Nipper – Beginner's Guide

Multiple Award Winning Security Software

Titania Nipper Version 2.6.2
Published November 2019

Titania Limited
Security House
Barbourne Road
Worcester
WR1 1RS

Telephone: (+44)1905 888 785
Technical Support: Support@titania.com
Licensing: Enquiries@titania.com
Nipper Support: https://www.titania.com/support/nipper-support/

TITANIA
Assured Accuracy

Contents

What is Titania Nipper?

Nipper from Titania is an auditing tool which quickly identifies undiscovered vulnerabilities in firewalls, switches and routers, automatically prioritizing risks to your organization.

The reports are written in plain English and can be exported in machine-readable formats. Where relevant, the reports explain security vulnerabilities that are found along with ratings for how potentially dangerous they are.

The following reports are currently available:

Security Audit
Perform a “best practice” security audit that combines checks from many difference sources including penetration testing experience.

Vulnerability Audit
Compares the device’s operating system version against the NIST NVD database for known software vulnerabilities, which includes links to manufacturers and third-parties.

CIS Benchmarks
A CIS benchmark audit for Cisco IOS 12, IOS 15 and Cisco ASA.

STIG Compliance
A DISA STIG compliance audit against specific STIG checklists.

PCI DSS Audit
A combination of our “Best Practice” Security Audit, Vulnerability audit, Configuration report, and CIS benchmarks to meet the current PCI requirements.

Filtering Complexity
Examines the network filtering rules and objects highlighting unused objects, overlapping and contradictory rules. Making sure your packet filtering is secure.

Configuration Report
A precisely detailed report on how your device has been configured.

Raw Configuration
Imports the actual full configuration of your network device into the audit.

Raw Change Tracking
Highlights any changes detected between the device’s current raw configuration and a previously-saved raw configuration report.

Filtering Differences

Analyses Security Audit and raw differences between the current configuration and a previously saved baseline file.

Nipper is typically installed and run from a workstation and most customers choose to manually retrieve their device configuration files, but there is support for network-based collection of configuration files for some of our most popular supported devices.

Once collated, the configuration files are audited by the software (usually very quickly) and one or more reports are generated according to user's choices.

Nipper is not a scanner and does not create network traffic by default. It is a configuration analyser which will significantly aid you in auditing infrastructure security, or as part of a penetration test.

What is the Nipper Beginner's Guide?

The **purpose** of this document is to provide a beginner's guide to Titania Nipper. The intended audience is therefore either anyone new to the Nipper software or anyone who needs a refresher on the features. It may also be useful as a reference for users; however, the **scope** is limited by design to those who are less familiar with the software. There are many options in the software and it is not practical to include them all in this Guide.

This Guide will therefore explain how to install, run and activate Titania Nipper, and take you through some of its most common/popular features.

This Beginner's Guide is based on the original Nipper Manual, which is made obsolete on the publication of this Guide.

It is based on **Nipper Release 2.6.1**

Should you have any further technical support questions about the software, please contact us: support@titania.com

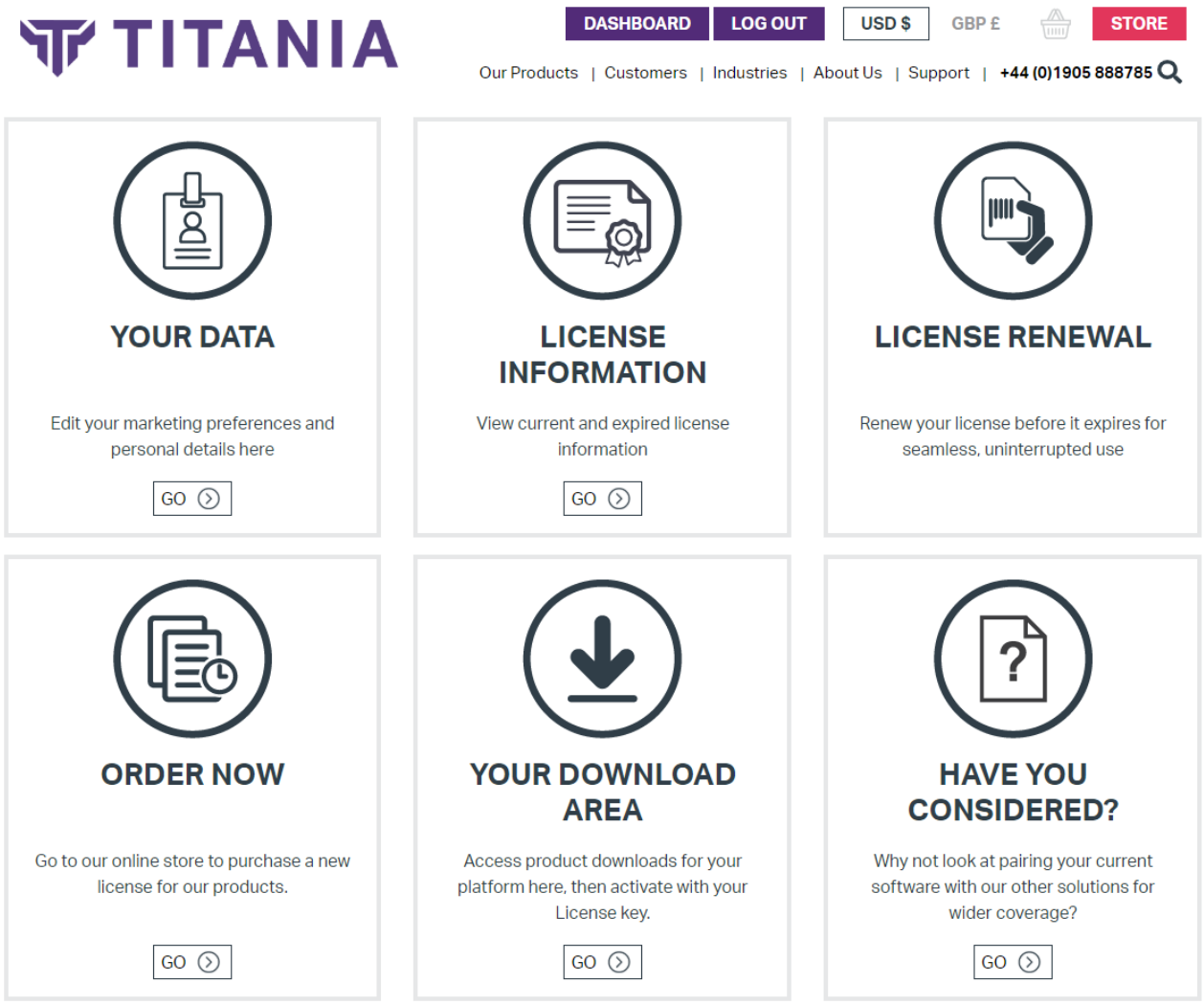
Prepared November 2019 by the Titania Technical Services Team

Installing Nipper

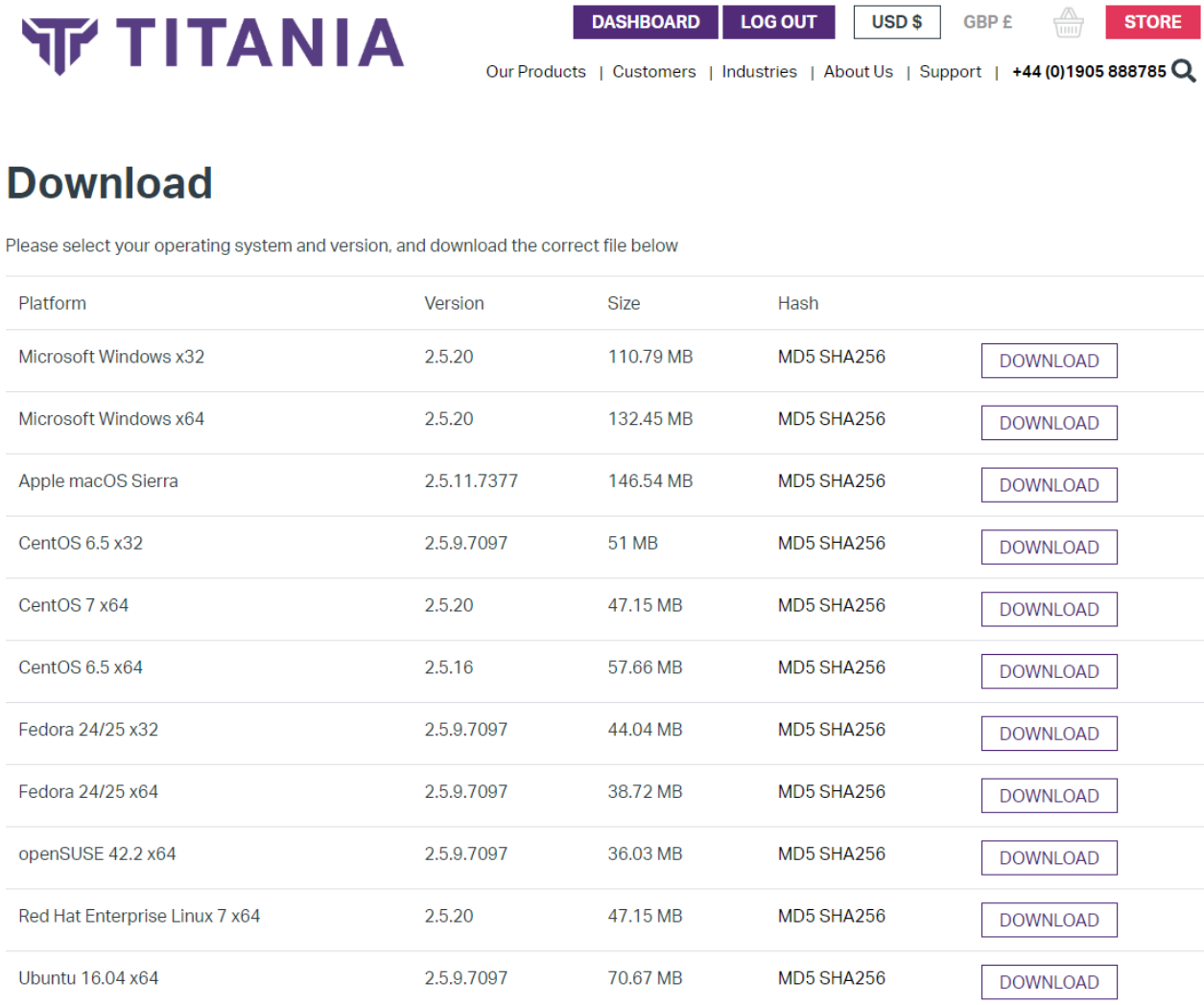
Nipper can be downloaded on a number of platforms including Windows, Mac and various Linux distributions.

Once you are a registered user of our website (https://www.titania.com), you can download Nipper by logging in to view your dashboard.

On this screen, you will be able to initiate the download process by navigating to Your Download Area, clicking Go then clicking on View Downloads for the relevant product.



From the Download page you can choose your operating system and architecture for the download you require (Windows, MAC, Linux).



Installing Nipper - general information

Nipper is installed and run from a local machine. That is, Nipper cannot be installed on a server and accessed remotely.

The software has been tested on server operating systems, but if installed as such you would still be required to operate the software locally, working at the same machine on which Nipper is installed.

The following chapter gives detailed instructions with screenshots on how to install Nipper on Windows operating systems. There are then two briefer chapters explaining how to install on Linux and Mac.

Please note that on some Linux operating systems, further commands and installation of dependencies may be required. This applies to Security Enhanced Linux and CentOS / Red Hat distributions. Please see the Linux installation chapter and/or the website for details.

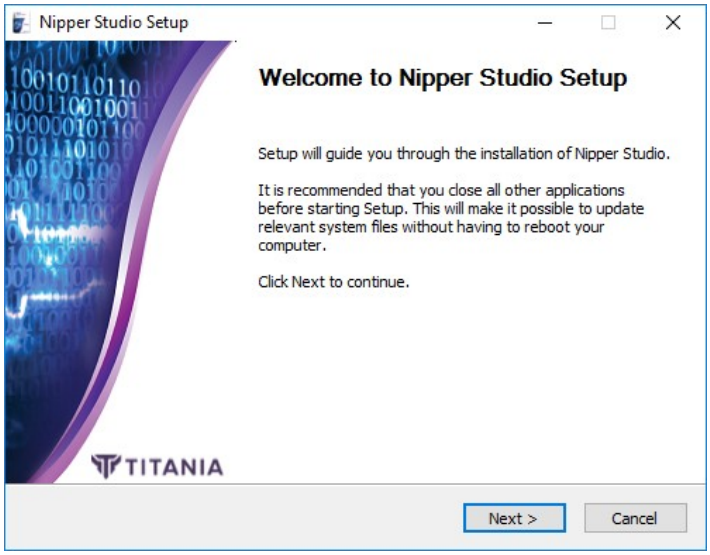
Nipper downloads come supplied with both SHA1 and MD5 hashes on the website, allowing you to check the integrity of the download.

The packages are code signed wherever possible and are both built in a clean, secure environment undergoing rigorous testing before upload to our servers.

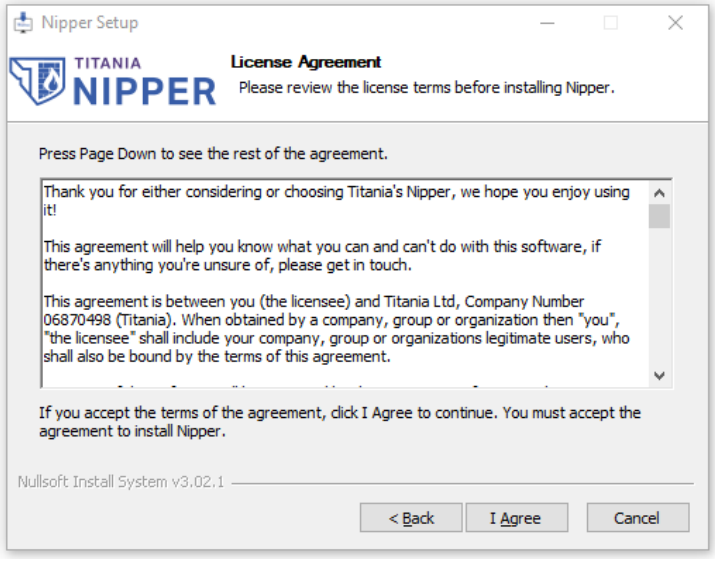
Installing Nipper on Windows Operating Systems

NB: We installed Nipper on Windows 10 x64 for this explanation. Naturally, Nipper is also supported on other Windows versions.

