Titania Nipper User Guide

Software Version: 2.13.X

Contents

Nipper v2.x User Guide

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

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 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.

The purpose of this guide is to provide a user's guide to Nipper and is aimed at anyone new to Nipper 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.

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

This User's Guide is based on Nipper Release 2.13.0

This document is intended to provide advice and assistance for the installation and running of Nipper software. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support staff if required.

No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.

The use of Nipper software is subject to the acceptance of the license agreement.

What reports are available in Nipper?

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.

- **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.

- **Cisco PSIRT Audit**: This report type utilises a Cisco PSIRT advisories file, managed by the global Cisco PSIRT team, to generate a more precise audit of vulnerabilities within Cisco Software.

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

- **CMMC**: Assess compliance with the DoD's Cybersecurity Maturity Model Certification.

- **NIST 800-171**: Assess compliance with security requirements recommended in NIST Special Publication 800-171.

- **STIG Compliance**: A DISA STIG compliance audit against specific STIG checklists.

- **SANS Policy Compliance**: A SANS policy compliance audit against specific SANS policy documents.

- **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.
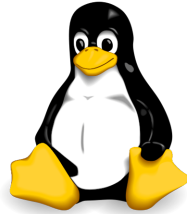
System Requirements

Below are the basic system requirements needed to operate Nipper

Microsoft Windows 7 or above (Server 2012 or above)

600MB disk space
4GB memory


GNU/Linux (Ubuntu, CentOS)

300MB disk space
2GB memory

How to download Nipper

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

Once you are a registered user of our customer account (https://account.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 "Downloads".
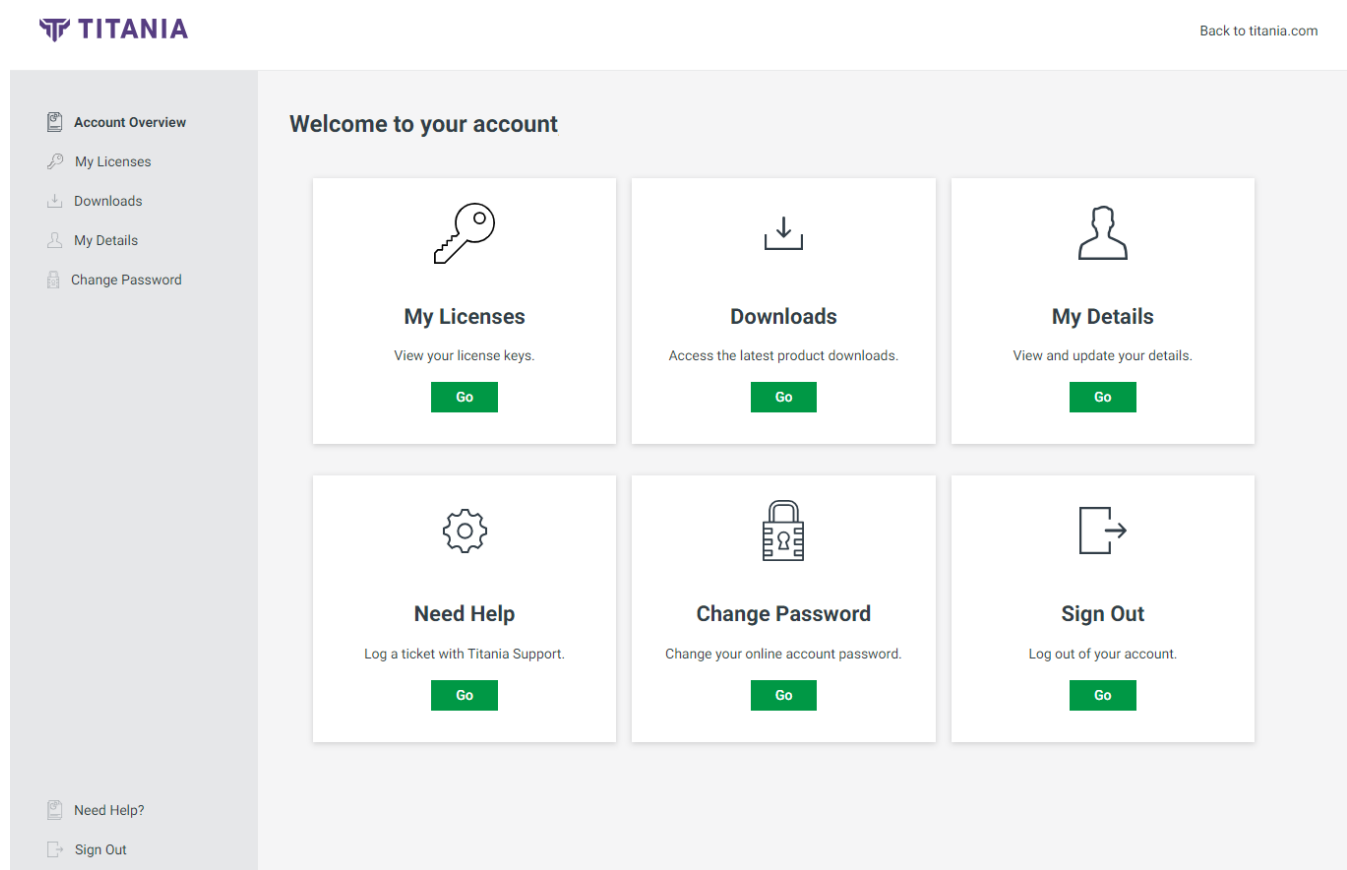
From the Download page you can choose your operating system and architecture for the download you require.

TITANIA

- Account Overview
- My Licenses
- **Downloads**
- My Details
- Change Password

Downloads

Nipper

	Platform	Version	Size	
Microsoft	Microsoft Windows x64	3.0.0	144.81 MB	Download
	Microsoft Windows x64	2.13.4	138.45 MB	Download
CentOS	CentOS 7 x64	2.13.2	68.34 MB	Download
Ubuntu	Ubuntu 18.04 x64	2.13.2	104.86 MB	Download

Installing Nipper

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 sections give detailed instructions on how to install Nipper on Windows and Linux operating systems.

> Please note that on some Linux operating systems, further commands and installation of dependencies may be required. Please see the Linux installation section for details.

> Note: 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 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 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 Nipper, and the Qt5 dependencies should be resolved for you.

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. nipperstudio-2.13.0-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. nipperstudio-2.13.0-centos-7-x86_64.rpm)

Ubuntu

Double clicking the .DEB installation file which is downloaded from the Download Portal will
carry out the installation as per the "Installing Nipper on Windows Operating Systems " on the
next page.

Installing Nipper on Windows Operating Systems

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

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

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

3. 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.

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

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

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

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

Adding a license to Nipper

The first time you run Nipper you will need to add your license.

1. When the add license wizard appears click **Add License**.

2. After you click **Add License**, you will be asked for your <u>Serial Number</u> and <u>Activation Code</u>. 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.

> Note: Nipper allows you to add multiple licenses and will set the most recently added license active by default. If you wish to change which license is currently in use this can be amended within **Tools** -> **Manage Licenses** (or **Ctrl & L**) and select **Make Active** on the appropriate license.

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

3. Enter the <u>Serial Number</u> and <u>Activation Code</u> details into the relevant boxes and click **Next**.

4. You will then be asked to agree to our license. Tick the box next to 'I have read and agree to the license' then click **Next**.

5. 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.

Offline Activation steps

Nipper can be installed, activated and used in a fully offline environment. Once you have installed Nipper you will be prompted to add a license.

