Purpose

This document describes how to install the Nagios Cross Platform Agent (NCPA) Version 3 on Windows, Linux and Mac OS X. NCPA is intended to simplify and universalize agent-based monitoring across different operating systems.

NCPA Installation Overview

This documentation covers installing NCPA using the ready-built packages for the following platforms:

- Windows 8+ / Windows Server 2016+
    - EXE Package
    - EXE Package (Silent)
- Linux
    - RHEL / CentOS / Oracle 7+, SUSE 15+
        - Nagios Repository
        - RPM Package
    - Ubuntu 20+/ Debian 9+
        - Nagios Repository
        - DEB Package
- Mac OS X 10.11+
    - DMG Package
- AIX, Solaris, and Legacy Linux Versions
    - NCPA v2

Active Vs Passive

NCPA can be used for both Active and Passive monitoring:

- **Active** = Nagios is responsible for performing the check on a schedule
- **Passive** = NCPA is responsible for submitting check results upstream to Nagios

The NCPA installer may prompt you for settings for active and passive. Active is the most common method used. If you are not using passive monitoring then you do not need to configure those settings.

Downloading NCPA Packages

Please visit the downloads page to find the relevant package for your operating system (OS):
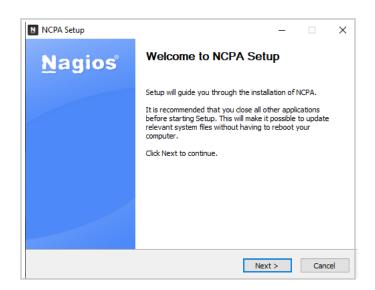
NCPA Downloads

If you are installing NCPA on Linux then the steps below for each Linux distribution will show you how to download the package at the command line, you do not need to download it right now.

Installing NCPA on Windows

The following instructions are for the graphical install of NCPA. If you wish to perform a silent installation please proceed to the Silent Install section.

1. Navigate to the location that the installer package was downloaded to and double-click the installer, this will bring up the Welcome screen.

   Click **Next** to continue.

Nagios®

2. The license agreement will be shown.

    Click **I Agree**.

3. The only setting that is required here is a **Token**. This is what your Nagios server will use to authenticate with NCPA.

    The Bind IP of 0.0.0.0 means that NCPA will listen on all Ipv4 addresses on the Windows machine. The default port of 5693 is used.
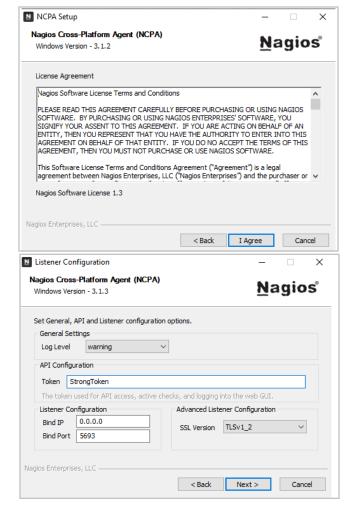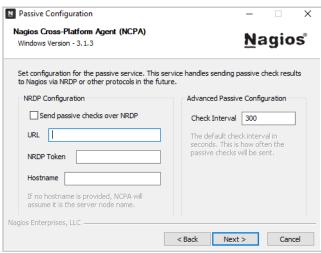
    Click **Next** to proceed.

4. The configuration screen for **Passive** checks will be shown. If you wish to use passive checks, you will need to check the **Send passive checks over NRDP** box to enable passive checks. You will also need to provide the following NRDP settings:

-   **URL:**

    This is the URL on your Nagios Host that accepts passive check results to be submitted.

-   **NRDP Token**

    This is the token you will be using when passing NCPA passive checks to Nagios for NRDP to accept the check. This is separate from the token that was provided for active checks.

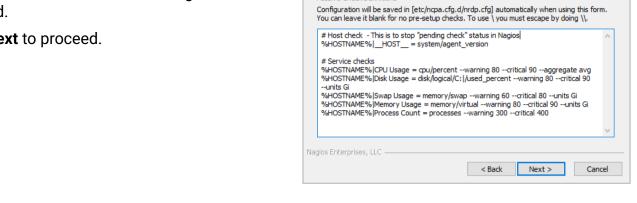The URL and NRDP token in Nagios XI are configured via **Admin** > **Check Transfers** > **Inbound Transfers**.