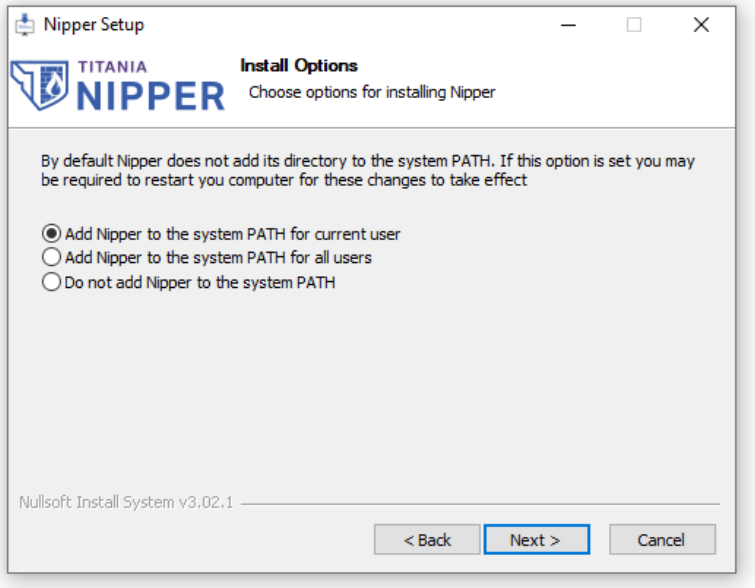
To install Titania Nipper, double-click on the Nipper download file and the Welcome Wizard box will appear. Click '**Next**' to continue.



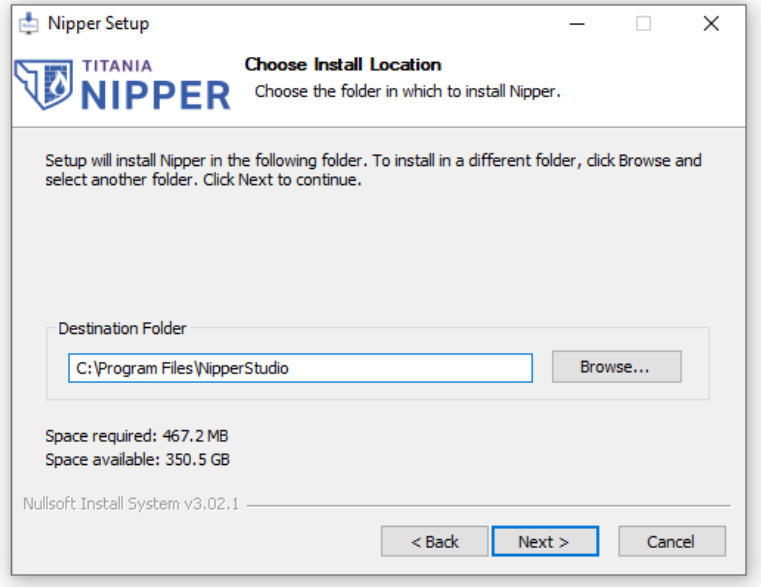
Read and agree to the license and click **'I Agree'** to continue.



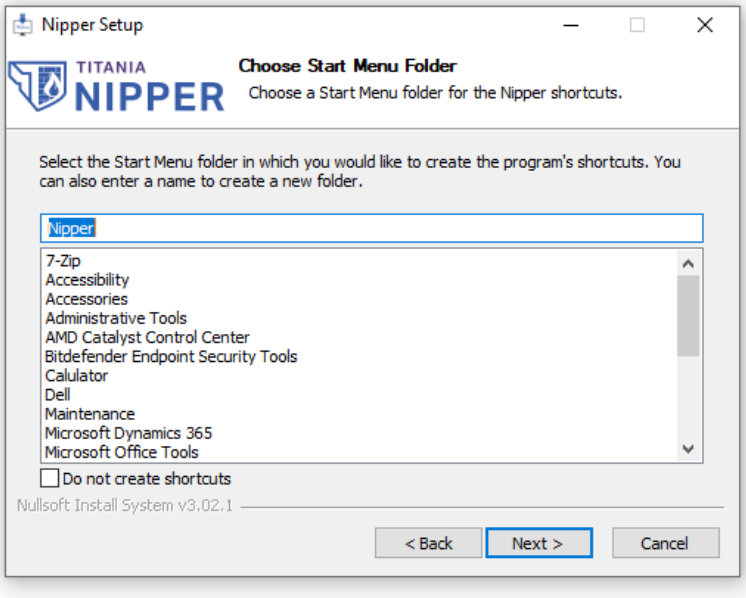
You will then see the Install Options screen. Here you can choose whether Nipper is installed to the system path for the current user, all users, or not on the system path at all. Click '**Next**' when ready.



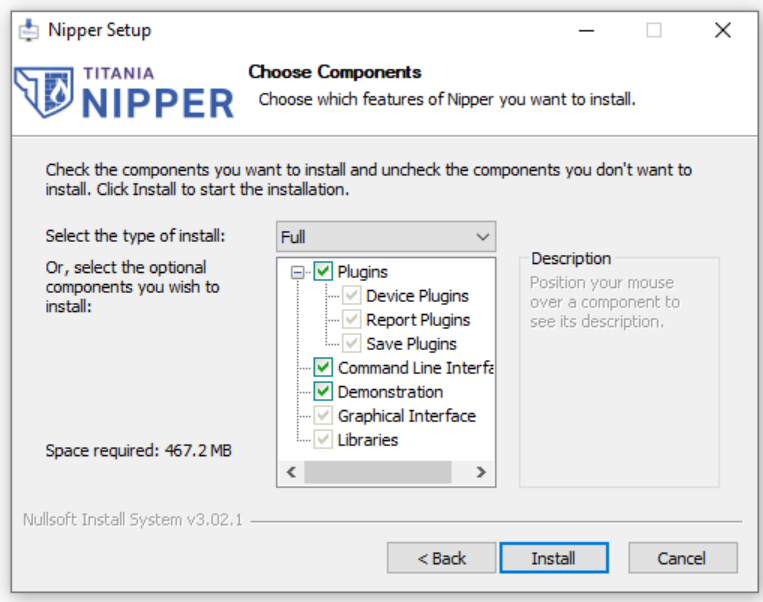
In the next window, choose where to install Titania Nipper. You can browse to a different location if you wish, or if you are happy with the default location, click '**Next'**.



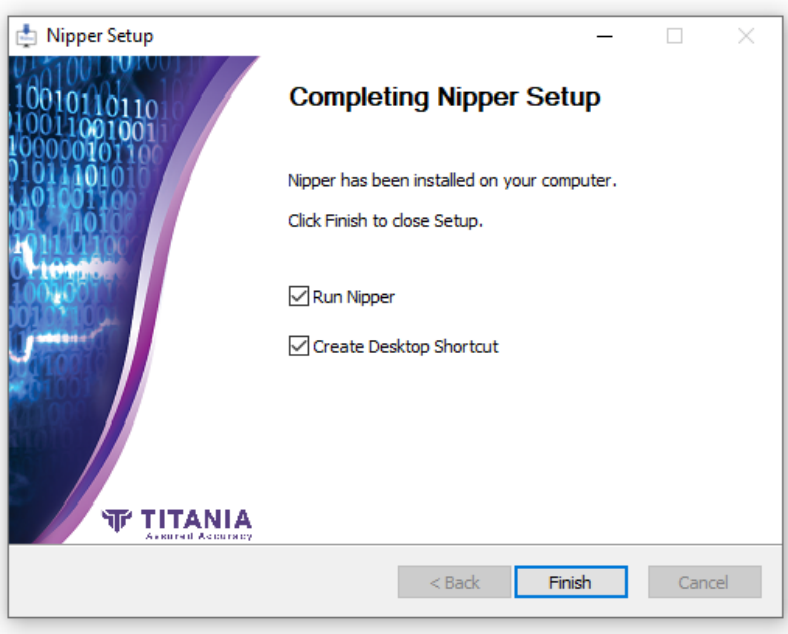
Next, you can choose the Start Menu folder where you want to install the shortcuts. Once you have done so, click '**Next'** to continue.



The next stage is to choose the components you want to install with Titania Nipper.



When you have selected your components and pressed **'Install'**, the software will install to your specifications and you will be taken to the final Nipper installation screen. To complete, select '**Finish'**.



Installing Nipper on Linux Operating Systems

On Linux operating systems, the preferred method is to install via the GUI and allow the package manager to deal with the installation.

SE Linux

If you are using Security Enhanced Linux and Nipper fails to start, you will need to execute the following commands as the root user:

```
chcon -t texrel_shlib_t /usr/lib/libnipper2.*
chcon -t texrel_shlib_t /usr/lib64/libnipper2.*
for x in `ls /opt/nipper/plugins/`; do chcon -t texrel_shlib_t /opt/nipper/plugins/$x; done
```

Nipper requires version 5 of the Qt framework to run. Qt5 is not available in the default RHEL/CentOS repositories, but it is available in EPEL (Extra Package libraries for Enterprise Linux) repository, which is available free and simple to install.

Installing the EPEL repository is a two-stage process, first you will need to download the rpm package containing the repository files for your distribution, and then you will need to install the package using the rpm command line tool.

You can copy and run the commands for your Linux distribution before attempting to install Titania Nipper, and the Qt5 dependencies should be resolved for you.

CentOS 6 (x32)

wget http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

rpm -iv epel-release-6-8.noarch.rpm

CentOS 6 (x64)

wget http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

rpm -iv epel-release-6-8.noarch.rpm

CentOS 7 (x64)

In order to install Nipper onto your machine, run the following commands:

yum -y install epel-release
yum -y update
yum -y install nipper-[rpm name].rpm (eg. nipper-2.6.1.2019-10-07-centos-7-x86_64.rpm)

If you still encounter issues installing Nipper on CentOS 7, use the following commands to update the yum repository and enable the community repository.

sed -i 's/enabled=0/enabled=1/g' /etc/yum.repos.d/CentOS-CR.repo
yum -y update
yum -y install nipper-[rpm name].rpm (eg. nipper-2.6.1.2019-10-07-centos-7-x86_64.rpm

Ubuntu

With Ubuntu usually the dependencies are already met but if your Ubuntu machine doesn’t install Nipper try to retrieve the QT5 dependencies:

sudo apt-get install build-essential

sudo apt-get install libx11-xcb-dev libglu1-mesa-dev

Fedora 32bit/64bit

When installing Nipper via the command dnf it should automatically detect the required dependencies

Once you have installed the file, you will be able to install Titania Nipper, to do this download the most recent Nipper version for OpenSuse, and simply click the file and it will install.

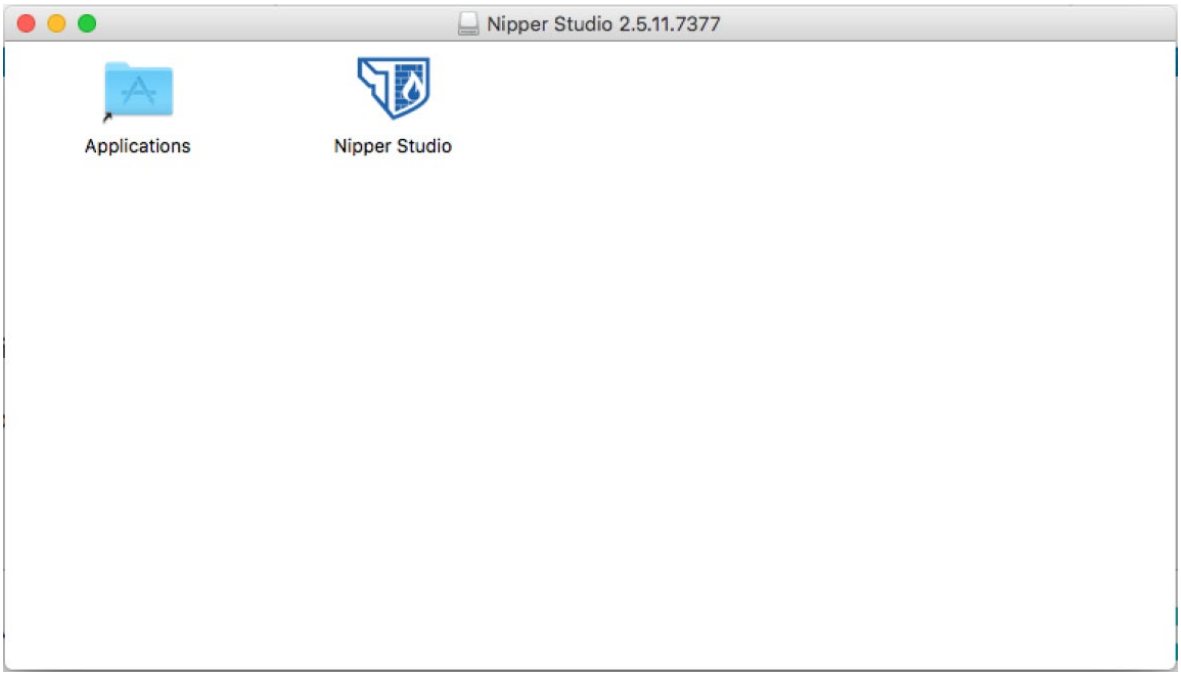
To install nipper through the CLI go to the directory that the file is held in and

type sudo zypper install nipper-* Nipper will then install.