1. Choosing **Add License** will take you to the screen requesting your Serial Number and Activation code. If you are unsure of these details these can be found by the license owner logging into https://www.titania.com and clicking My Account.

2. Make sure **Show Options** is selected then click **Next**.

3. When you have a read and agreed to the Nipper License agreement, check the box next to 'I have read and agree to the license', then click **Next**.

4. Select **Off-line file transfer**, then click **Next**.

5. You will now need to save the License Activation Request on to a USB pen drive or other removable media as you will need to transfer the License Activation Request on to a system that has an internet connection. Select the **Save License Activation Request** button to save this.

6. Transfer the License Activation Request on to a system that has internet connectivity and go to https://sync.titania.com/offline.php and upload the Activation request.

7. Click **Choose File** then upload the License Activation Request file generated from the offline installation of Nipper. Click **Download Response** to download the titania-response.nlr file, save the titania-response.nlr file to your removable media and transfer back to the offline system.

8. Click the **Load License Activation Response** button and load the titania-response.nlr file.

9. Click **Next** and Nipper will now be licensed and fully activated.

Navigating around Nipper

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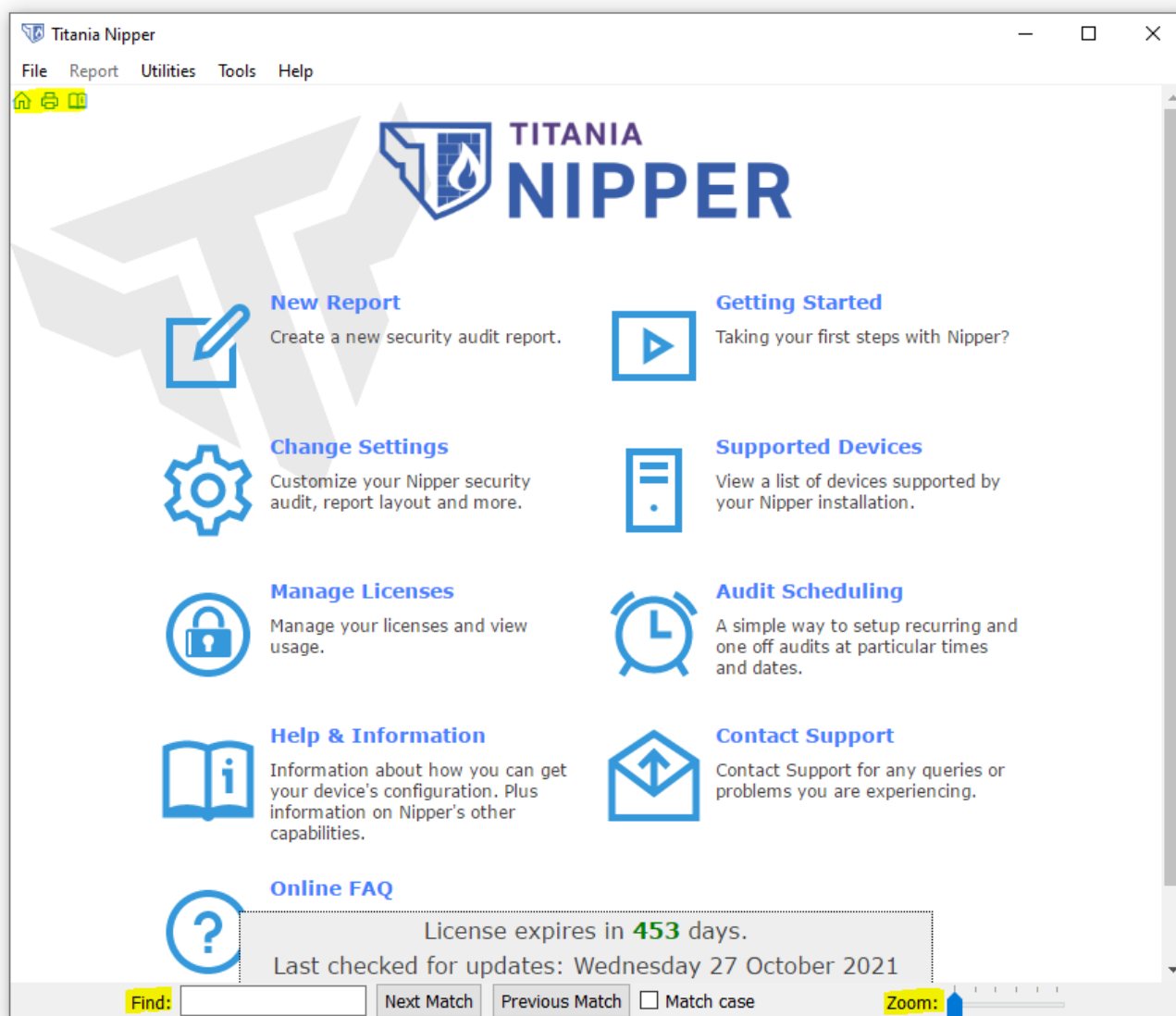
We have highlighted navigation icons on the top left of the page and the search toolbar at the bottom of the page.

Also, when moving around 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. Guidance for this is shown in "Creating your first report with Nipper" on page 18

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.

Manually retrieve configuration files
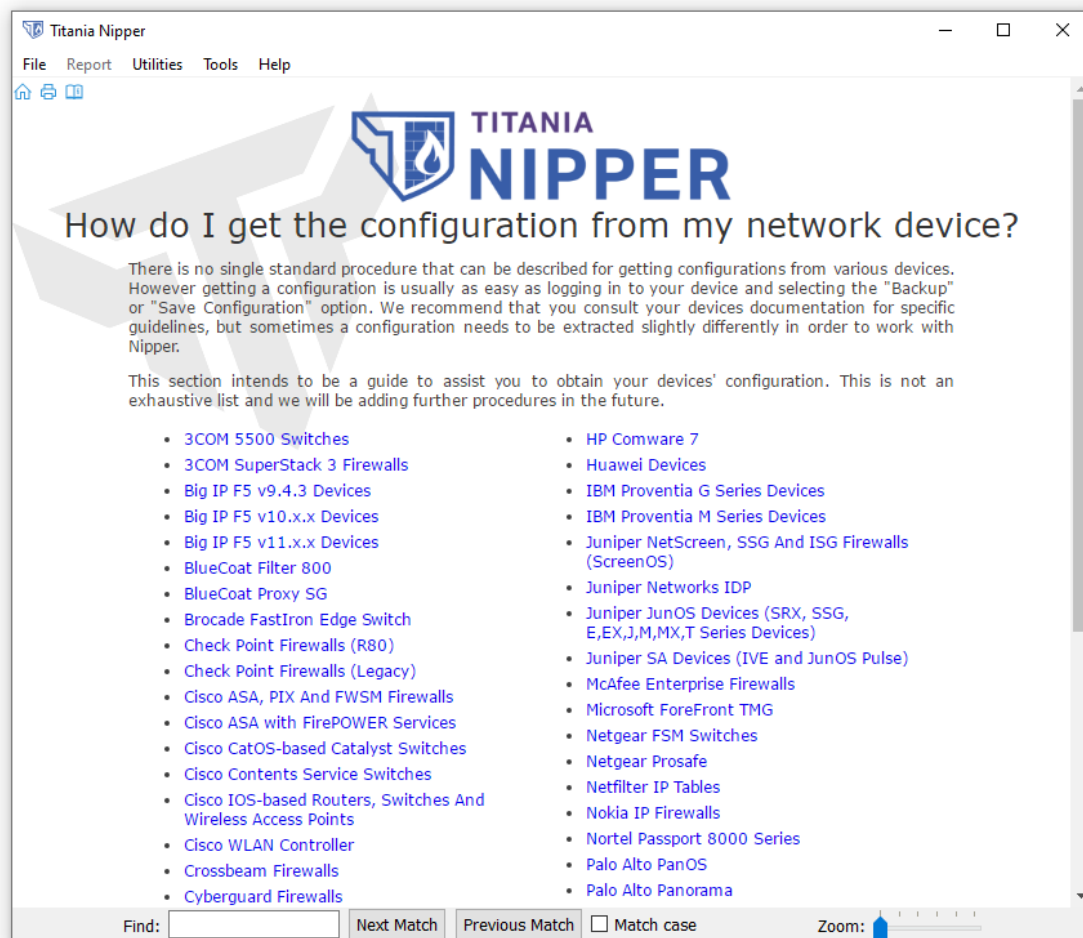
Here, we explain how you can find instructions on how to manually retrieve your configuration files.

