
<input type="checkbox"/>		Source Working	2025-12-08 13:32:42	
<input type="checkbox"/>	192.168.145.51	-	2025-11-17 16:18:01	

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

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"
```

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

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"
```

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

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](#)