TITANIA NIPPER

Titania Nipper CLI Guide

Software Version: 2.13.X

Last updated: October 10, 2023

TITANIA

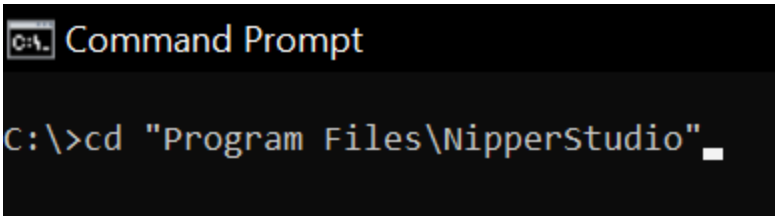
CLI Guide

This guide is to assist with the usage of Nipper when using Command Prompt (Windows) or Terminal (Linux). The commands for Windows and Linux are the same. There are multiple parts to the guide, with activating your license, adding files to audit with Nipper etc.

Locating Nipper

After you have installed Nipper to get started with using CMD/Terminal you will need to navigate to the install directory. With Linux you may not have to navigate to the directory so you will be able to run any commands from your home directory in Linux.

Windows:



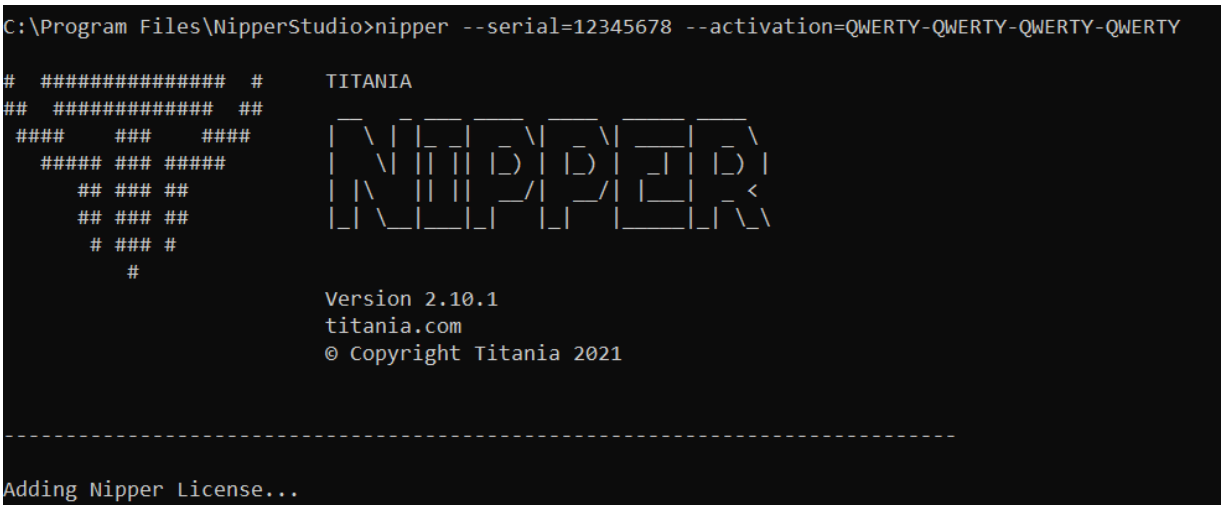
Linux:

Adding a license into Nipper

To audit devices in Nipper you will need to activate a license, to do this you will need the Serial Number and Activation Code. This can be found either by email from Titania, or on your account on our website: www.titania.com

Once you've got your Serial and Activation you will need to enter the below into Nipper with your details:

```
Nipper --serial=xxxxxxxx --activation=xxxxx-xxxxx-xxxxx-xxxx
```



Once you have done the above you will be able to use Nipper.

Setting Reports

When auditing a device, you can specify the reports you would like before, for the full list of reports run the command

```
nipper --help=report
```

Below are some examples of code to disable/enable reports:

All reports enabled:

```
nipper --all-reports=on
```

Security report disabled:

```
nipper --security=off
```

Auditing a singular device

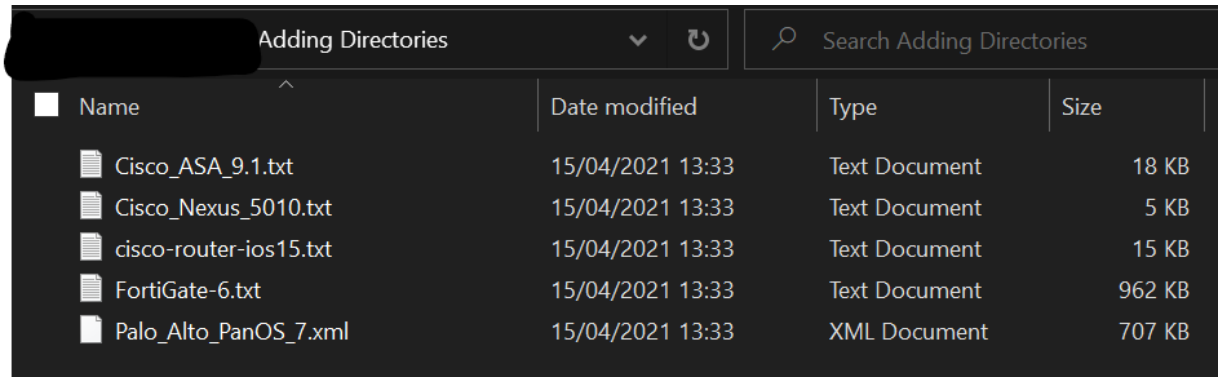
Here we will add a singular device, you can also set what reports you would like to use in the same command, example of an audit for a Cisco ASA below:

```
nipper --input="C:\Program Files\NipperStudio\demo-files\Cisco_ASA_9.1.txt" --secur-
ity=on --output="C:\Program Files\NipperStudio\demo-files\Cisco Audit.html
```

To start these, you will need to specify an input, which has to be to the directory of the device, you will need permission to access this file. Then afterwards you can specify what reports you want, or if you have already specified these prior, you only need to add the output which can be any directory you have write access too, you will need to specify the file extension, we would recommend .html if you are looking to review the report.

Auditing a Directory

When using the CLI to audit Nipper, you will need to first need to create or use a current directory which Nipper will have access to, I have already created one as shown below:



After doing this you will need to specify the directory in the “--input=” command, a full example is below:

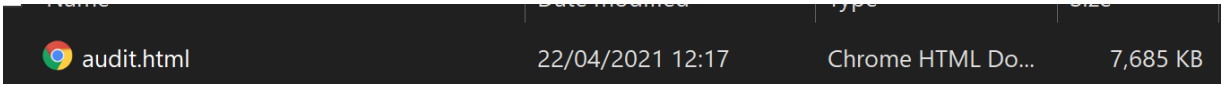
```
C:\Program Files\NipperStudio>nipper --input="C:\Adding Directories" --output="C:\Adding Directories\audit.html"
```

Specify the Directory

```
nipper --input="C:\Adding Directories" --output="C:\Adding Directories\audit.html
```

Nipper will then read the directory, it will not read any other directories in this path, and then audit any configurations inside of this. This is similar to adding singular devices where you can specify the reports in between the input and output

It will then output the report, in any supported extensions:



Scope of the audit, showing every device that was in the directory:

Device	Name	OS
Cisco Router	CiscoIOS15	IOS 15.0
Cisco Adaptive Security Appliance Firewall	Office-Cisco-ASA	ASA 9.1(1)
Cisco Nexus	TitaniaNexus5010	NX-OS 4.1(3)N2(1)
Fortinet FortiGate Firewall FGVM64	Test	FortiOS 6.4.2
Palo Alto Firewall	PA-200	PANOS 7.0.0
Palo Alto Virtual System	PA-200-vsys1	PANOS

Auditing a network device

Here we will be auditing a device with Nipper that we are connecting to using Nipper, this will mean that you won't have to retrieve the configuration yourself as Nipper will do this. Example shown below:

Command:

```
nipper --remote-device=192.168.0.0 --ios-router --protocol=ssh --port=22 --user-
name=admin --password=password --output="C:\audit.html"
```

To start these, you will need to specify the IP/Model/Protocol/Port/Username/Password. The user will need read access, for some other devices they may need some extra permissions. Then afterwards you can specify what reports you want, or if you have already specified these prior, you only need to add the output which can be any directory you have write access too, you will need to specify the file extension, we would recommend .html if you are looking to review the reports.

Auditing network devices via CSV

Here we will need to specify the remote device(s) you are auditing, and then before you output the report, you need to make a csv file by using this command:

```
--network-device-csv="C:\network_device.csv
```

Full example shown below:

Command:

```
 nipper --remote-device=192.168.0.0 --ios-router --protocol=ssh --port=22 --user-
name=admin --password=password --network-device-csv="C:\network_device.xml" --out-
put="C:\audit.html"
```

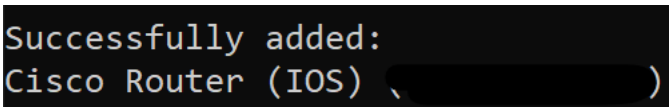
After doing the above you will be able to use whenever you got audit those device(s), using this command as your input, which was create in the last step.

```
--input=network_device.xml
```

Full example:

```
nipper --input=" network_device.csv" --output="audit2.html"
```

Nipper will also show you, what device it has been able to connect to:



We hope that you have found this guide useful and now feel confident in using the CLI.

If you would like to know more about how to get the most out of your software or have any questions then please feel free to contact our support team on: Telephone Number: (+44)1905 888 785 E-mail: support@titania.com