1. Open Nipper, whereupon you will be presented with the homepage.

2. Click on 'Help & Information', which will present you with the following screen:
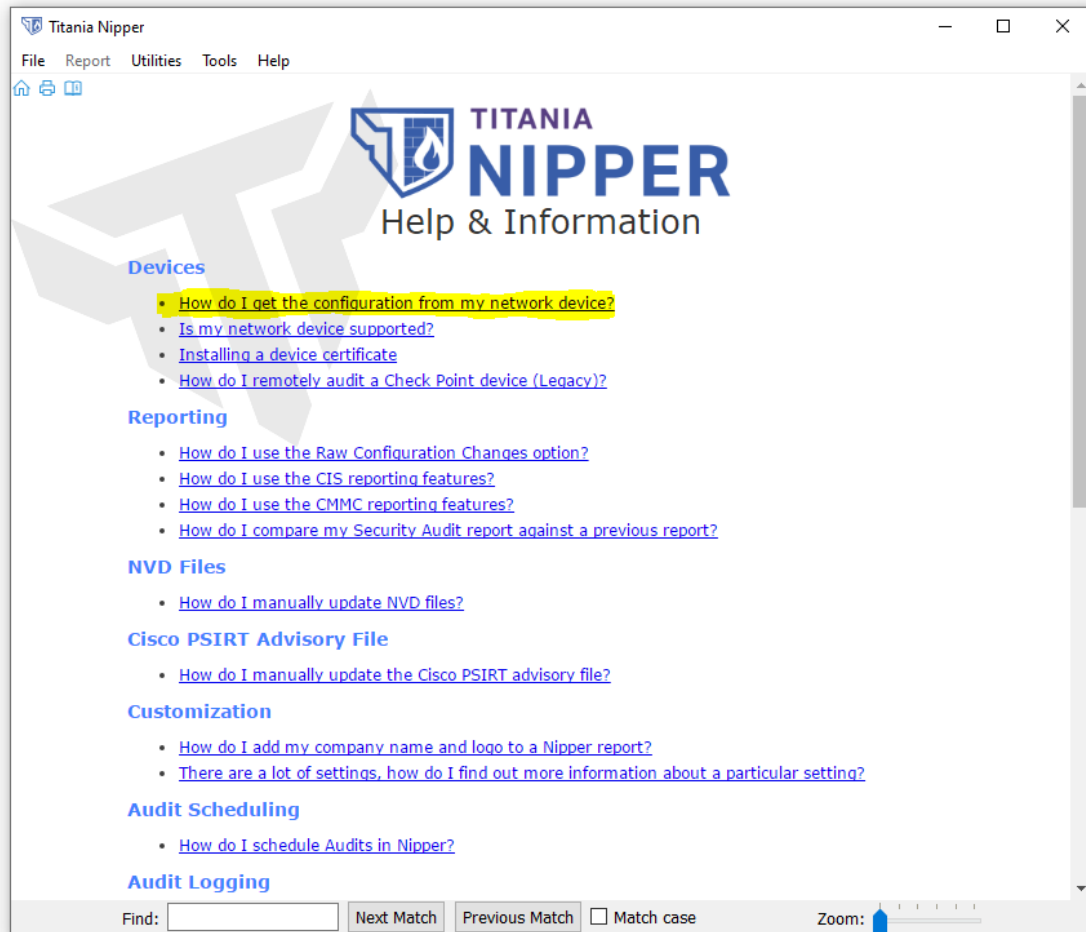
3. Click on 'How do I get the configuration from my network device?' to bring up the following screen and then select your device:

How do I get the configuration from my network device?

There is no single standard procedure that can be described for getting configurations from various devices. However getting a configuration is usually as easy as logging in to your device and selecting the "Backup" or "Save Configuration" option. We recommend that you consult your devices documentation for specific guidelines, but sometimes a configuration needs to be extracted slightly differently in order to work with Nipper.

This section intends to be a guide to assist you to obtain your devices' configuration. This is not an exhaustive list and we will be adding further procedures in the future.

- 3COM 5500 Switches
- 3COM SuperStack 3 Firewalls
- Big IP F5 v9.4.3 Devices
- Big IP F5 v10.x.x Devices
- Big IP F5 v11.x.x Devices
- BlueCoat Filter 800
- BlueCoat Proxy SG
- Brocade FastIron Edge Switch
- Check Point Firewalls (R80)
- Check Point Firewalls (Legacy)
- Cisco ASA, PIX And FWSM Firewalls
- Cisco ASA with FirePOWER Services
- Cisco CatOS-based Catalyst Switches
- Cisco Contents Service Switches
- Cisco IOS-based Routers, Switches And Wireless Access Points
- Cisco WLAN Controller
- Crossbeam Firewalls
- Cyberguard Firewalls

- HP Comware 7
- Huawei Devices
- IBM Proventia G Series Devices
- IBM Proventia M Series Devices
- Juniper NetScreen, SSG And ISG Firewalls (ScreenOS)
- Juniper Networks IDP
- Juniper JunOS Devices (SRX, SSG, E,EX,J,M,MX,T Series Devices)
- Juniper SA Devices (IVE and JunOS Pulse)
- McAfee Enterprise Firewalls
- Microsoft ForeFront TMG
- Netgear FSM Switches
- Netgear Prosafe
- Netfilter IP Tables
- Nokia IP Firewalls
- Nortel Passport 8000 Series
- Palo Alto PanOS
- Palo Alto Panorama

Find: [ ] Next Match Previous Match ☐ Match case Zoom:

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. There are copies of these instructions, which can be accessed by anyone (no user account required) at Device Guides
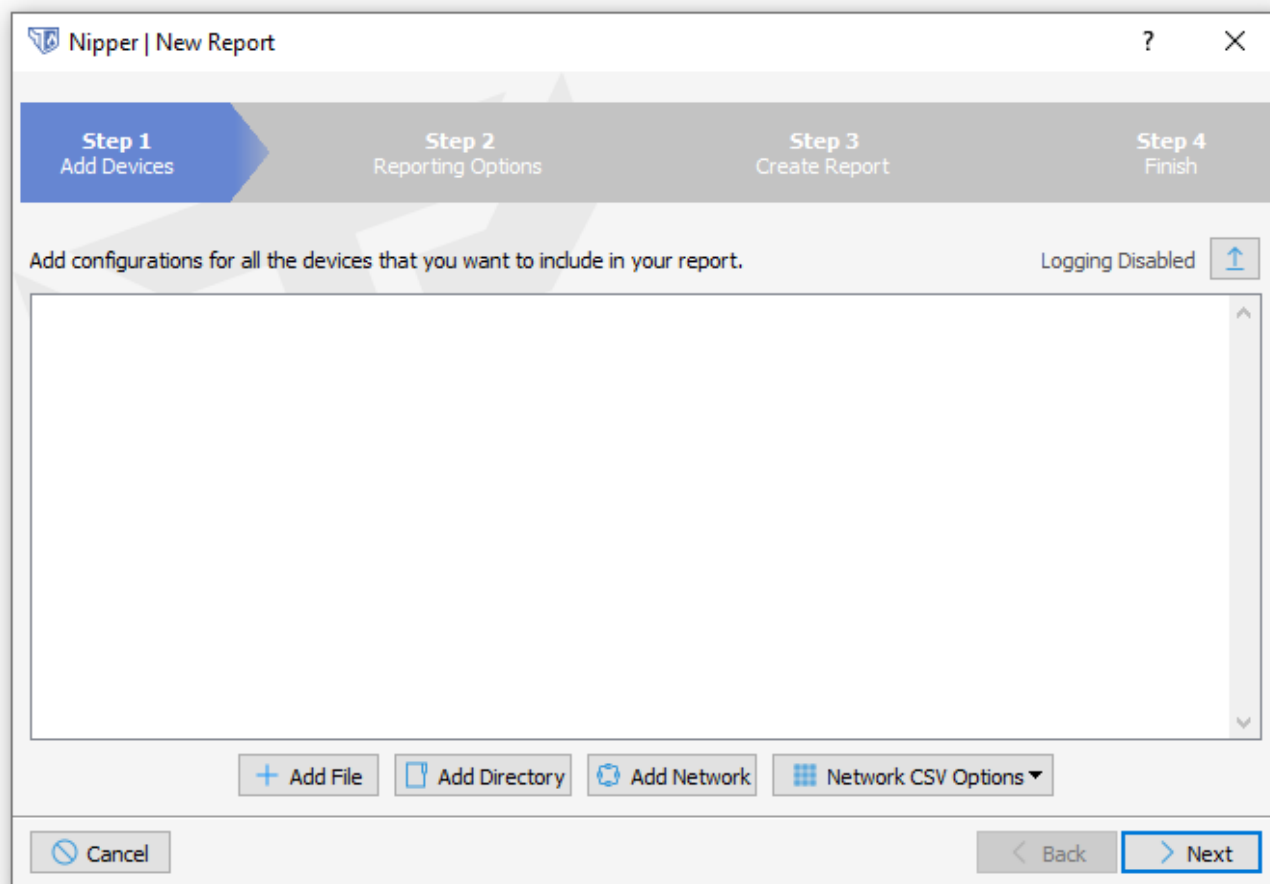
If you are unable to find the instructions to retrieve the configuration from a supported device either in the Nipper software or on our website, please inform support@titania.com. In the meantime, you should be able to find the relevant details in the device's documentation.

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 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 Nipper. If you are adding your own files, you will need to navigate to wherever you have stored the files.

Add File

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.

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.
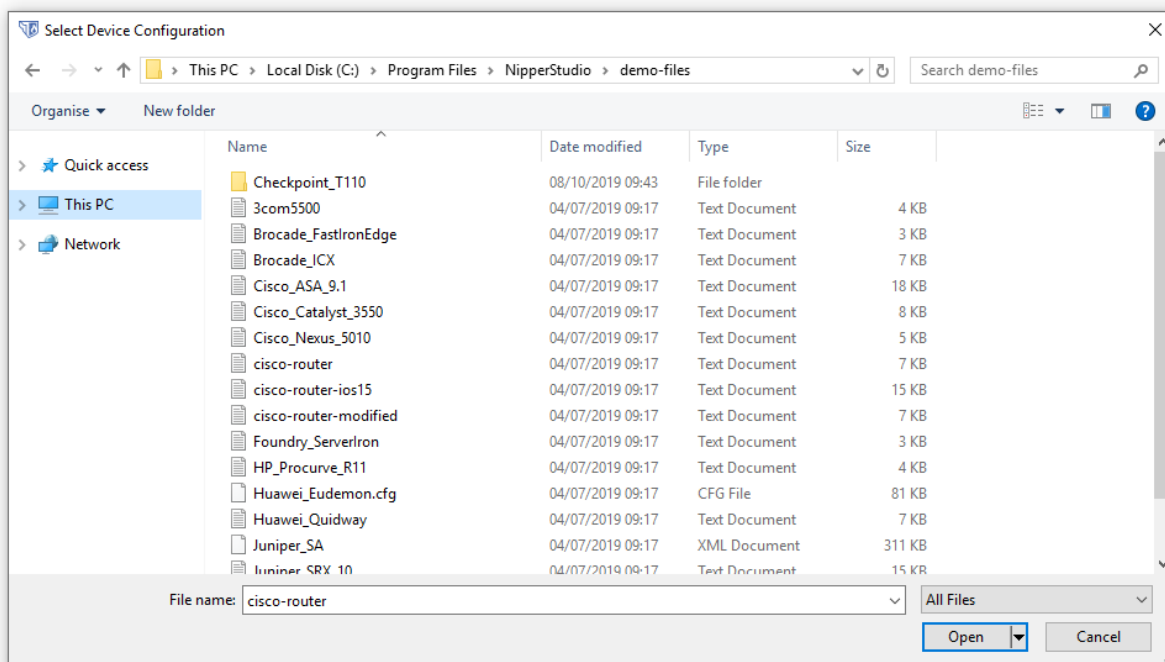
Add files remotely

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

Add Remote Config   ?   ✕

Device Type

Name: [▼]

Version: [▼]

Device Details

Host Address: [192.168.1.1]

Username: [admin]

Password: [   ]

Show Password: ☐

Protocol

Protocol to Use: [▼]

Port: [   ]

Privilege Password: [   ]

Show Password: ☐

Proxy Server

Address: [   ]   Port: [   ]

[⊙ Add]   [⊘ Cancel]

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.

Adding a Directory

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.

To audit a directory you will need to direct Nipper to an existing folder containing multiple configuration files which Nipper is able to access.