- **Hostname**

The hostname that the passive checks belong to on the Nagios server. Click **Next** to proceed.

5. Continuing with Passive checks, you will be presented with the default passive service checks that will be executed and send to your Nagios server. These can be changed if required.
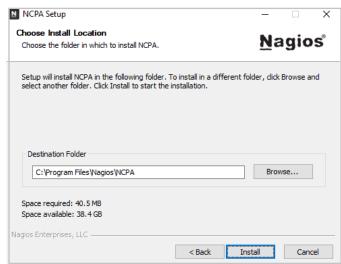
Click **Next** to proceed.

6. You will be presented with the install location. Change the destination folder if required.

Click the **Install** button to install NCPA.
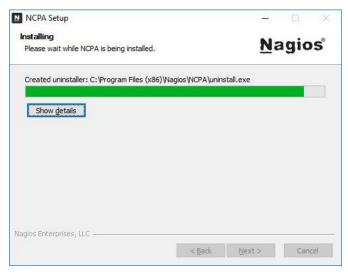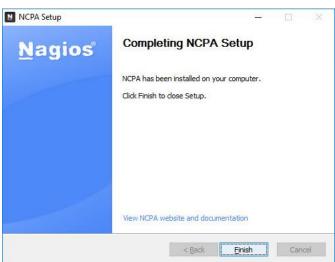
7. Wait while NCPA is installed and configured.

8. Click **Finish** once NCPA has been installed.

The Windows Installer will automatically add a port permission for the **Bind Port** specified (port 5693 by default). This is the port Nagios will use to communicate with NCPA, and the port you will use to access the Web GUI.

Nagios®

Installing NCPA on Windows - Silent

The installer also supports a silent install, which allows system administrators to easily manage their network workstations without disrupting the workflow of the office. The following arguments are currently supported:

Directive	Explanation
/S	This is how you tell the installer you are performing a silent install
/D	The directory to install NCPA to. This is optional, must be the last argument, cannot contain quotes, and must be an absolute path.
/TOKEN	The token that will be used to access the agent's API and web interface
/IP	The IP address to bind to. The default is **0.0.0.0** which binds to all IPv4 addresses. Use **::** for binding to IPv6 addresses.
/PORT	The port to bind to. The default is **5693**.
/NRDPURL	This is the URL on your Nagios Host that accepts passive check results to be submitted
/NRDPTOKEN	This is the token you will be using when passing NCPA passive checks to Nagios for NRDP to accept the check. This is separate from the token that was provided for active checks.
/NRDPHOSTNAME	The hostname that the passive checks belong to on the Nagios server

Here is an example employing NRDP settings for passive checks. Note that this is a single long command, and that you will need to replace the arguments with your own NRDP and NCPA settings:

```
ncpa-latest.exe /S /TOKEN='Str0ngT0k3n' /NRDPURL='http://10.25.5.12/nrdp/'/
NRDPTOKEN='NRDP_T0k3n' /NRDPHOSTNAME='S1601'
```

The Windows Installer will automatically add a port permission for the Bind Port specified (port 5693 by default). This is the port Nagios will use to communicate with NCPA, and the port you will use to access the Web GUI.

There are several methods for installing NCPA on Linux depending on your OS distribution. You will need to establish a terminal session as a `root` user to complete these steps.

Installing NCPA on RPM-Based Linux

Using the Nagios Repository (Recommended)

The Nagios Repository can be used to install NCPA on RHEL / CentOS / Oracle Linux 7+ and SuSE 15+. The first step is to install the repository by following the steps outlined in the **Installation of Nagios Repo** section of the Nagios Repositories page for your version of Linux:

Once the repository has been installed you will need to execute the following command to install NCPA:

```
yum install ncpa -y
```

Now that NCPA has been installed please proceed to the Configuring NCPA section of this document.