Installing Nipper on Mac Operating Systems

Before installing Nipper on to your Mac device, you must first remove any previous versions of Nipper from the device. Using the terminal of the Mac with these commands-

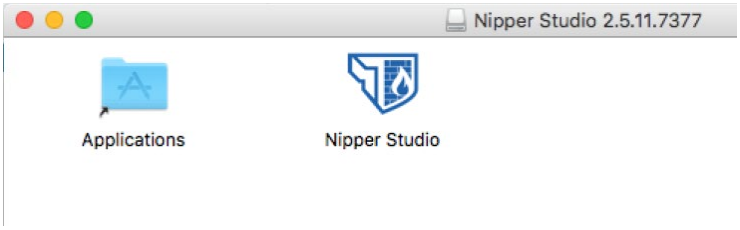
```
sudo rm -rf /usr/bin/nipper*

sudo rm -rf /usr/lib/libnipper*

sudo rm -rf /Library/Frameworks/Qt*

sudo rm -rf /Library/Frameworks/libnipper*

sudo rm -rf /Applications/Nipper\Studio.app/

sudo rm –rf ~/Library/Preferences/com.titania.*
```



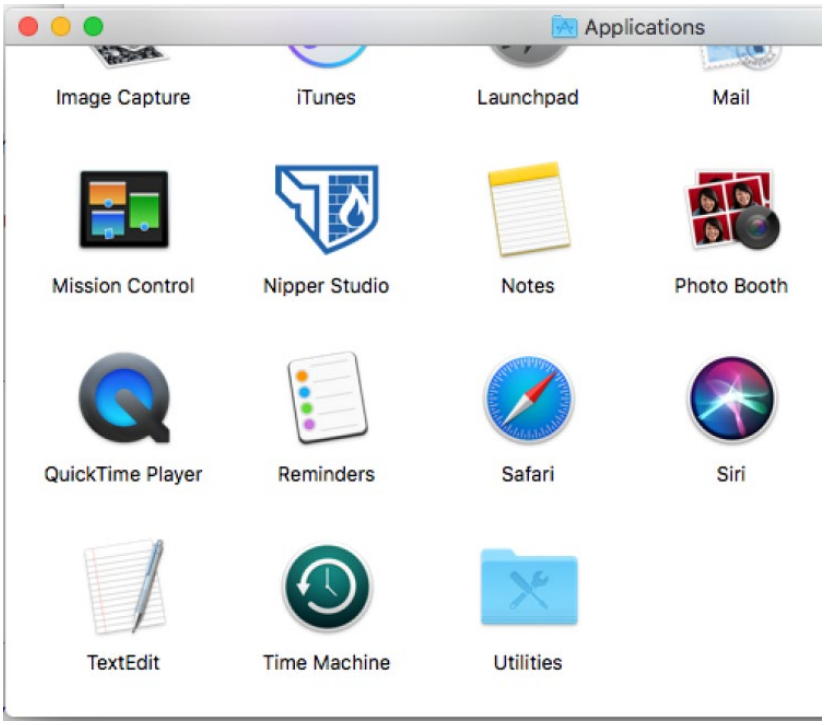
To install Nipper go to the Titania website and download the latest Nipper program: https://www.titania.com/

Now simply double click the Nipper file, which will begin the install process. The Mac will verify the download.

You will now be shown a window with the Nipper logo and the Applications folder within it, simply drag the Nipper icon into the application folder and this will install Nipper on to the Mac.



Following this, open the applications folder and launch Titania Nipper.

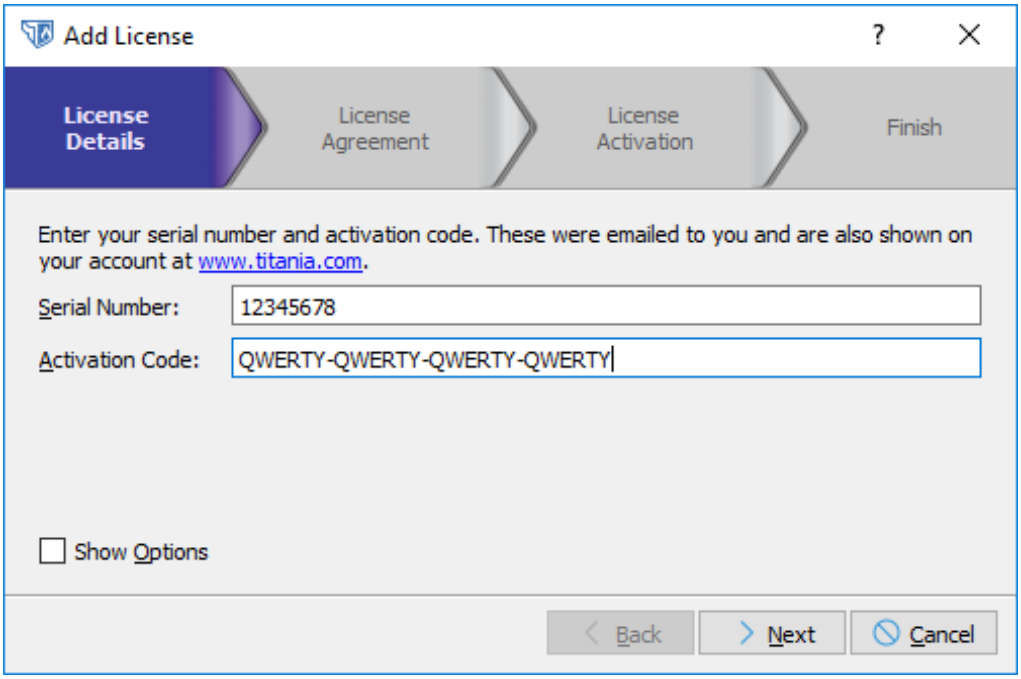


Adding a license to Nipper

The first time you run Nipper you will need to add your license. When the add license wizard appears click '**Add License**.'

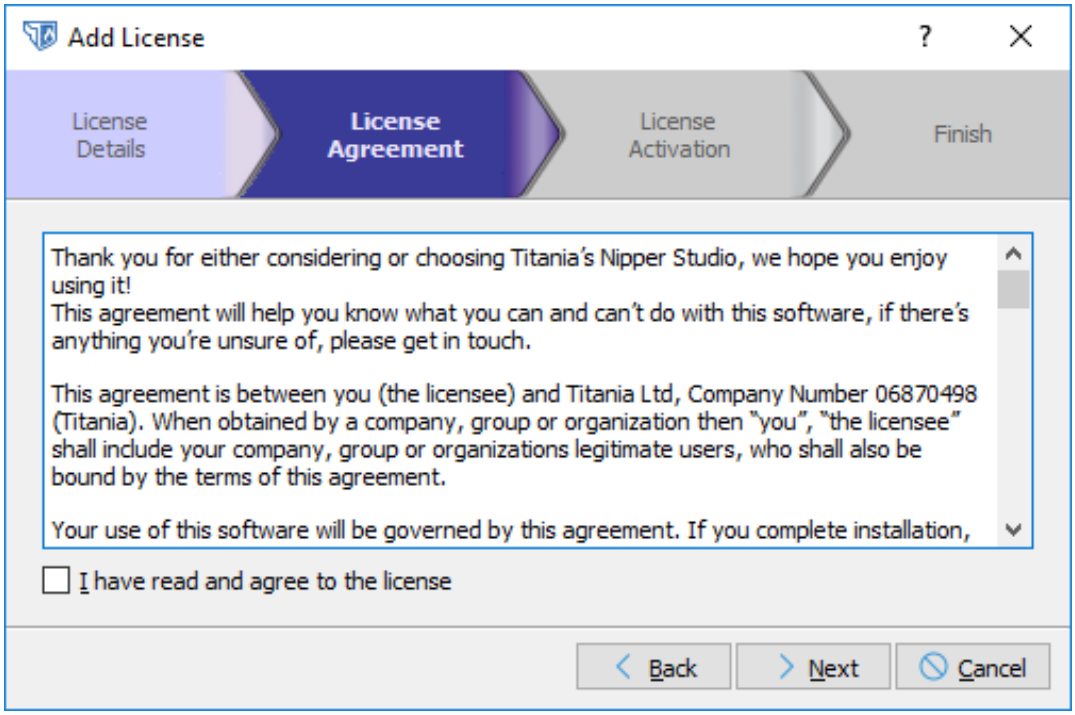
After you click '**Add License'**, you will be asked for your Serial Number and Activation Code. This information will have been emailed to you when you purchased the license. It can also be accessed through the Titania website, www.titania.com by logging into your account and then going to '**Your account'**. Both the **'Login'** and the **'Your Account'** buttons are on the upper right-hand side of the page.

The **'Show Options'** tick-box allows you to activate the license in multiple ways including online, offline or challenge & response modes.



Enter the Serial Number an Activation Code details into the relevant boxes, as above, and click **'Next'**.

You will then be asked to agree to our license, as below:

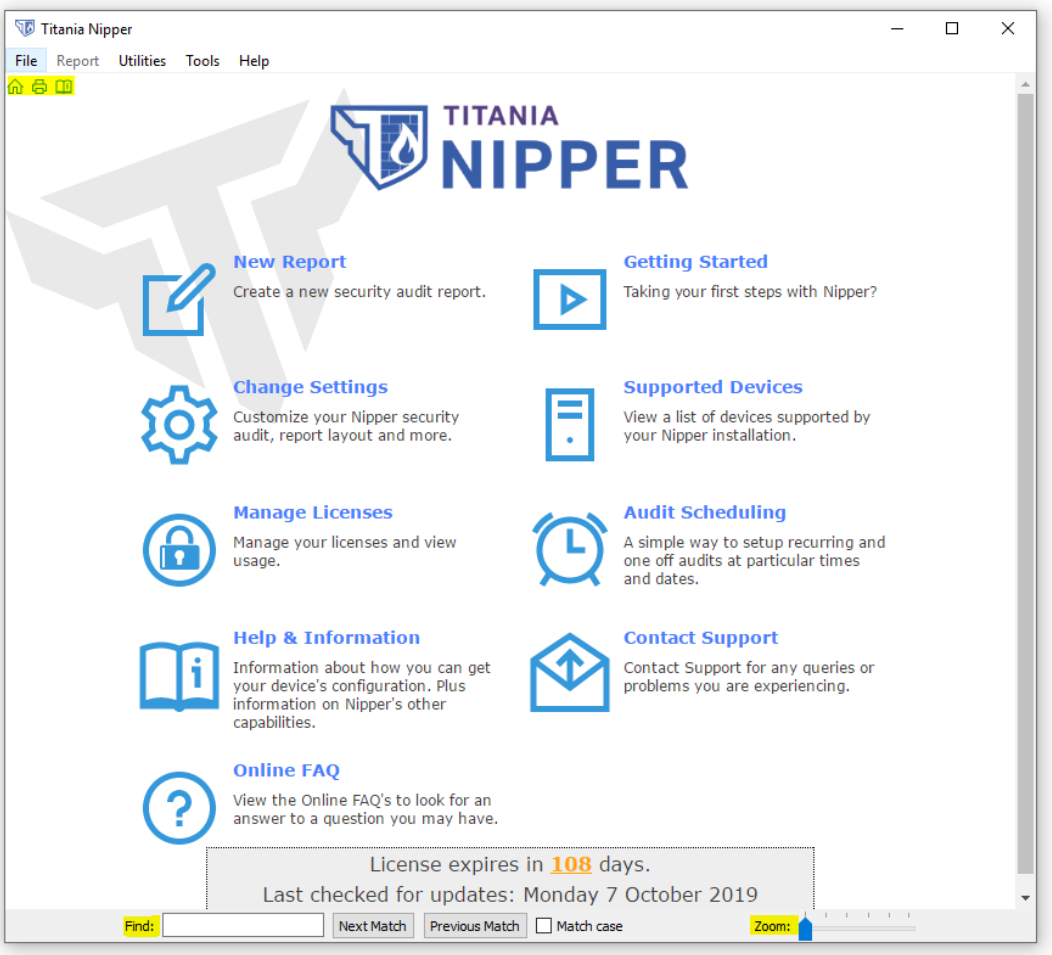


After a brief License Activation screen, the license will be added into the software. Click '**Finish**'.

Nipper is now fully installed and licensed on your machine, and you are ready to begin.

Navigating around Nipper

This is the Nipper homepage:



We have highlighted navigation icons on the top left of the page and the search toolbar at the bottom of the page.

Also, when moving around Titania Nipper, for example when you have a report open, you can right click on the Nipper window to bring up **a 'Go Back'** icon which will take you back a screen.

Obtaining device configuration files

In order to perform an audit of your devices, Nipper needs to access the native configuration file of the relevant devices.

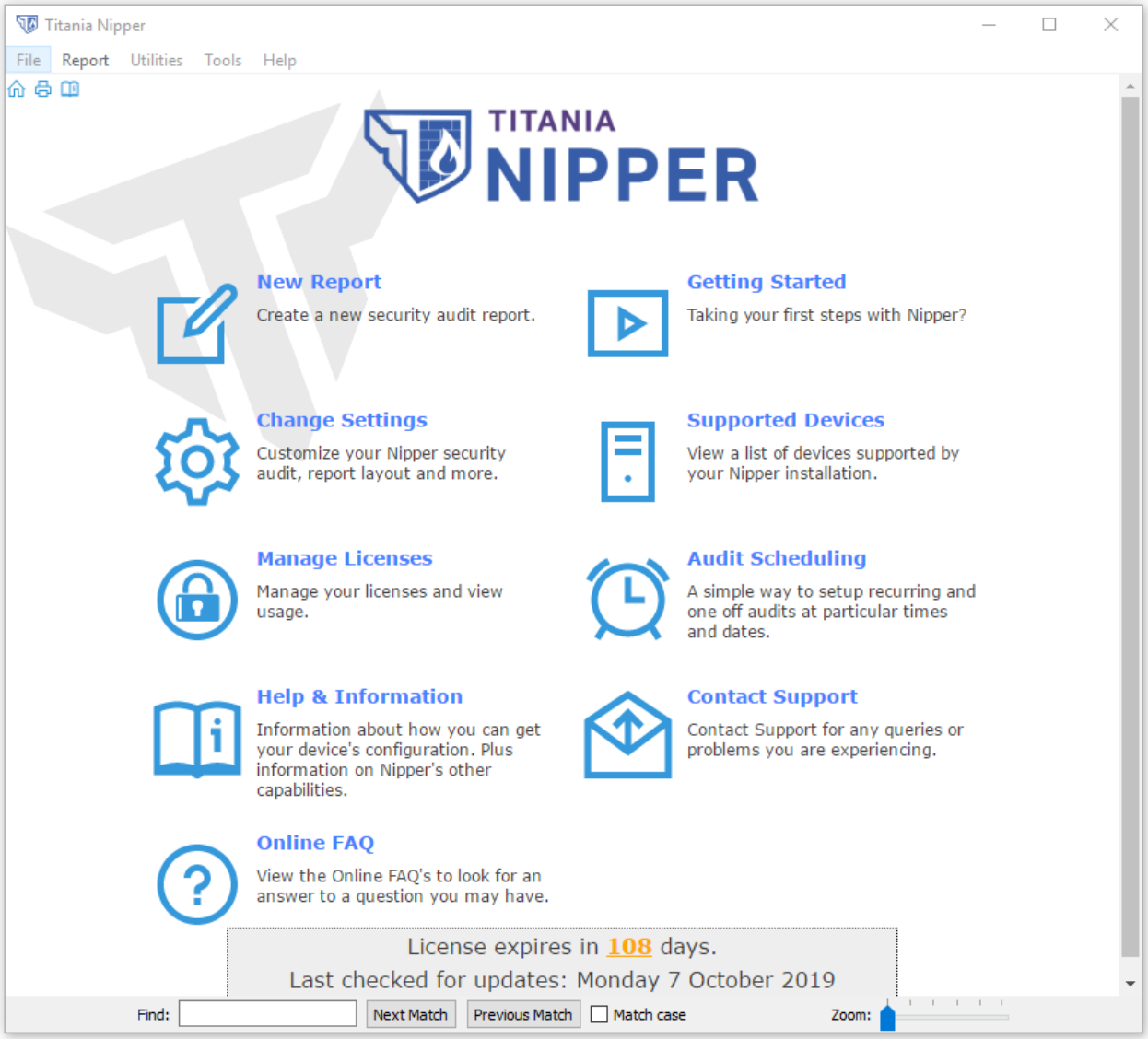
There are presently two ways to achieve this:

- You can manually extract the configuration files you need.
- For some devices you can access the configuration file over the network.