1. To direct Nipper to your directory choose **New Report** on the main menu, and then **Add Directory.**

2. Navigate to the directory with the configurations inside. Select the folder.

3. The report screen will contain all of the configurations:
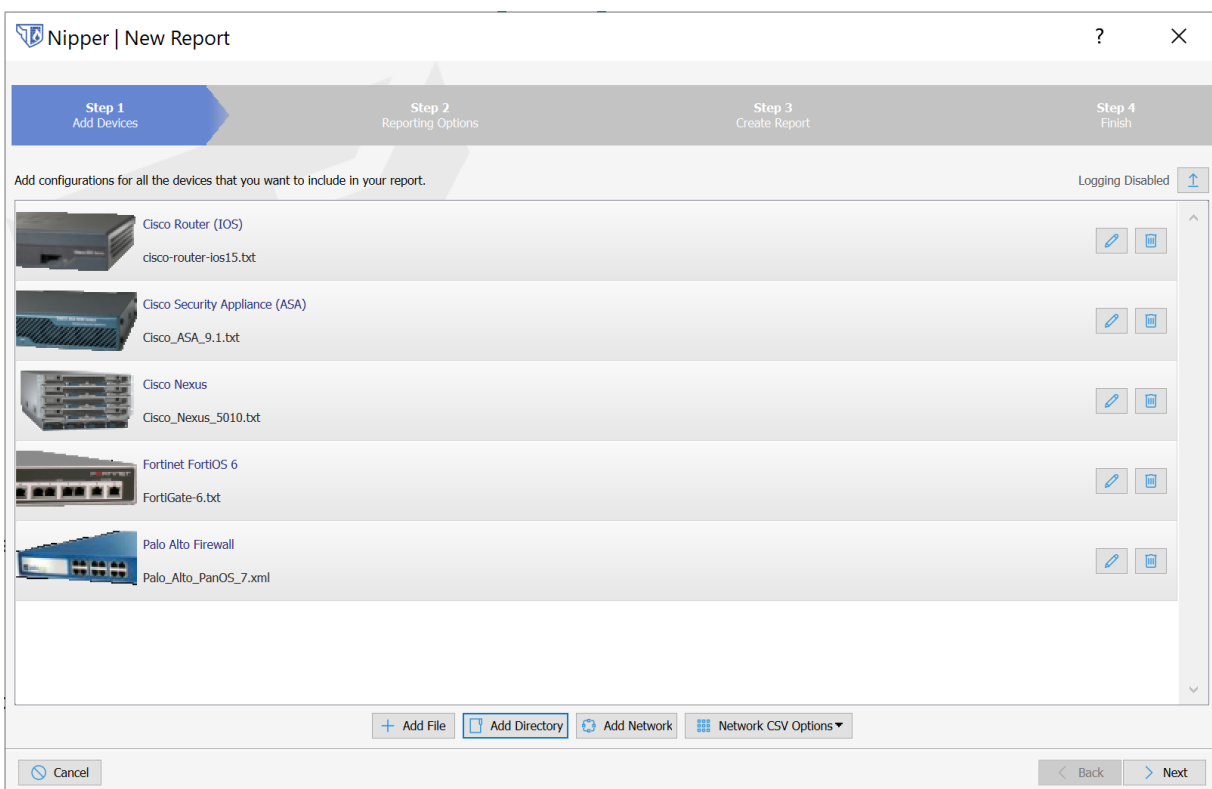
After completing the steps above you will now be able to audit multiple configuration without individually selecting them. This will also assist with managing configurations.

Adding network devices via CSV

Creating a CSV list of devices allows you to bulk import the stored credentials of multiple devices to allow Nipper to directly retrieve their configurations via the network.

1. Initially you will need to create a new report and manually add your chosen network devices using the **Add Network** option.

2. Once you have your required devices listed choose **Network CSV Options** then **Export Network Devices as CSV.**

3. This will generate a file similar to below which can be stored for later audits or shared with colleagues to use with their Nipper tool.

| Device Type	Version	Host Address	Username	Password	Protocol	Port	Timeout	Privilege Password
Cisco Router (IOS)	DEFAULT	10.200			SSH		5000	
Cisco Security Appliance (ASA)	DEFAULT	10.200			SSH		5000	

> ✖ Please note the information in this CSV is not encrypted so it is strongly advised to store this in a secure location appropriate to your organisation's policies and procedures.

1. Select **Network CSV Options** and **Import Network CSV**. Navigate to the location you have stored your CSV file.

2. To import and audit the devices listed within the CSV simply choose **New Report** from the main menu then **Add Network**.

3. You will be able to add or remove devices (using **Add Network**) if required from the New Report screen and export this list as an updated CSV.

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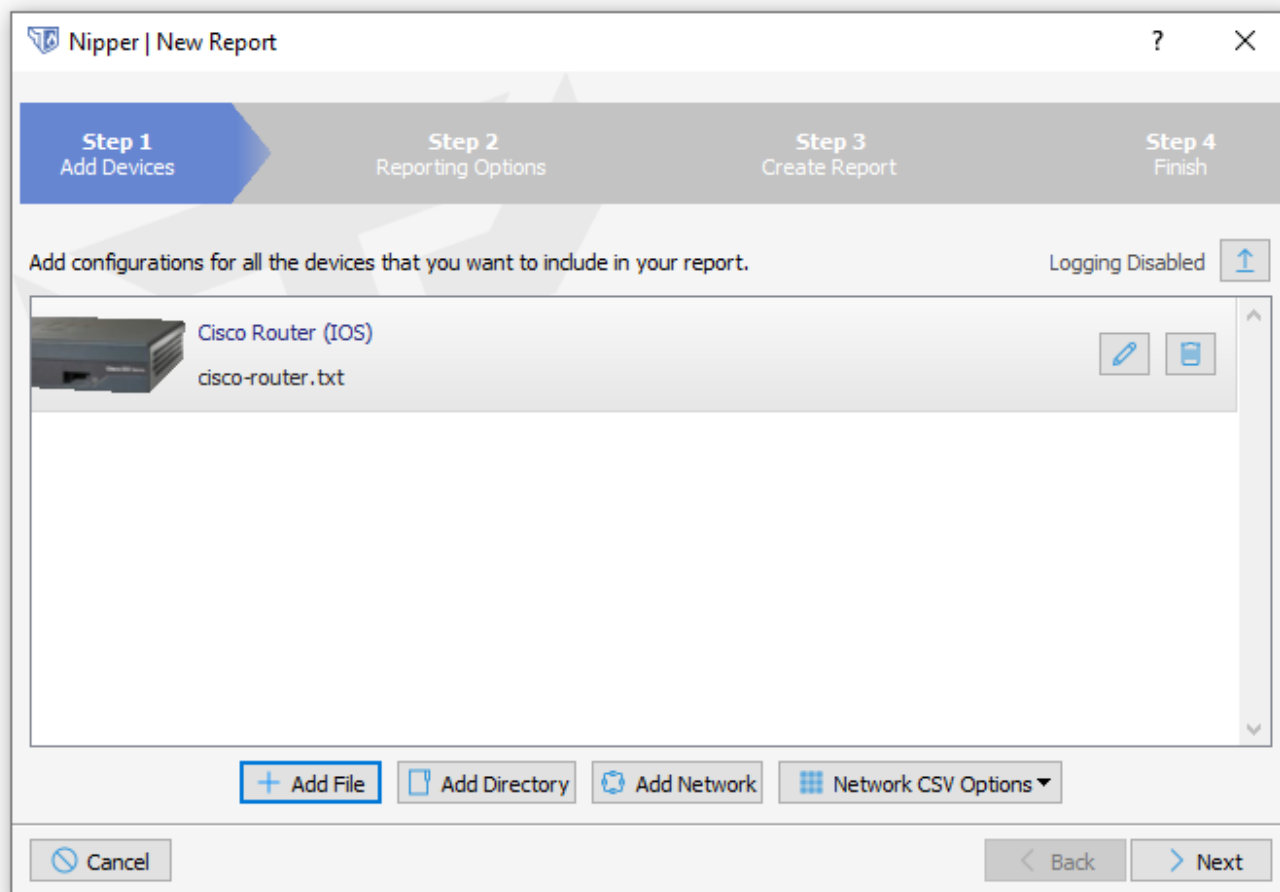
As you can see, the most recently added device is shown, along with the same options to add additional devices as previously discussed. You can add multiple devices if you wish to generate a multi device report.