Manual RPM Installation

An RPM package can be used to manually install NCPA on RHEL / CentOS / Oracle Linux 7+ and SUSE 15+. Begin by downloading the latest RPM to your `/tmp` directory, using `wget` from the command line, replacing `<version and arch>.rpm` with the actual name of the file:

```
cd /tmp
wget https://assets.nagios.com/downloads/ncpa3/<version and arch>.rpm
```

Next, install the RPM package using the `rpm` command:

```
rpm -ivh /tmp/ncpa-<version and arch>.rpm
```

Now that NCPA has been installed please proceed to the Configuring NCPA section of this document.

Installing NCPA on Deb-Based Linux

Using the Nagios Repository (Recommended)

The Nagios Repository can be used to install NCPA on Debian 9+ and Ubuntu 20+ Linux. The first step is to install the repository by following the steps outlined in the **Installation of Nagios Repo** section of the Nagios Repositories page for your version of Linux.

Once the repository has been installed you will need to execute the following command to install NCPA:

```
apt-get install ncpa
```

Now that NCPA has been installed please proceed to the Configuring NCPA section of this document.

Manual DEB Installation

A DEB package can be used to manually install NCPA on Debian 9+ and Ubuntu 20+ Linux. Begin by downloading the latest DEB file to your `/tmp` directory, using `wget` from the command line, replacing `<version and arch>.rpm` with the actual name of the file:

```
cd /tmp
wget https://assets.nagios.com/downloads/ncpa3/<version and arch>.rpm
```

Next, install the DEB package using the `dpkg` command:

```
dpkg -i /tmp/ncpa-<version and arch>.deb
```

Now that NCPA has been installed please proceed to the Configuring NCPA section of this document.

Installing NCPA on OSX

A DMG package can be used to install NCPA on Mac OS X. At this time, the installation on Mac requires root permissions (can be done via sudo) and needs to run using the cmdline. First download the latest DMG file and **mount it**. Then run the following command:

```
sudo zsh /Volumes/ ncpa-latest.x86_64.dmg /install.sh
```

Unlike Windows installer there is currently no "click and go" installation method. However, the script handles both install and upgrades. It does the following for you:

- Creates the nagios user and nagios group (if necessary)
- Creates the `/usr/local/ncpa` directory (if necessary) and moves all NCPA files to that location
- Sets permissions on `/usr/local/ncpa` to `nagios:nagios` and `775`
- Sets up services that auto-start for both Listener and Passive services and manually starts them

Once successfully installed, you can unmount the NCPA installer and continue to the web GUI.

Now that NCPA has been installed please proceed to the Configuring NCPA section of this document.

AIX, Solaris, and Legacy Linux Versions

Although not yet supported in NCPA v3, there are NCPA v2 packages for AIX, and Solaris. NCPA 2 downloads for AIX, Solaris, and older Linux versions can be found here in the Download Archive, and the NCPA v2 guide can be found here. You can also install NCPA from source by following the Building NCPA documentation.

Configuring NCPA

This section is specifically for the Linux / Mac OS X installations as they do not provide configuration options as part of the installer. However the configuration file in Windows is the same, hence the information here is also valid for Windows.

This documentation will only focus on configuring NCPA for Active checks. Passive checks are covered in the following documentation:

Using NCPA For Passive Checks

The NCPA configuration file is located here:

```
/usr/local/ncpa/etc/ncpa.cfg
```

Execute the following command to open the file in vi:

```
sudo vi /usr/local/ncpa/etc/ncpa.cfg
```

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

Find the following line:

```
community_string = mytoken
```

Change it to your required token, for example:

```
community_string = Str0ngT0k3n
```

When you have finished, exit insert mode by pressing **Esc**, then save the changes in vi by typing:

```
:wq
```

and press **Enter.**

You will now need to restart the ncpa service for these changes to take affect, please proceed to the Restart Service section of this documentation.