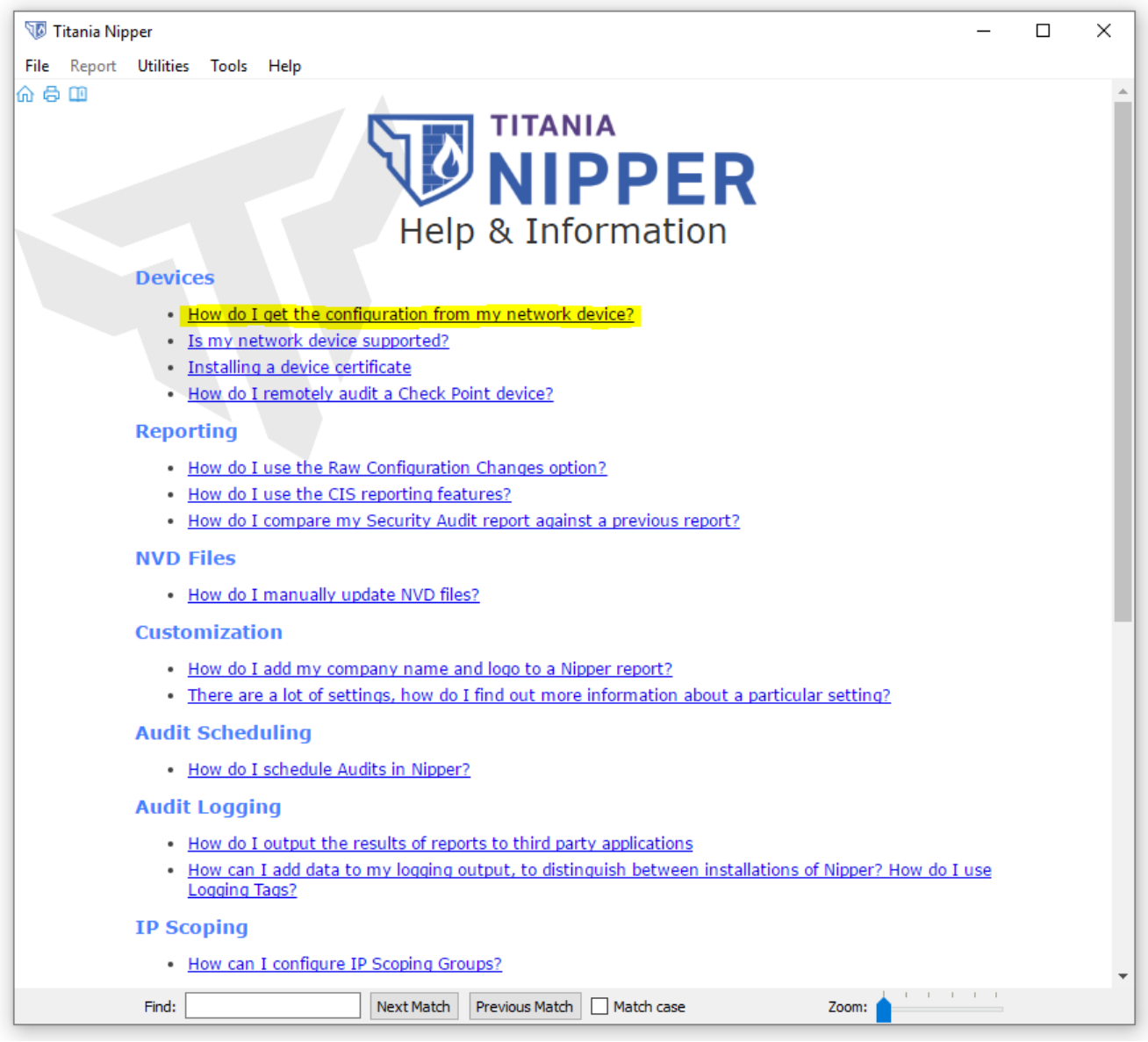
Many of our customers still prefer to manually extract the configuration file from the device, because it is arguably more secure and does not increase network traffic. For others, the convenience of network access is a bonus.

In the next section we will briefly demonstrate both methods. Here, we explain how you can find instructions on how to manually retrieve your configuration files.

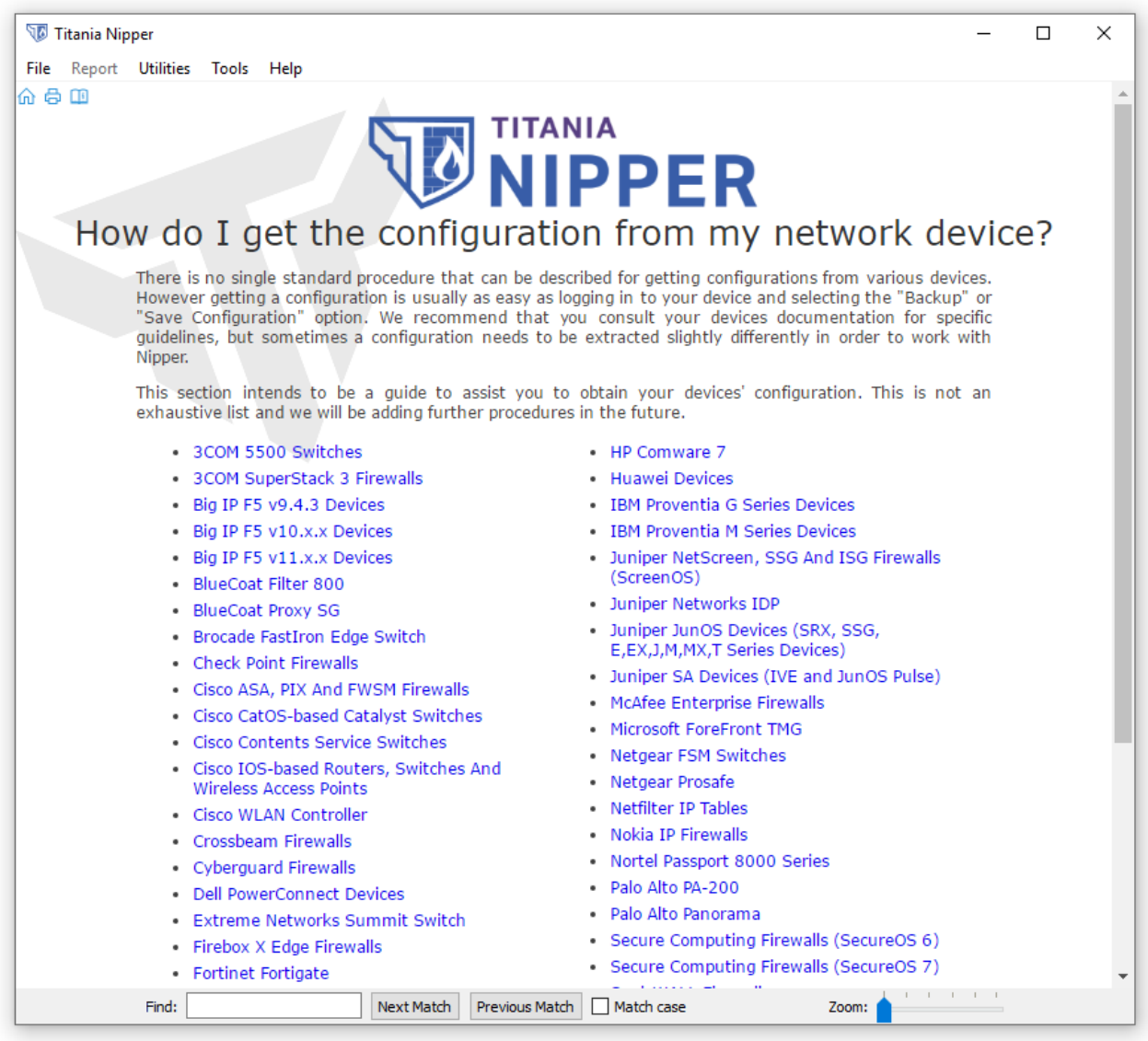
First open Titania Nipper, whereupon you will be presented with the homepage:



Click on '**Help & Information**', which will present you with the following screen:



Click on **'How do I get the configuration file from my network device?'** to bring up the following screen:



If you are an auditor preparing to visit a client site, it may be useful for you to advise your client how to retrieve the configuration themselves. The Titania website has copies of these instructions on the Nipper support page, which can be accessed by anyone (no user account required) at https://www.titania.com/products/nipper/user-guides/

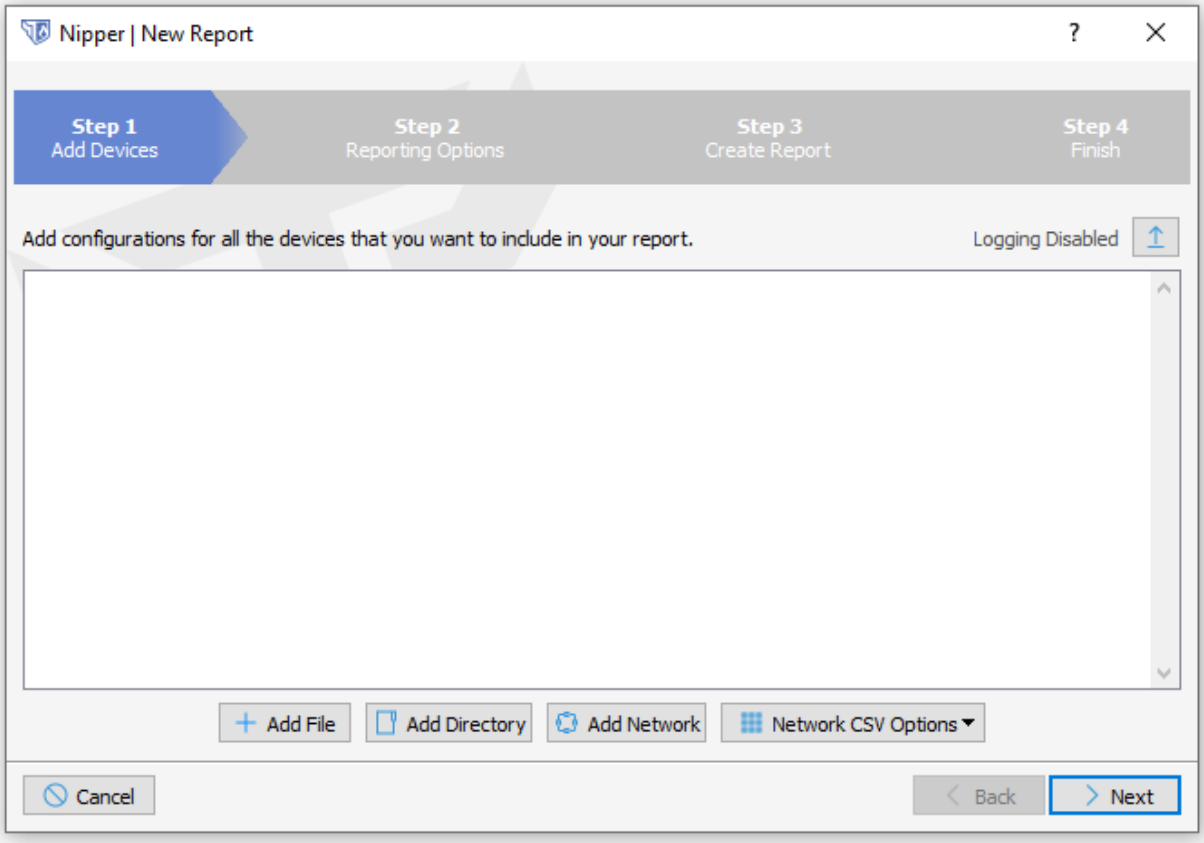
If you are unable to find the instructions to retrieve the configuration from a supported device either in the Nipper software or on our website, please inform support@titania.com . In the meantime, you should be able to find the relevant details in the device's documentation

Creating your first report with Nipper

Adding the configuration files

Here we will add files to Nipper and demonstrate how to create a report using remote files.

From the Nipper home page, select **'New Report'** (or File, New Report). You are presented with the following screen:



You can see the following four options:

'Add File' looks for a single, manually exported device configuration file.

'Add Directory' looks for a directory containing one or more manually exported device configuration files.

'Add Network' will allow you to add the configuration files of supported devices remotely.