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 from the config file, audit findings may not be 100% accurate.
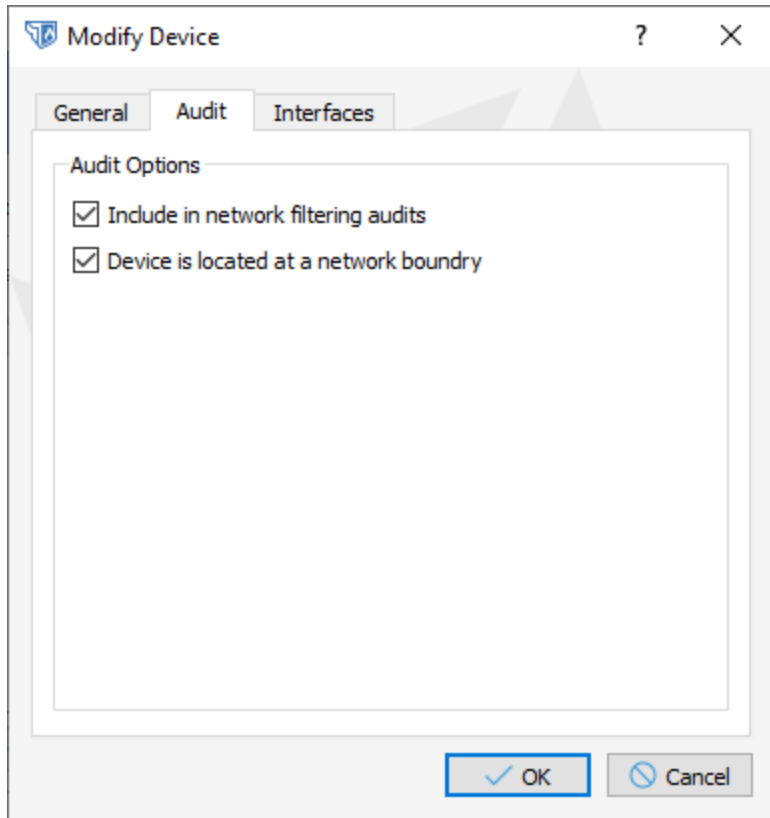
Hostname: Name of the network device

Device Model: Model of the network device

OS Version: Operating System version of the network device (to major/minor level only i.e. 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 utilized for STIG audits:
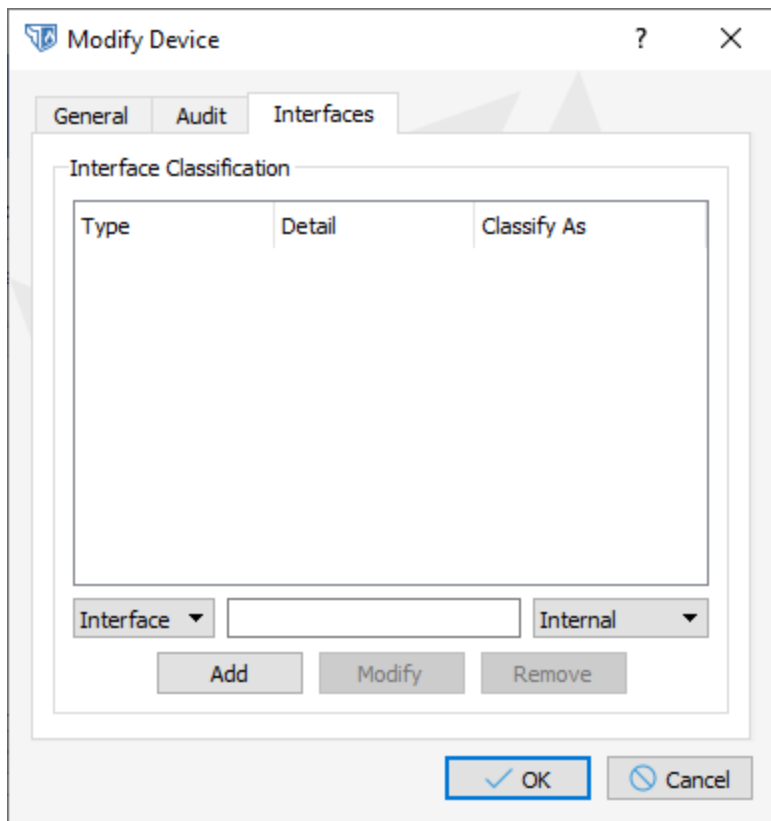
Interface Classification: This is used in the STIG audit type to stop Nipper prompting for manual interface information.

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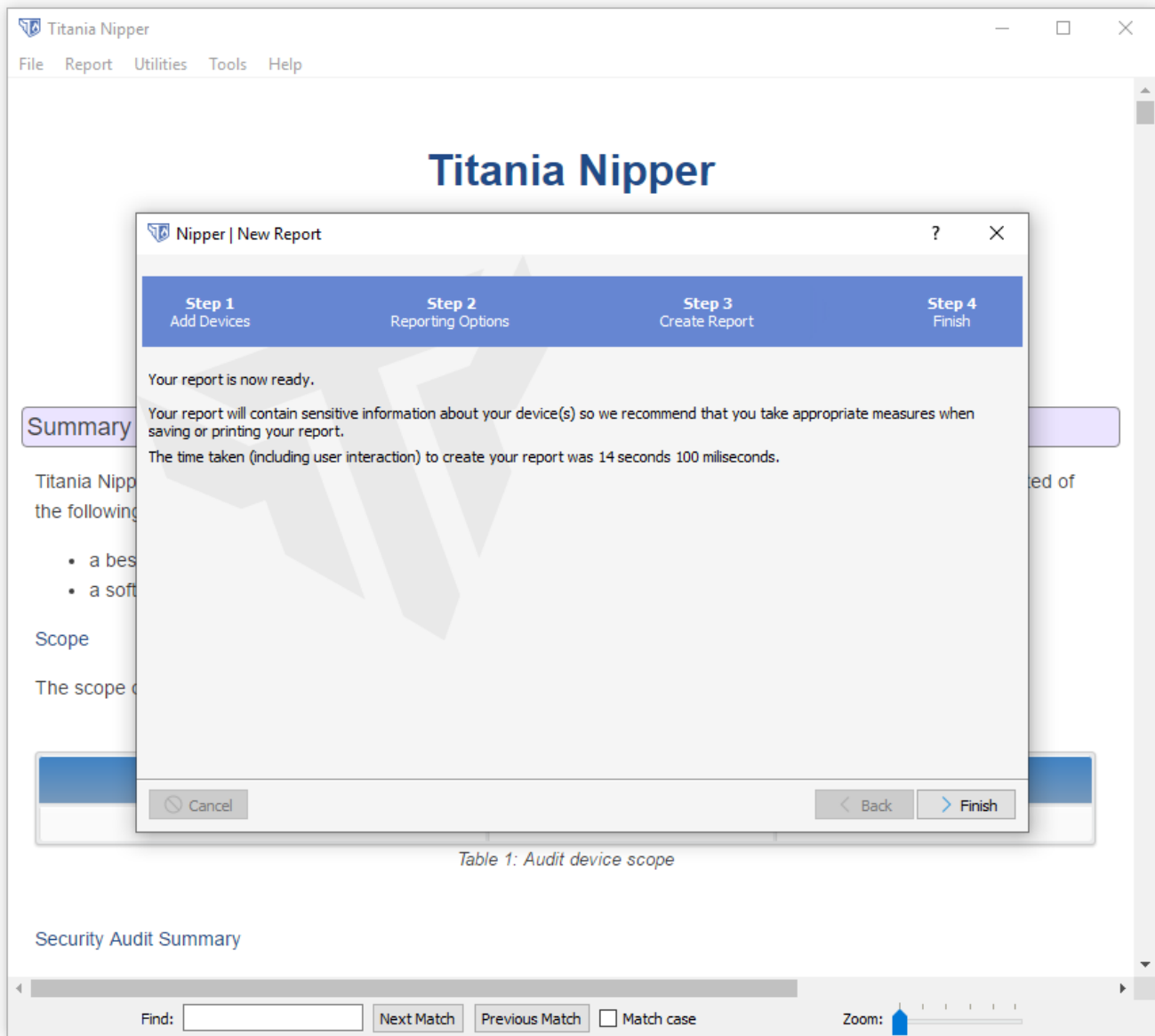
You will see the time taken to generate the report is displayed. This is often extremely quick, although it can take longer depending on what options are selected.