NAGIOS®

Restart Service

The command required for this will differ depending on your OS and version:

RHEL / CentOS / Oracle Linux

```
systemctl restart ncpa
```

Ubuntu

```
sudo systemctl restart ncpa
```

Debian

```
systemctl restart ncpa
```

Mac OS X

```
sudo launchctl stop com.nagios.ncpa
sudo launchctl start com.nagios.ncpa
```

Now that the ncpa_listener service has been restarted please proceed to the [Configure Firewall - Linux](#) section of this document.

Nagios®

Configure Firewall – Linux

A firewall rule needs to be created on your Linux machine to allow incoming traffic to NCPA on TCP Port 5693. The command required for this will differ depending on your OS and version.

RHEL / CentOS / Oracle Linux

```
firewall-cmd --zone=public --add-port=5693/tcp
firewall-cmd --zone=public --add-port=5693/tcp --permanent
```

Debian

```
iptables -I INPUT -p tcp --destination-port 5693 -j ACCEPT
apt-get install -y iptables-persistent
```

Answer yes to saving existing rules.

Ubuntu

```
sudo ufw allow 5693/tcp
```

Mac OS X

The firewall is not enabled by default and allows port 5693.

Now that the firewall has been defined please proceed to the Test NCPA section of this document.

Test NCPA

To ensure that the installation was successful and NCPA is now listening, try accessing the web interface of the agent. In order to do this you will need to know:

- The IP Address of the machine you installed NCPA on
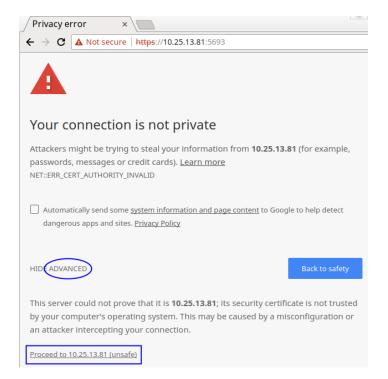- The token / community_string you configured NCPA to use

Open a web browser and connect to the NCPA web interface using the following URL:

```
https://<NCPA IP Address>:5693/
```

You will be presented with a security message. This is completely **OK** and expected. NCPA is using self signed certificates as it allows the communication to be encrypted. Your web browser is warning you because it does not know about the certificate.

You will need to click **Advanced** and then **Add Exception** or **Proceed to xxx** to allow you to use the NCPA page.
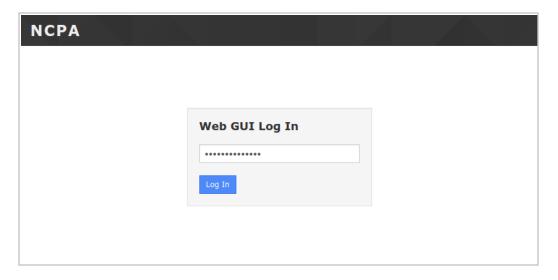
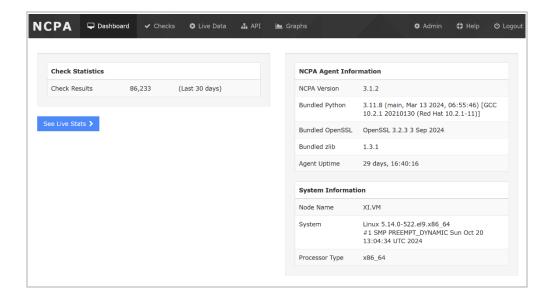More information on certificates is explained in the Understanding Certificate Warnings KB article.

Nagios®

You will then be shown the NCPA login page. Type the token in the field and then click the **Log In** button:

Once you log in you will be placed on the Dashboard page with a summary of the NCPA version and machine it is running on:

Congratulations, NCPA is now ready to be monitored by Nagios.Please proceed to the Configuring Nagios section of this document.

Configuring Nagios

Configuring Nagios

Now that NCPA is installed on the remote machine, you can monitor the machine using the NCPA monitoring wizard in Nagios XI. Please refer to the following documentation for detailed steps:

Monitoring Devices Using The NCPA Agent And Nagios XI

The NCPA agent has built-in documentation in web interface, this is located on the **Help** tab. This gives the options to view or change configuration settings remotely as well as access additional info on NCPA.

Finishing Up

This completes the documentation on Installing NCPA v3. 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