Under **'Network CSV Options'** there are two options:

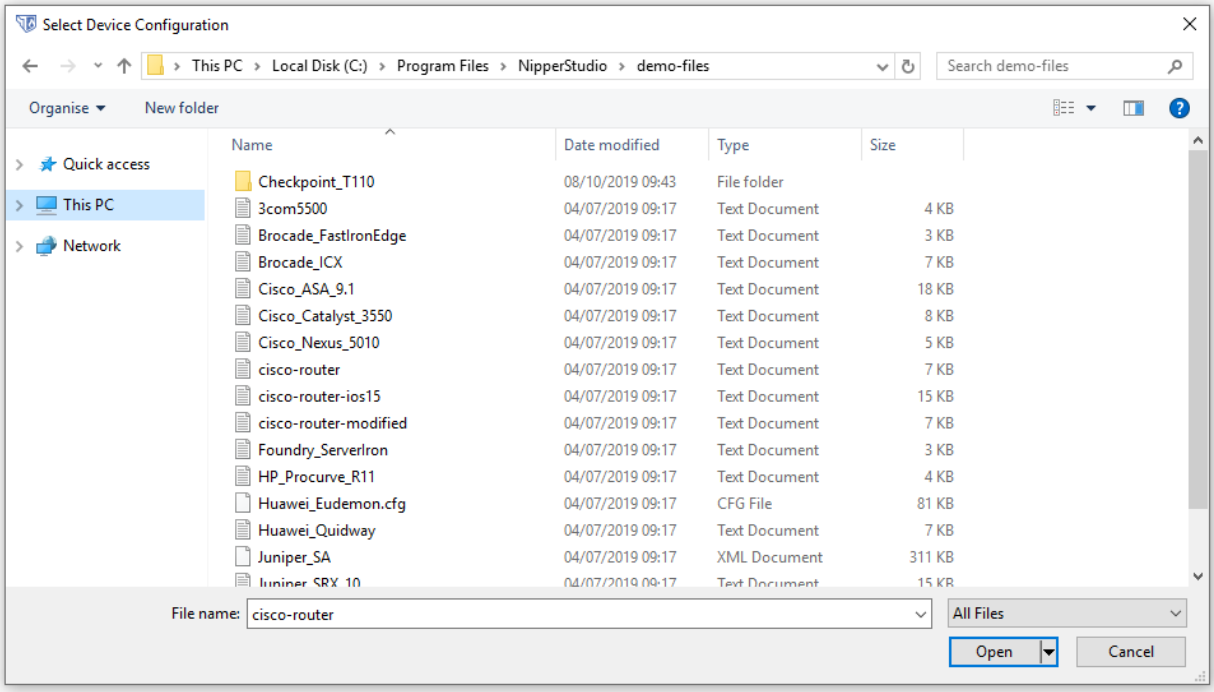
'Import Network CSV' will enable you to add multiple devices via a CSV input.

'Export Network Devices as CSV' generates a CSV from the networks that are available in the format that can be re-imported using 'Import Network CSV'.

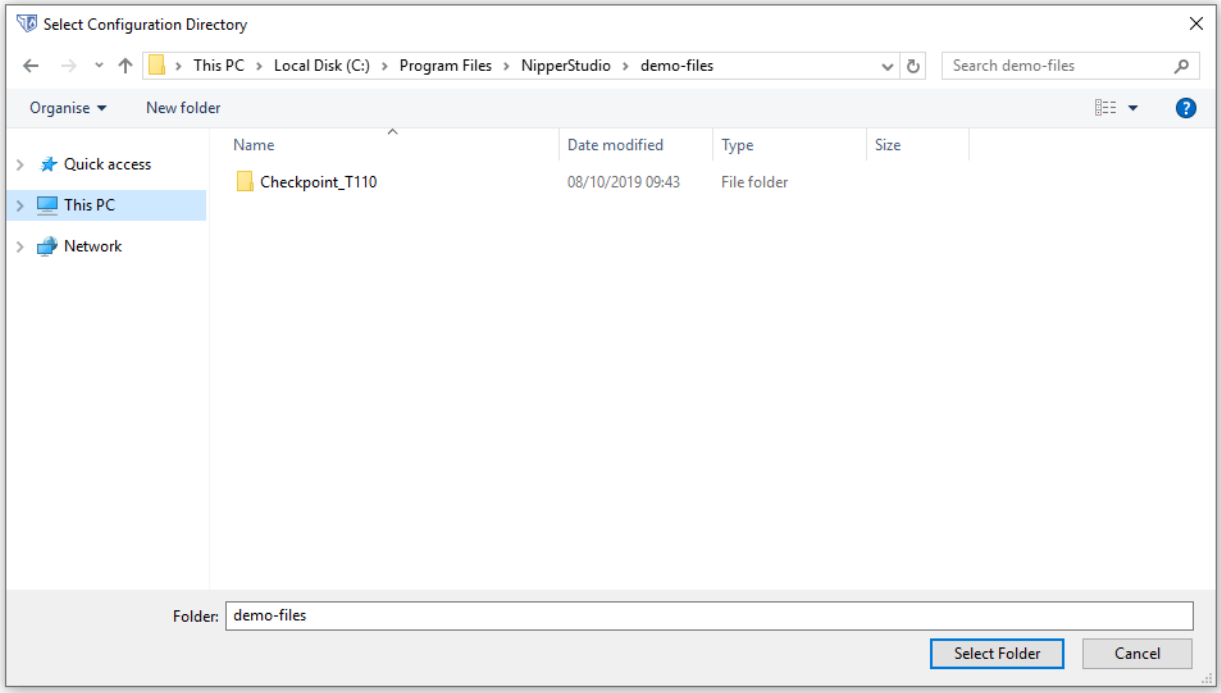
In this Guide, we will use the demonstration files supplied with Titania Nipper. If you are adding your own files, you will need to navigate to wherever you have stored the files.

If you select **'Add File'** on a new Nipper installation you should be able to see the 'Demo files' directory. On older installations it is likely that you will have navigated away from this default installation directory. On Windows you will find this under C:\Program Files[x86]\nipperstudio. On Linux systems it will be under /opt/nipper. On Macs it will also be under /opt/nipper.

The following screen-shot shows the screen after you have clicked on **'Add File'** and opened the demo-files directory. Note that Nipper is expecting a single device configuration.

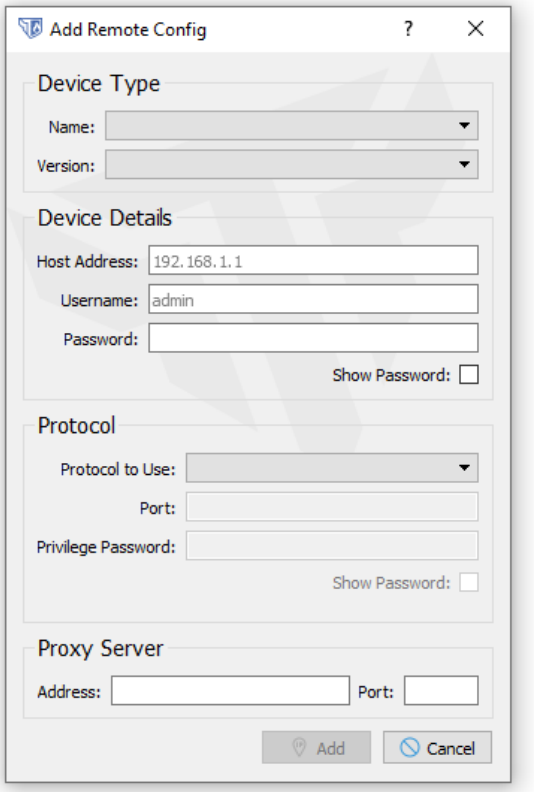


Nipper supports auditing multiple devices in a directory. The only limits to this are the capabilities of your machine, although auditing a very large directory of configurations might take a considerable amount of time, and 64 bit architectures are preferred for this type of operation. In the screen capture below, you see we have selected **'Add Directory'** and we are able to add the whole demo-files directory.



Adding files remotely to Nipper

Selecting **'Add Network'** presents you with the following screen:



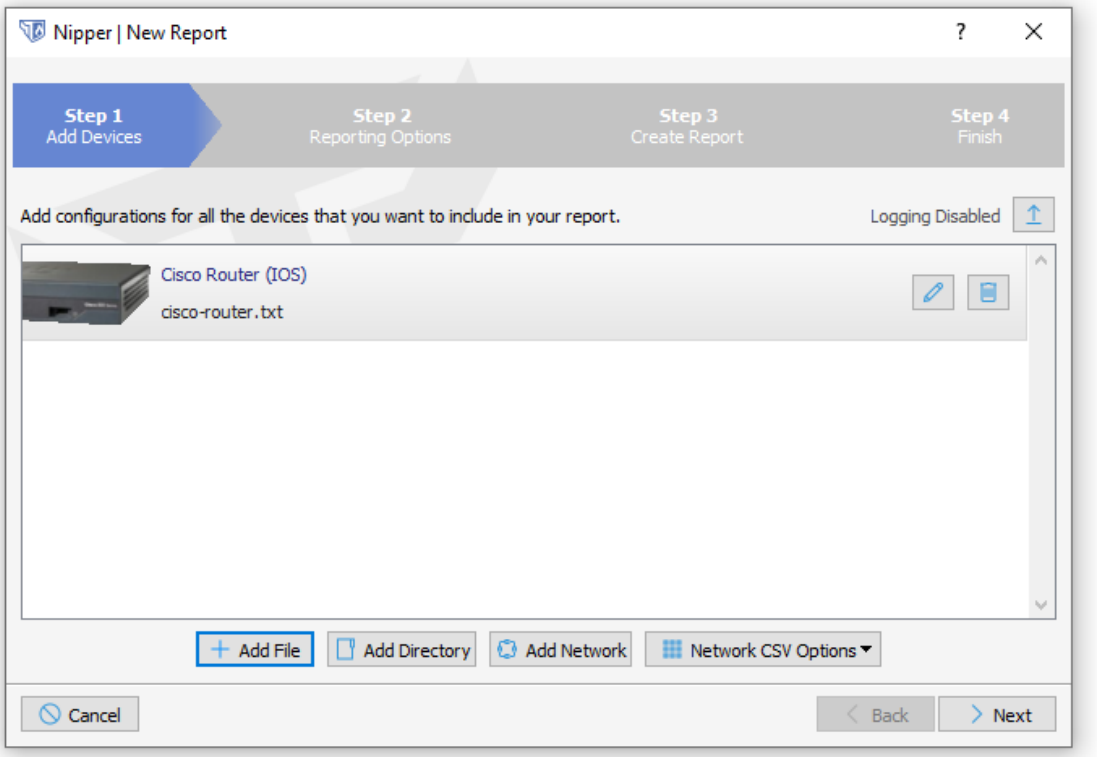
The Device Type section allows you to choose the type of device you want to audit. Only those devices supported by Nipper for remote configuration collection will be displayed here. The Version field can be left as 'default'; this is included for future functionality.

The Device Details section requires you to enter the basic information for your device. The Protocol section allows you to enter the protocol and port, along with the password required to elevate privilege in order to obtain access to the configuration file.

There is also a section to add Proxy Server details if required.

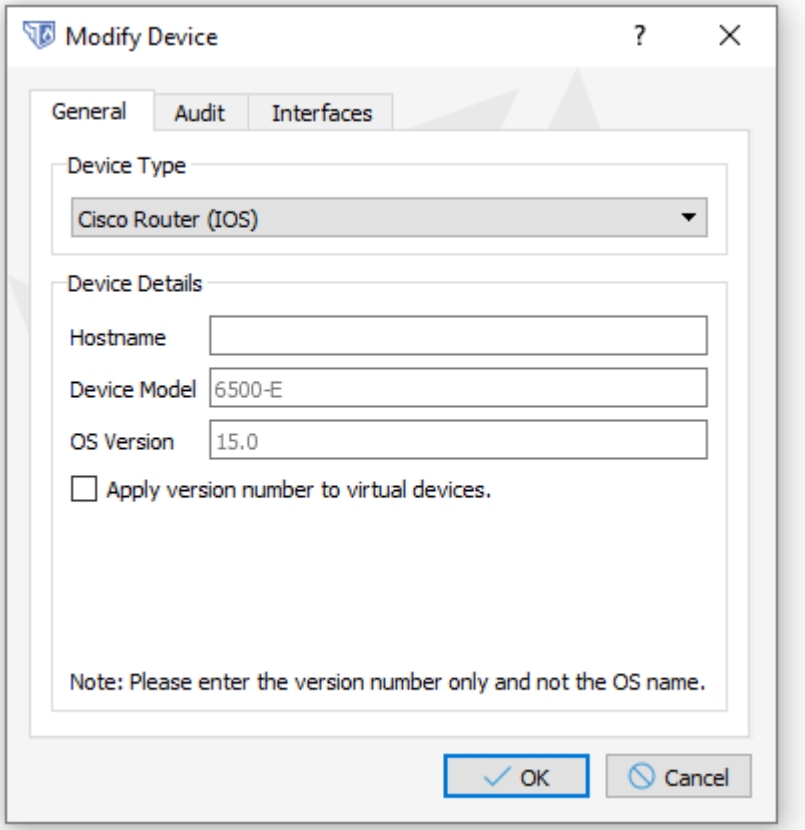
Report options

Once you have added your devices, you will now be presented with the next step in the New Report Wizard, which looks like this:



As you can see, the most recently added device is shown, along with the same options to add additional devices as previously discussed. You can add multiple devices if you wish to generate a multi device report.

Each device also has the tool icon and the remove device icon next to it. Naturally, the bin icon simply removes the device. Clicking on the pencil icon brings up the following menu:



You will see in this case (as is normal) Nipper has automatically detected the device type. The **'General'** tab allows you to add further details as per below.

Device Type: Used for manually setting the device type. Please note that, if this is altered from the device type identified by Nipper Studio from the config file, audit findings may not be 100% accurate.