You may now like to take the time to read through the report and see the issues highlighted.

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 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**'.

Audit Report Settings

From the **Reports** 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.

Nipper | New Report   ?   ✕

Choose all the report sections that you would like included in your report and their order. You can configure each report section using the "Settings" buttons.

IP Scoping Group: [None ▼]

☑ Security Audit

🔒 Perform a "best practice" security audit that combines checks from many different sources including penetration testing experience.

↑ ↓   [Settings]

☑ Vulnerability Audit

🛡 A report detailing publically known software vulnerabilities in the device firmware/software versions, including links to manufacturer and third-party references.

↑ ↓   [Settings]

☑ Cisco PSIRT audit

CISCO Cisco PSIRT vulnerability audit of software/firmware versions against Cisco's database of known
Cisco PSIRT vulnerabilities. The report includes a description, references, ratings, and more.

↑ ↓   [Settings]

☐ CIS Benchmarks

CIS Benchmarks A CIS Benchmarks audit using select profile. Note, support is currently limited to specific devices, any included in the report that are not supported will be ignored.

↑ ↓   [Settings]

⊘ Cancel   ‹ Back   › Next

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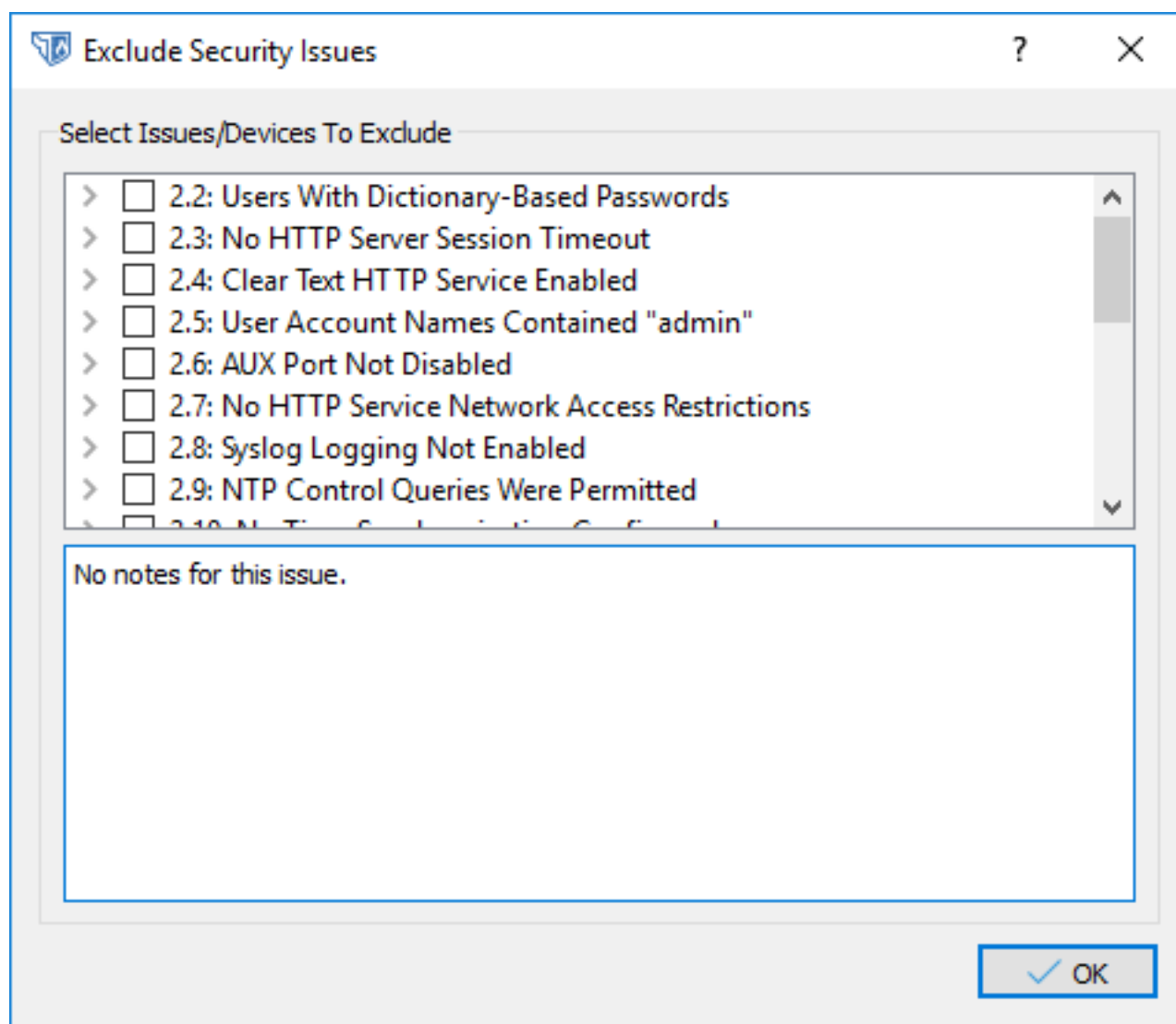
Select the issues you wish to exclude and click **OK**. Nipper will warn you that the report needs to be regenerated and that some details may be lost. When you go ahead, you will see that the relevant details have been removed from the report and the remaining issues will have been re- numbered appropriately.

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 **Change Settings** on the Nipper home screen.

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

Nipper - Settings

General | Scoping

General

Define a list of IP addresses to include in your audit scope.
Addresses outside of the defined scope will be excluded from your audit report.

IP Group 1 | IP Group 2

IP Address

1.2.3.4	🗑 Remove
10.200.4.3/24	🗑 Remove
12.4.6.8-12.4.6.100	🗑 Remove
192.168.0.1	+ Add IP

