

Configuring Inbound Checks in Nagios XI 2024

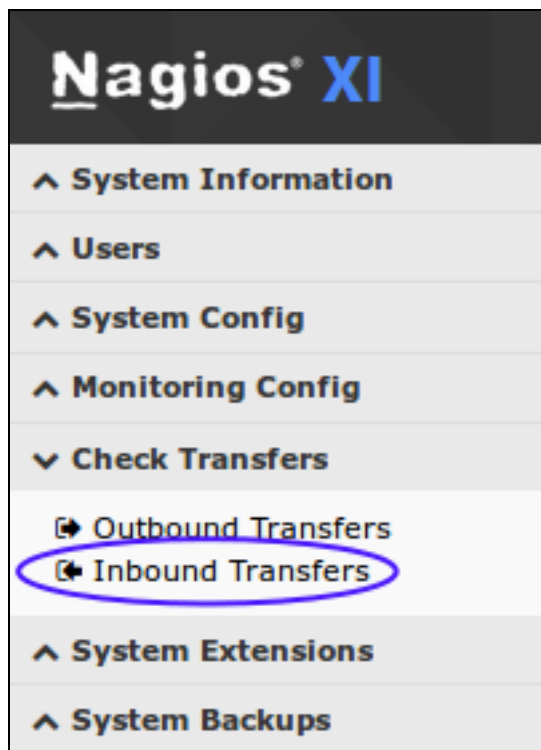
Inbound Transfer APIs

There are two different APIs for handling inbound check transfers (passive checks) in Nagios XI:

NRDP

- NRDP is a newer web-based API that operates over port 80 (HTTP) or 443 (HTTPS)
- NSCA
 - NSCA operates over TCP port 5667, and while it is older than NRDP, it is supported by many more Nagios addons than the newer NRDP API

Both methods provide the same functionality however NRDP is the method we recommended using. The main reason why is that NRDP is easy to setup, configure and maintain in the long term.



Accessing Transfer Settings

You can configure inbound transfers by navigating to **Admin > Check Transfers > Inbound Transfers** in the interface of Nagios XI.

The Inbound Transfers settings page allows you to configure both the [NRDP](#) and [NSCA](#) APIs.

NRDP Configuration

External applications, services, and remote servers must use an authentication token when sending check results to the NRDP API.

1. You can configure multiple authentication token to support different client if you wish. The first time you configure NRDP, a random token will be generated for you. You can change the token to an alpha-numeric string of your choosing.

2. Click the **Update Settings** button to save the NRDP settings.

Inbound Check Transfer Settings

These settings affect Nagios XI's ability to accept and process passive host and service check results from external applications, services, and remote Nagios servers. Enabling inbound checks is important in distributed monitoring environments, and in environments where external applications and services send data to Nagios.

NRDP NSCA

NRDP Settings

Access Info: The NRDP API can be accessed at <http://192.168.4.18/nrdp/>
Note: Remote clients must be able to contact this server on port 80 TCP (HTTP) or 443 TCP (HTTPS) in order to access the NRDP API and submit check results. You may have to open firewall ports to allow access.

Authentication Tokens: 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.

gmr57|78796m0

Update Settings Cancel

NSCA Configuration

Before you can enable inbound check transfers via the NSCA API, you must configure your Nagios XI server as follows.

1. Establish a terminal session to your Nagios XI server as the root user. Edit the `/etc/xinetd.d/nsca` file in the vi editor using the following command:

```
vi /etc/xinetd.d/nsca
```

When using the vi editor, to make changes press `i` on the keyboard first to enter insert mode. Press `Esc` to exit insert mode.

2. Modify the `only_from` statement to include the IP addresses of hosts that are allowed to send data (or comment it out to allow all hosts to send data). This is a space separated list, for example:

```
only_from = 127.0.0.1 10.25.18.22 10.25.18.23
```

When you have finished, save the changes in vi by typing:

```
:wq
```

and press Enter.

Restart the xinetd service using the following command:


```
service xinetd restart
```

Once you've made these changes **Navigate to the NSCA** tab on the Inbound Transfers page. External applications, services, and servers that send passive checks results to Nagios XI using the NSCA API should encrypt the transmitted data.

The Nagios XI server and each client must be using the same:

- Decryption / encryption method
- Password

3. Click the **Update Settings** button to save your settings.



Inbound Check Transfer Settings

These settings affect Nagios XI's ability to accept and process passive host and service check results from external applications, services, and remote Nagios servers. Enabling inbound checks is important in distributed monitoring environments, and in environments where external applications and services send data to Nagios.

NRDP

NSCA

NSCA Settings

▲ Configuration Required
 Before you can enable inbound data transfer via NSCA, you must configure settings to allow external hosts/devices to communicate with NSCA.

To do this, follow these steps:

1. Login to the Nagios XI server as the `root` user
2. Open the `/etc/xinetd.d/nsca` file for editing
3. Modify the `only_from` statement to include the IP addresses of hosts that are allowed to send data (or comment it out to allow all hosts to send data)
4. Save the file

I have completed these steps.

Access Info: NSCA is configured to run on this machine on port **5667 TCP**.
Note: Remote clients must be able to contact this server on port 5667 TCP in order to access NSCA and submit check results. You may have to open firewall ports to allow access.

Decryption Method: None (Not secure) ▼
 The decryption method used on check data that is received via NSCA.
Important: Each sender must be using the same encryption method as you specify for the decryption method here.

Password: ••••••
 The password used to decrypt check data that is received by NSCA.
Important: Each sender must be using this same password.

Update Settings

Cancel

Firewall Configuration

Modification of firewall settings between the remote data sources and the Nagios XI server may be required in order to allow inbound check results to be sent to Nagios XI.

The NRDP works on TCP port 80 using the HTTP protocol OR TCP port 443 the HTTPS protocol.

NSCA uses a custom protocol that runs on TCP port 5667.

Firewalls must be configured to allow inbound and outbound traffic over the ports used by the API(s) you choose to utilize for handling inbound checks.

Configuring Objects

Nagios XI must be configured to monitor hosts and services that it received passive check results for. If it is not configured with a host or service when a passive check arrives, Nagios XI will add that host or services to a list of Unconfigured objects (Admin > Monitoring Config > Unconfigured Objects). Until this is done, Nagios XI will not do anything with the check results it receives.

The Nagios XI administrator can then easily configure the host and service in the monitoring engine. Further information can be found in the following documentation:

[Monitoring Unconfigured Objects With Nagios XI](#)

Complimentary Documentation

Nagios XI can also send check results to another Nagios XI server. This is explained in detail in the following documentation:

[Configuring Outbound Checks With Nagios XI](#)