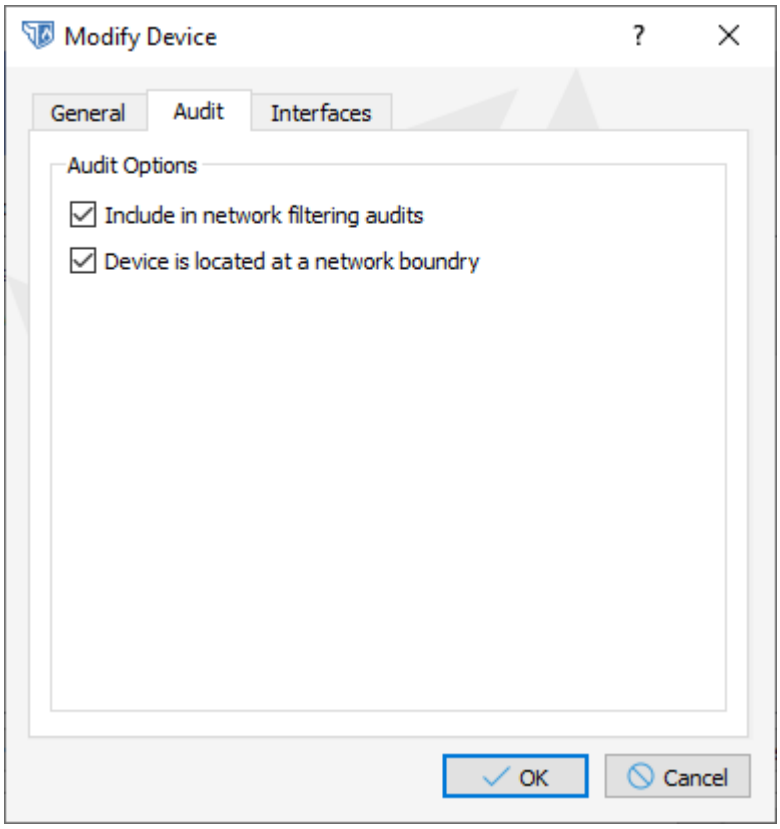
Hostname: Name of the network device

Device Model: Model of the network device

OS Version: Operating System version of the network device (to major/minor level only ie. 8.4 rather than 8.4.23)

Apply version number to virtual devices: Used to push manual amendments on this page onto virtual device for audits.

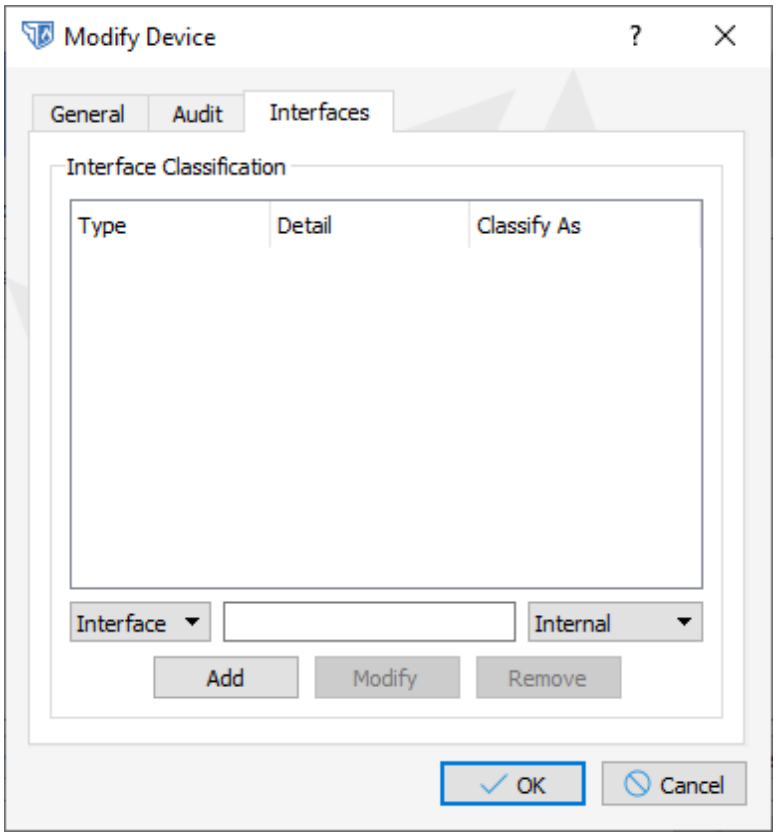
The **'Audit'** tab includes the following functionality:



Include in network filtering audits: Enabled by default. Unticking will remove filtering audit checks from the reports.

Device is located at a network boundary: Enabled by default. This is used in the IDS (Intrusion Detection Systems) check as a guard around the add Unicast RPF Issue.

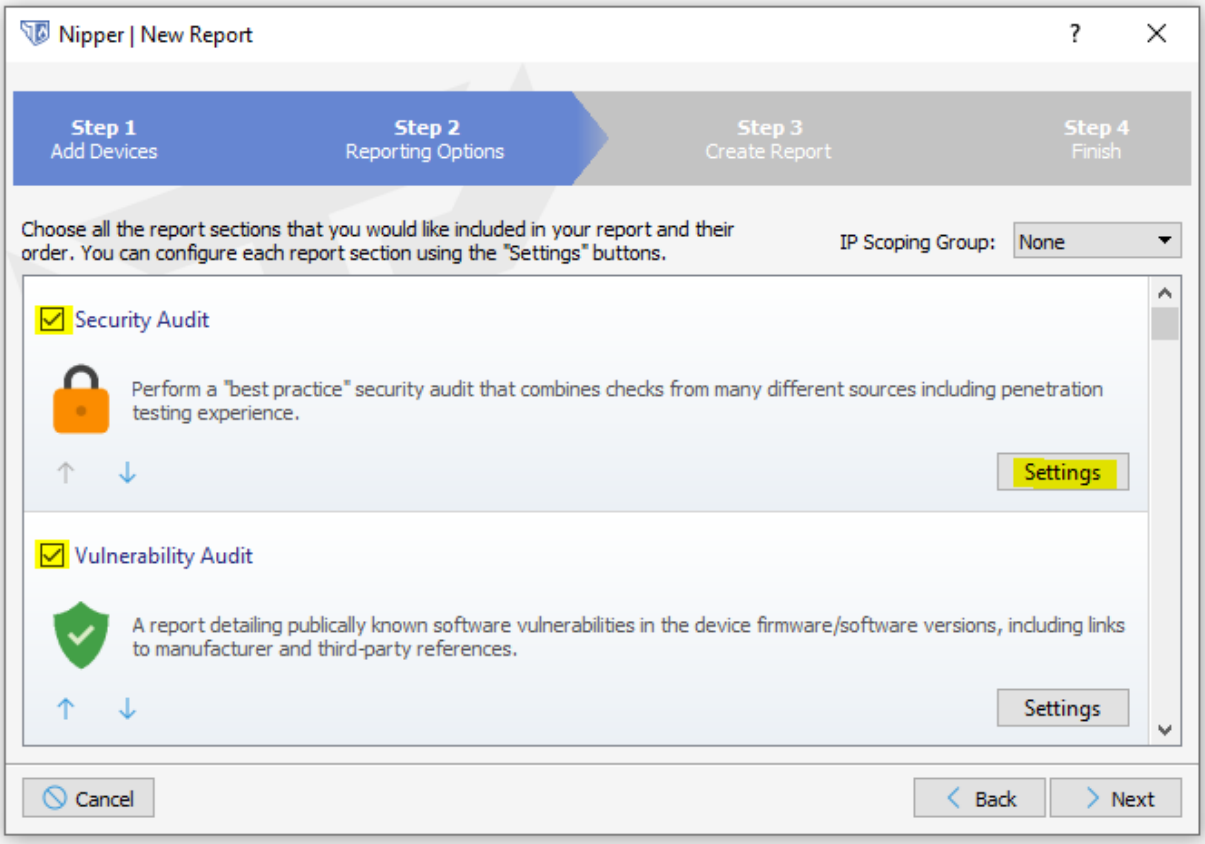
The **'Interfaces'** tab is mainly utilised for STIG audits:



Interface Classification: This is used in the STIG audit type to stop Nipper Studio prompting for manual interface information.

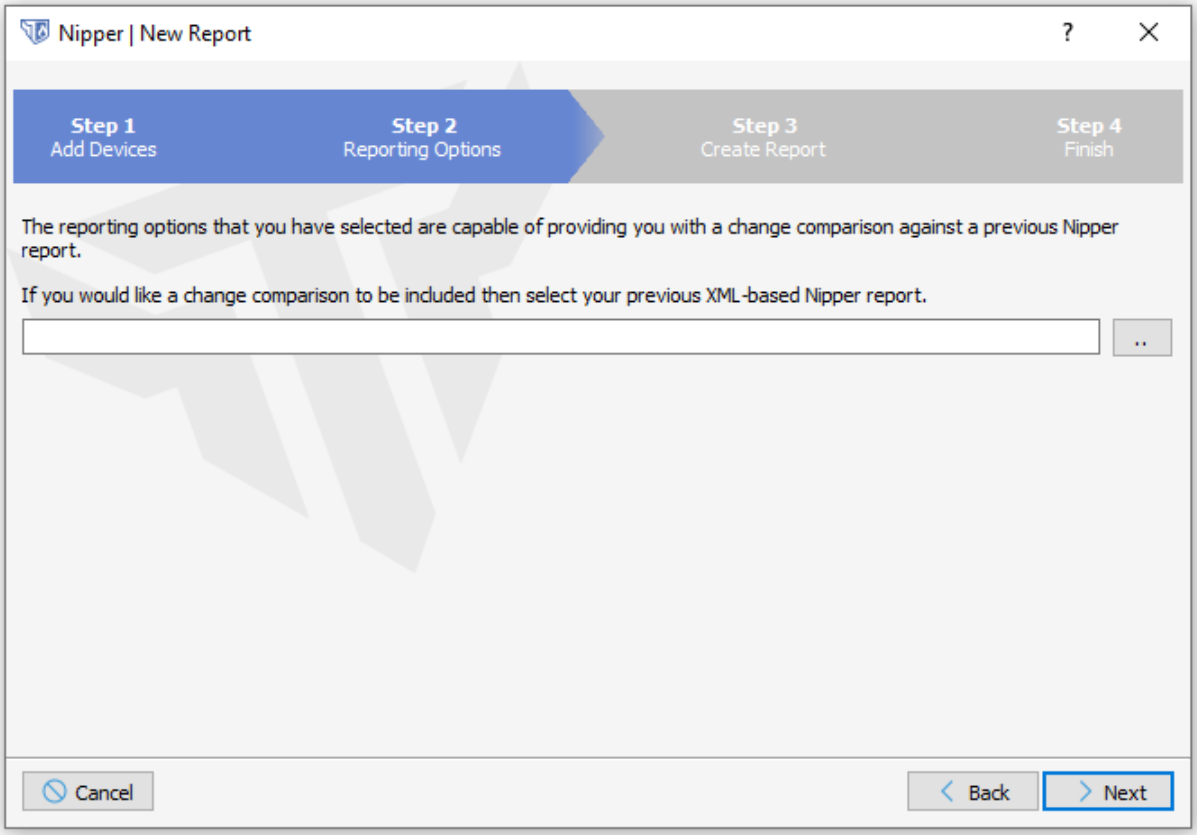
When you have finished making any changes you need here, click **'OK'** to return to the New Report Wizard.

Once you have added all the devices you wish to audit, and modified them if required, clicking **'Next'** in the New Report Wizard will take you to the Reporting Options menu:



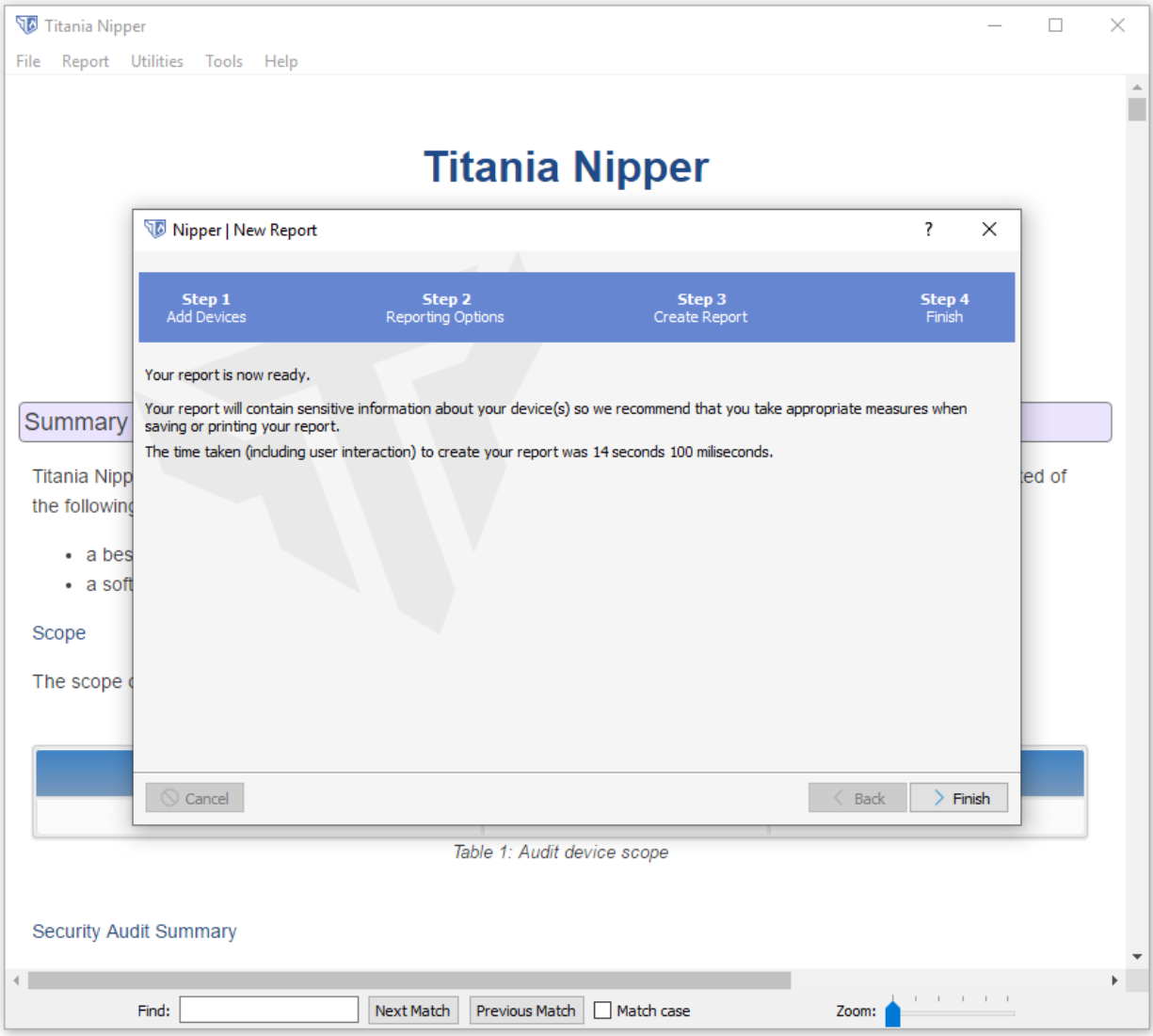
As you can see, the different report types are listed, with a brief description of what each report contains. Each report has a check box which determines whether it will be included in your final report, an up/down arrow allows you to determine the report sections position in the larger report and there is also a **'Settings'** button for selecting advanced options.

Once you have chosen your reporting options, click **'Next'** to proceed. The next screen may allow you to run a comparison against a previous report:



This screen will appear if you have **'Security Audit'** or **'Raw Change Tracking'** selected in Reporting Options, and we will return to how to do this later in the Guide.

Click '**Next'** again and you will now generate your first report, like so:



You will see the time taken to generate the report is displayed. This is often extremely quick, although it can take longer depending on what options are selected.

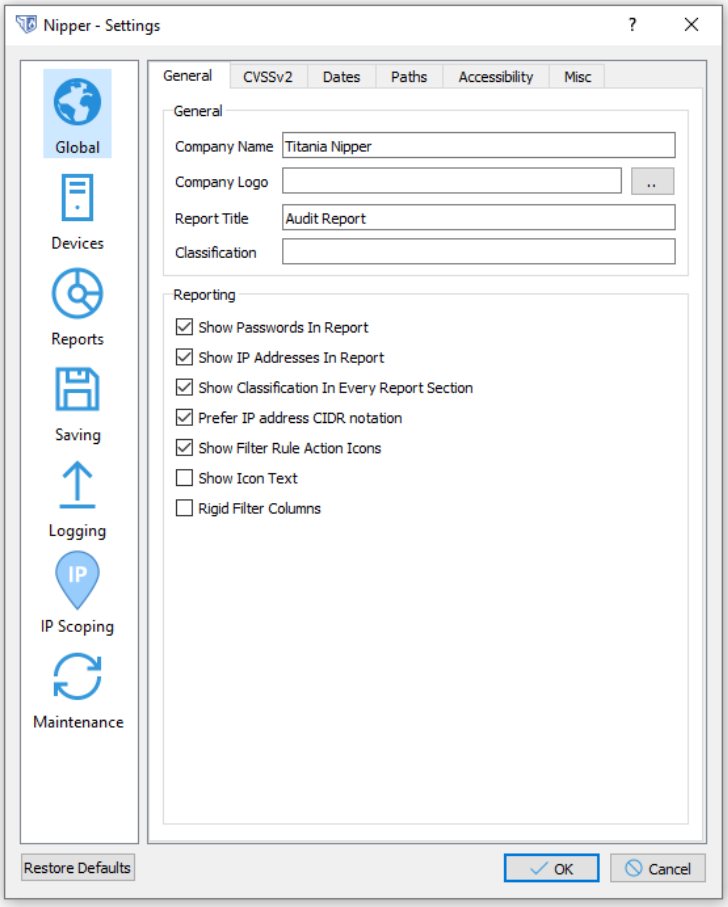
You may now like to take the time to read through the report and see the issues highlighted. Next, we will move on to various options for customising your reports.

Customizing Nipper Settings

By default, Nipper will present you with a vast amount of audit information. In these settings you can filter and refine the information presented within your reports as well as other useful options for Nipper's operation. **Settings** can either be found on the Nipper home screen or under **Tools** (or Ctrl & T).

General

This tab gives you the option to make changes to how the report displays.



Here is a list of fields that can be changed on an Audit report, once saved they will not change until there is further user input. These include:

Company Name – Modify the company name that will be used within the report

Company Logo – A logo for use in the report output

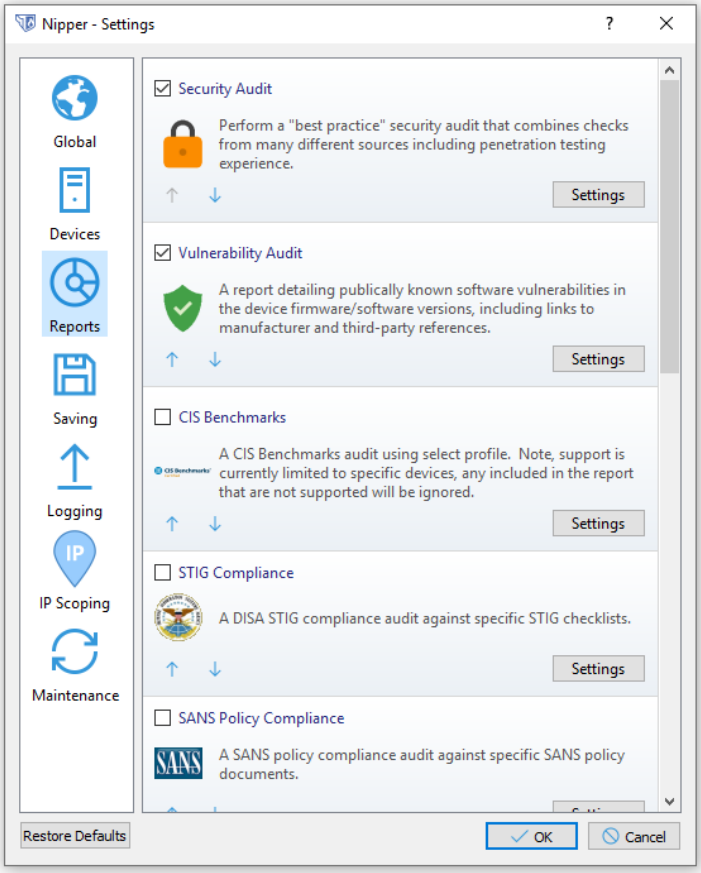
Report Title – The default title for the report, can be in the page header of some save formats

Classification – Allows you to classify the document displaying this on the first page, on every if selected

If you want to apply these changes to a report you currently have open, you will need to go to **'Report'** then **'Regenerate Report'**.

Reports

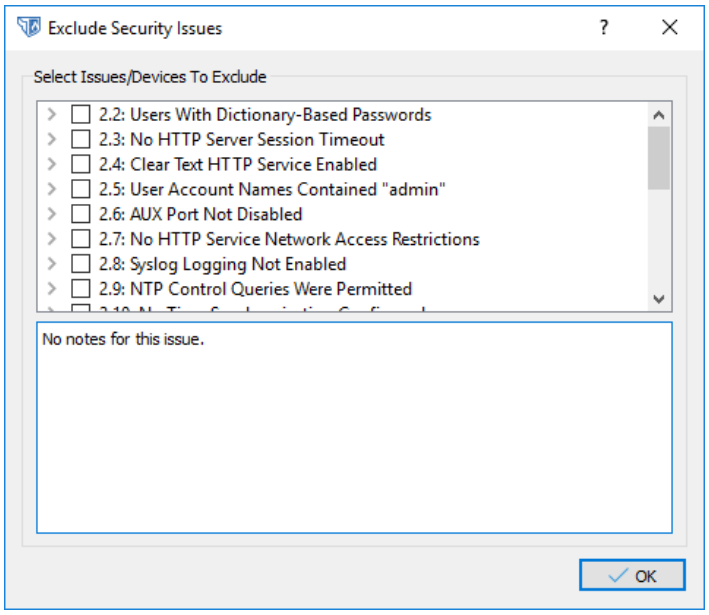
From this icon you can manage and customize the types of audits you carry out. Each audit report has its own settings and the report types can be moved into a specific order by using the arrow buttons. The order in which they are set here will also be the order that the Nipper audit report will list them.



Excluding Issues

The standard report settings may reveal some issues which you know are not issues for your company, for example if a certain device is in a test environment, or you have already located the problem and have decided that it is not a serious threat. Whatever the reason, Nipper allows you to easily remove any issue you like from a report.

After you have produced your report and identified the issues that you would like to remove, select **'Report'**, **'Exclude Issues'** to produce the menu below:



Select the issues you wish to exclude and click **'OK'**. Nipper will warn you that the report needs to be regenerated and that some details may be lost. When you go ahead, you will see that the relevant details have been removed from the report and the remaining issues will have been re- numbered appropriately.

IP Scoping Guide

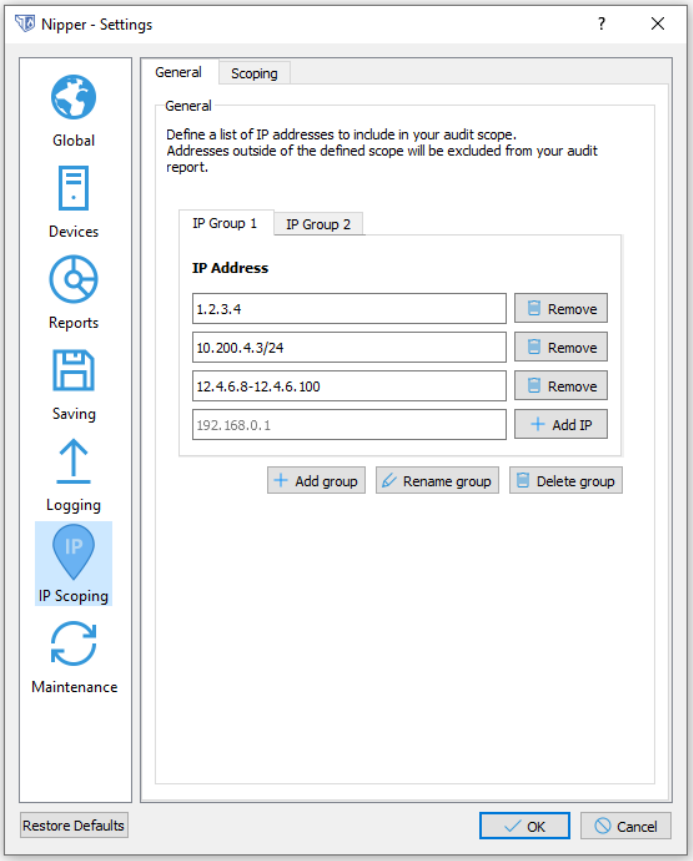
The **IP Scoping** feature allows you to reduce the scope of your audit to specific sets or ranges of IP addresses. For example, allowing us to focus in on rules that interact with a particular zone.

Configuring IP Scoping

You can define an **IP Scope** in the **IP Scoping** tab within the Settings. Settings can be accessed in any one of the following ways:

- Selecting **Settings** from the Tools menu.
- Using the shortcut, **Ctrl+T**.
- Clicking the **Change Settings** on the Nipper home screen.

Select the **IP Scoping** tab on the left to access the IP Scoping Settings sub-section.

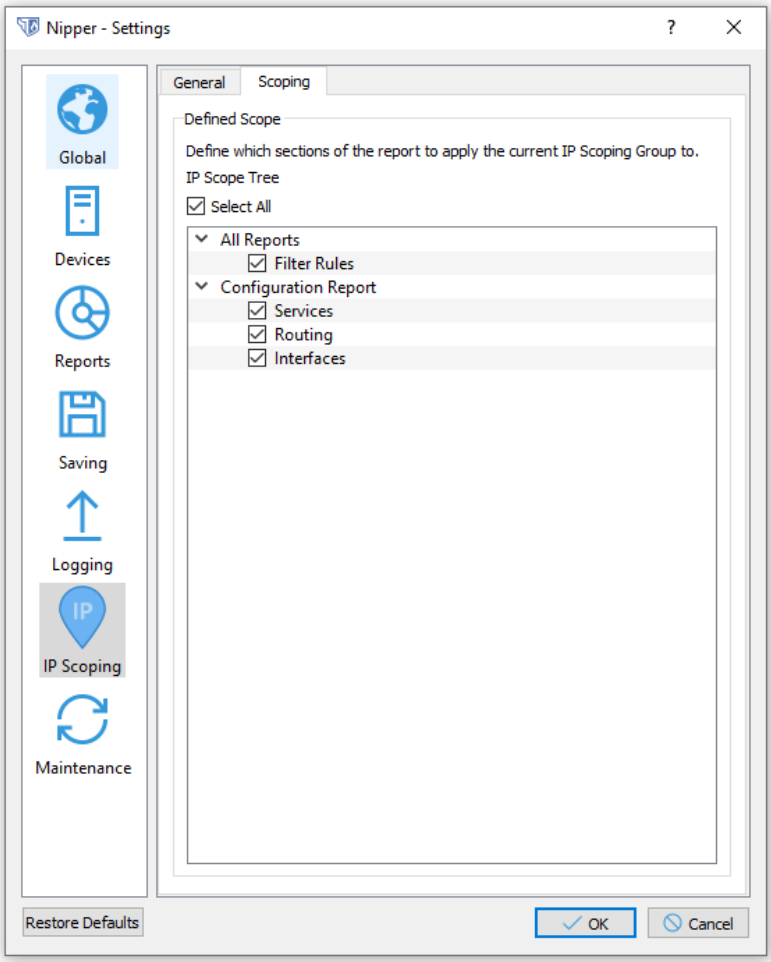


From the **General** tab, one or more **IP Scoping Groups** can be specified by adding IP Addresses. Any single one of these defined **IP Scoping Groups** can then be selected to be applied to the report, during report generation, as explained later in the **Selecting a current IP Scoping Group** section.
To add an IP to a Group, navigate to the IP Address Textbox, enter the desired IP Address, and click the **Add IP** button.
Nipper accepts **IP Scoping Group** IP Addresses in any of the following formats:

- A single IPv4 address, such as 192.168.0.1
- IPv4 CIDR Aggregations, such as 192.168.0.1/24
- IPv4 Ranges, such as 192.168.0.1-192.168.0.2

Please Note: Internet Protocol version 6 (IPv6) is not currently supported.

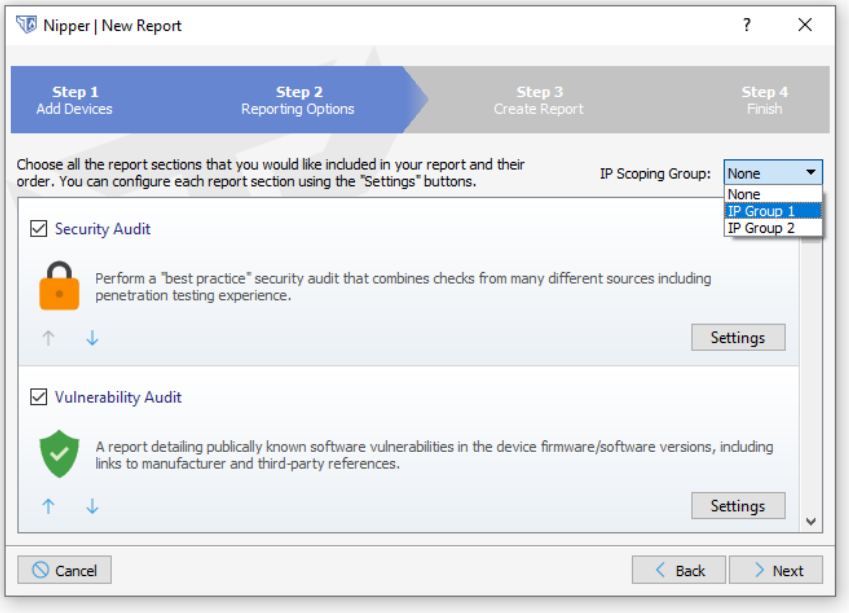
The **Scoping** tab allows more fine-grained control over which report sections are to be considered when applying the current **IP Scoping Group**.



Selecting (or deselecting) a section within this tab will instruct Nipper to apply (or not apply) the current **IP Scoping Group** to that portion of the report, accordingly.

Selecting a current IP Scoping Group

Setting the Current **IP Scoping Group** is done during the Report Generation process. On the 'Step 2 - Reporting Options' page of the **New Report Wizard**, you can set which **IP Scoping Group** to apply with the **IP Scoping Group** drop-down, located towards the upper right corner of the page.



Details of the IP Scoping Group that was applied are subsequently reflected in the Summary section of the final report, as shown below:

IP Scope

The IP scope of this audit was limited to the IP ranges listed in Table 2.

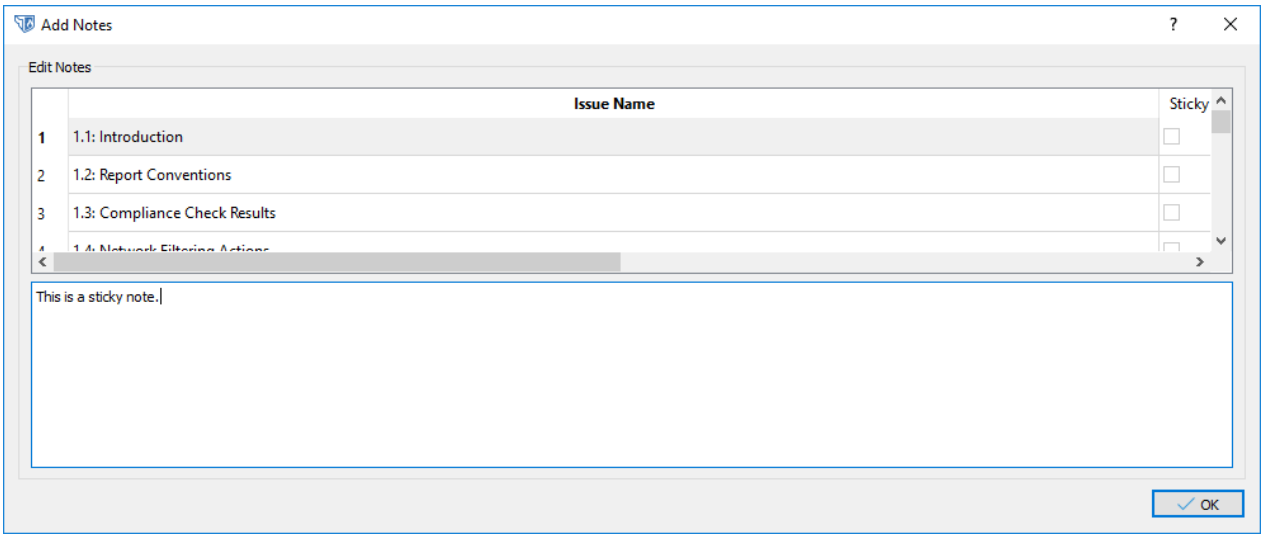
IP Scope
1.2.3.4
10.200.4.3/24
12.4.6.8-12.4.6.100

Table 2: Audit IP scope

By configuring and applying IP Scoping, and consequently removing inapplicable information in the final report, the relevance of Nipper reports, when auditing network devices which serve several different purposes, is vastly improved.

Adding Issue Notes

You can also add your own notes for each issue by going to **‘Report’** (once you have generated and audit report) then **‘Add Issue Notes’**. Again, simply select the issue and write what you would like to include. Click **‘OK’** to save the note.

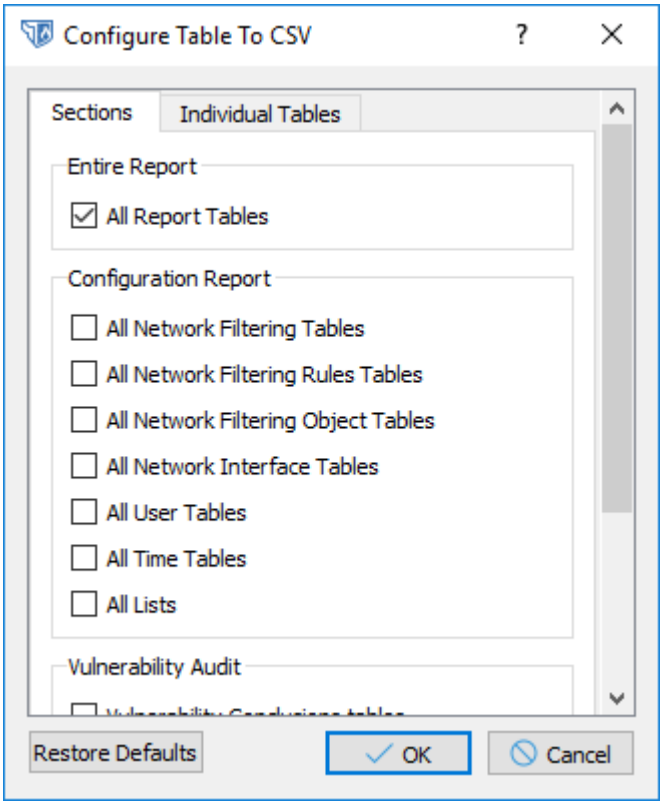


Saving Your Reports

Nipper reports can be saved out into a variety of formats, including PDF, HTML and XML. You can view the saving options by selecting **'File'** then **'Save'**.

Saving Tables

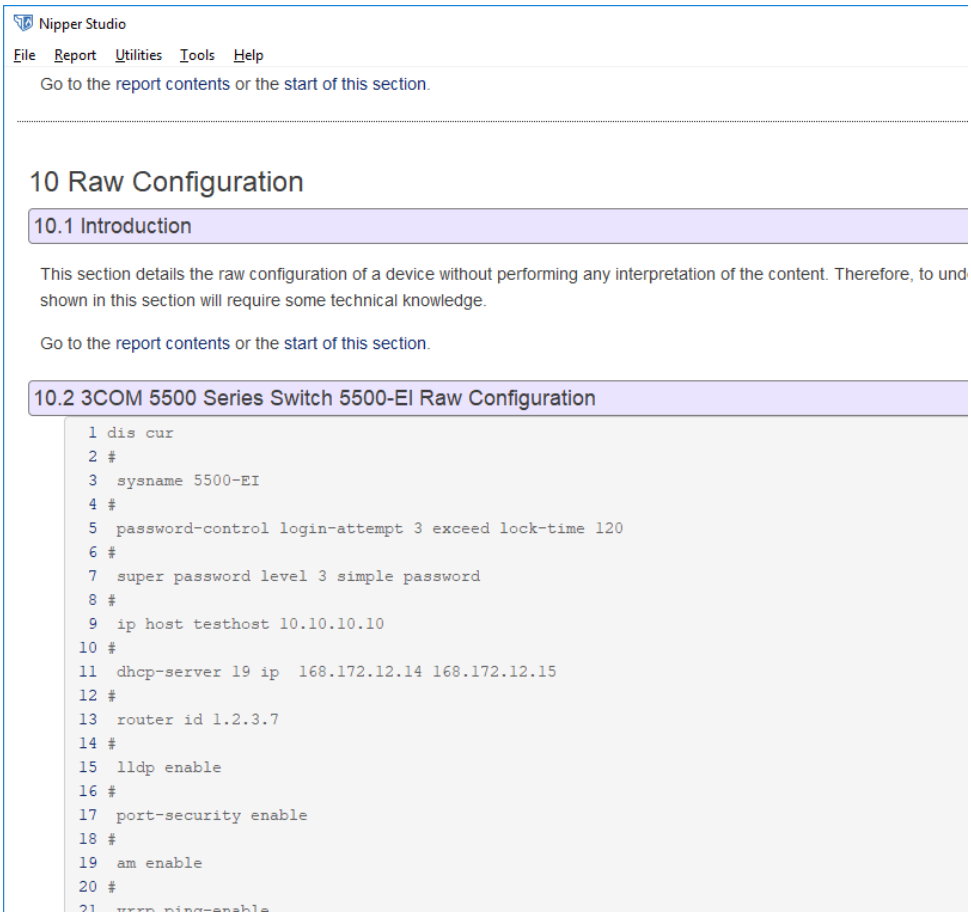
You can save out all or some of the tables in the Nipper report. Go to the **'Save'** menu and select **'Table to CSV'** or **'Table to SQL'**. You are given the option of what section of tables that you would like to save out or you can select individual tables (shown below).



Check the boxes you want to save and then simply click **'OK'** and save the files.

Report comparison

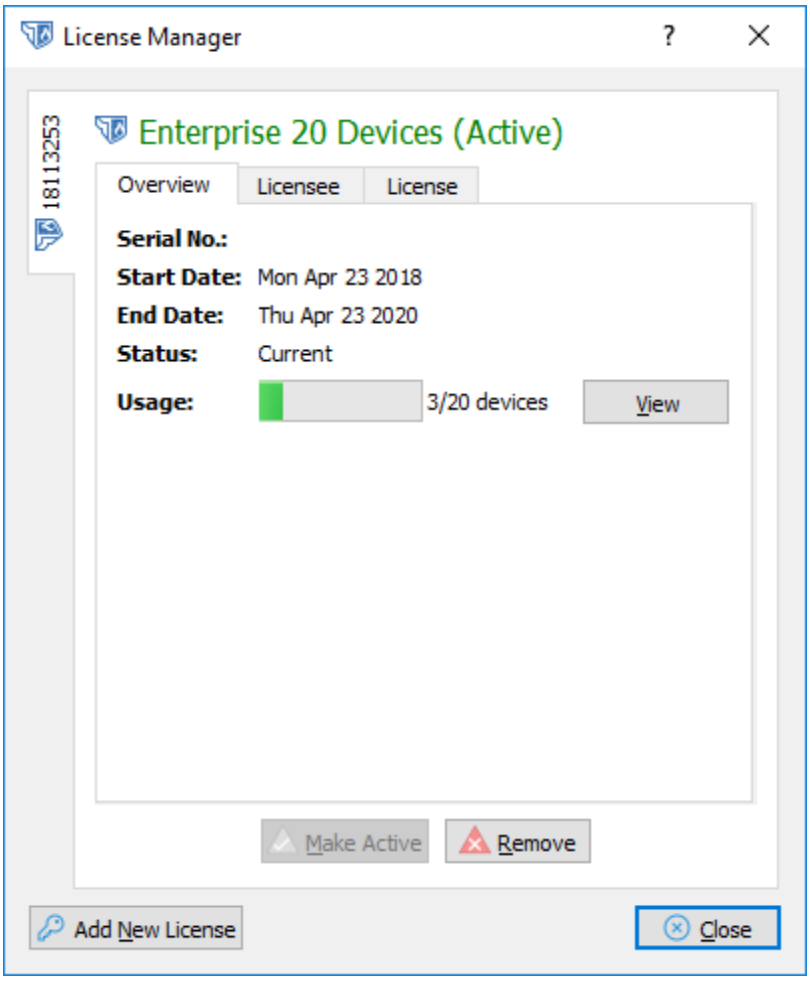
Security Audit Reports and Raw Configuration reports allow you to compare them to previous versions. Please see the example Raw Configuration Changes report below:



In order to make a comparison, first audit your device using Titania Nipper, selecting either Security Audit or Raw Configuration, and save the result as an XML file. When you later come to re-audit the report, if you select either Security Audit or Raw Configuration Changes, you will be asked if you want to add an XML file for comparison.

Managing licenses

Nipper allows you to add and view your licenses, manage multiple licenses and view a list of the devices you have audited. To do this, go to ‘Tools’, ‘Manage Licenses’. The window below will appear:



The tabs along the top of the window are: **‘Overview’**, **‘Options’**, **‘Licensee’** and **‘License’**. The **‘Overview’** tab is above, listing key details of the license. **‘Options’** explains what features are enabled in the license, **‘Licensee’** has the details you entered on the website when you registered and **‘License’** has the license text, agreed when you activated.

The tabs on the left hand side are labelled with the serial numbers of your respective licenses, allowing you to look through them for information on each individual license.

You will also see the **‘Make Live’** and **‘Remove’** buttons at the base of this license and note that the **‘Make Live’** button is currently greyed out. Where you have multiple licenses and are currently viewing an inactive license, this button will make it live. **‘Remove’** will remove the current license.

To add another license, click on **‘Add License’** then follow the instructions (which will be the same as those in ‘Adding a license to Titania Nipper’ within this Guide).

If you click on the **‘View’** button next to the device usage, Nipper will list the devices you have audited, by their hostname and the date they were audited.

Conclusion

We hope that you have found our Beginner’s Guide to Nipper useful and now feel confident in navigating your way around Titania Nipper’s features.

There are many more features and if you would like to know more about how to get the most out of your Nipper 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

Further support documents can also be found on our website www.titania.com