+ Add group | ✎ Rename group | 🗑 Delete group

Global | Devices | Reports | Saving | Logging | IP Scoping | Maintenance

Restore Defaults | ✓ OK | ⊘ Cancel

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

> Note: Internet Protocol version 6 (IPv6) is not currently supported.
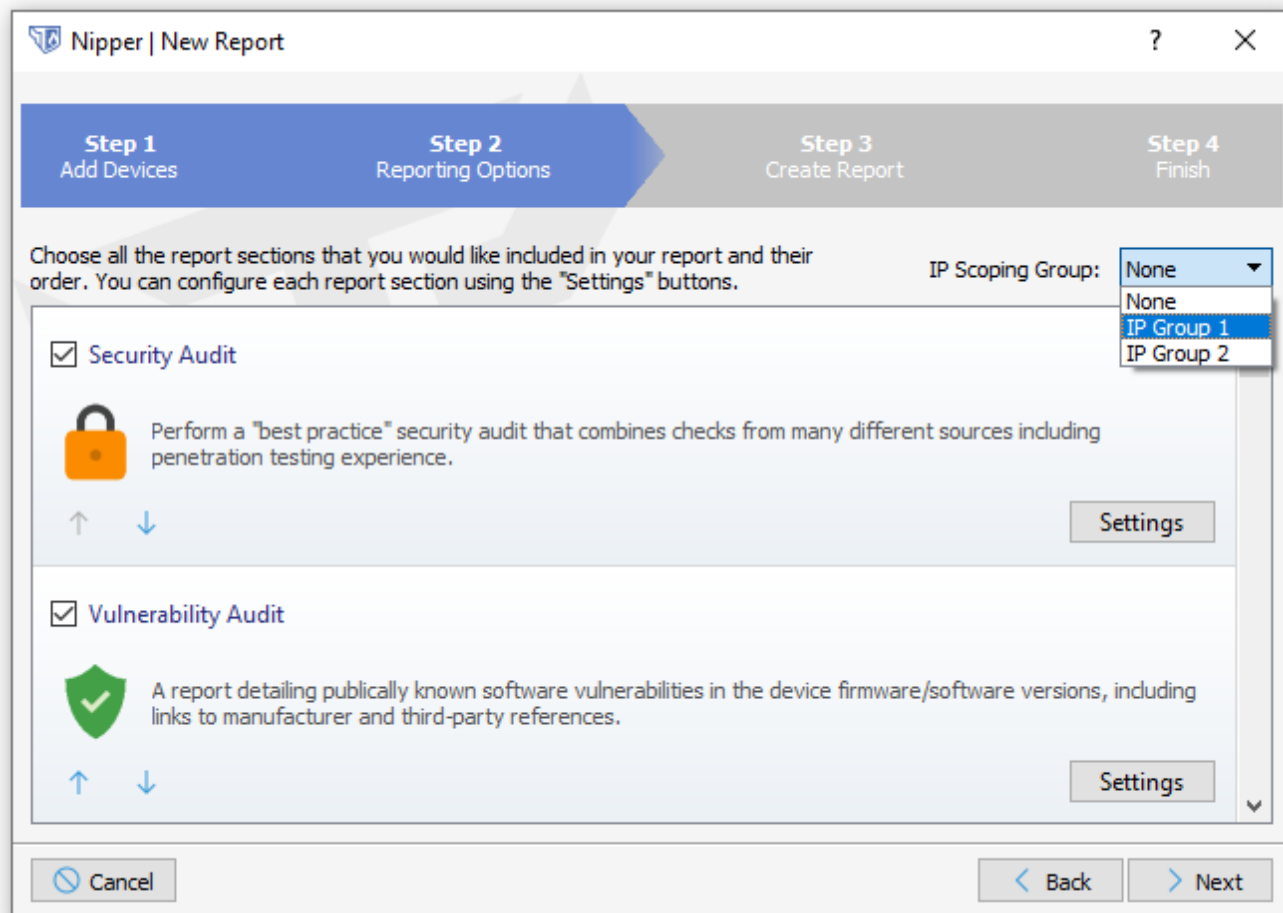
The **Scoping** tab allows more fine-grained control over which report sections are to be considered when applying the current **IP Scoping Group**.

Nipper - Settings

General | **Scoping**

Defined Scope

Define which sections of the report to apply the current IP Scoping Group to.

IP Scope Tree

☑ Select All

- ∨ All Reports
  - ☑ Filter Rules
- ∨ Configuration Report
  - ☑ Services
  - ☑ Routing
  - ☑ Interfaces

Global

Devices

Reports

Saving

Logging

IP Scoping

Maintenance

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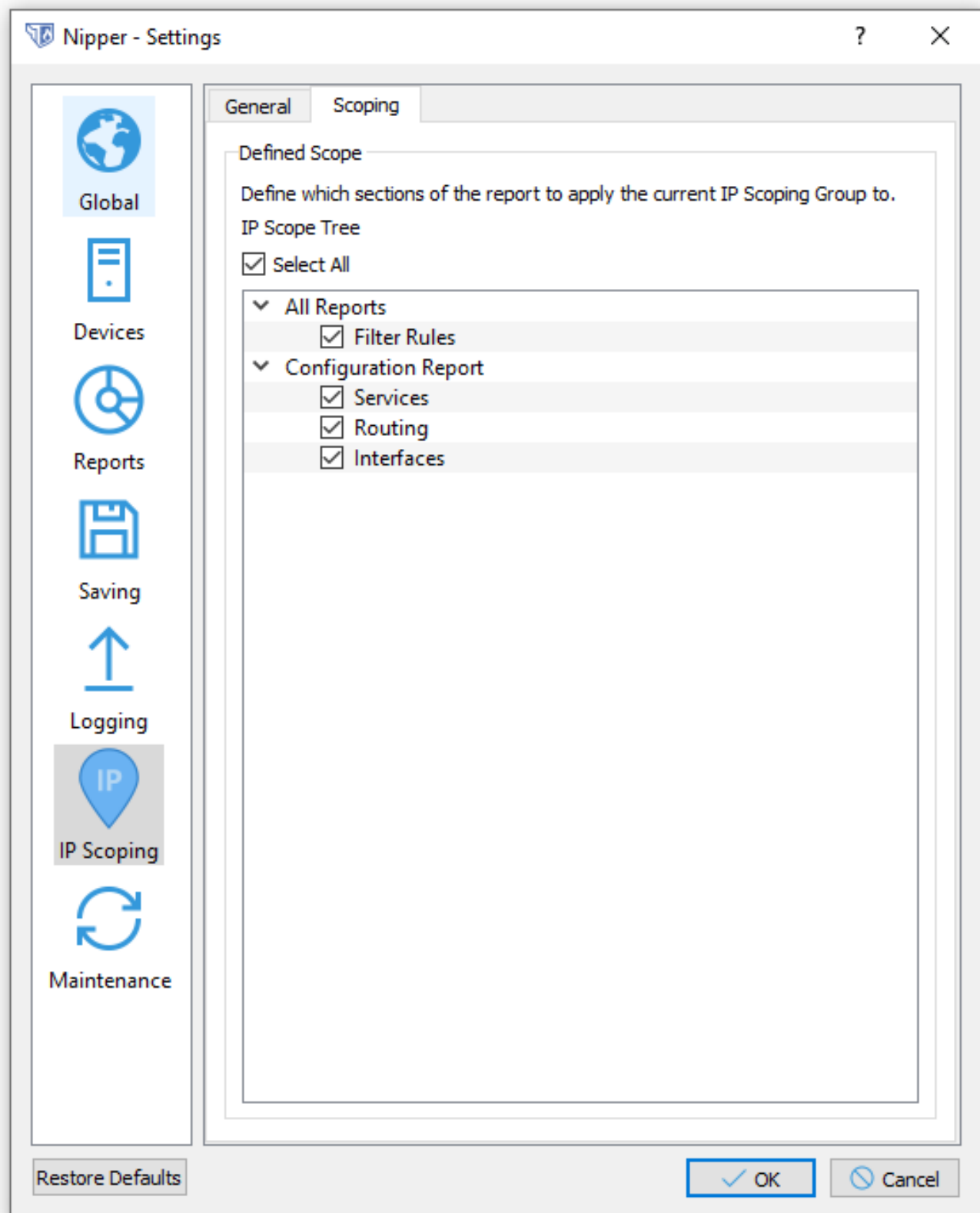
Selecting (or deselecting) a section within this tab will instruct Nipper to apply (or not apply) the current **IP Scoping Group** to that portion of the report, accordingly.

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

1. 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**.

2. Again, simply select the issue and write what you would like to include.

3. 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.

1. 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
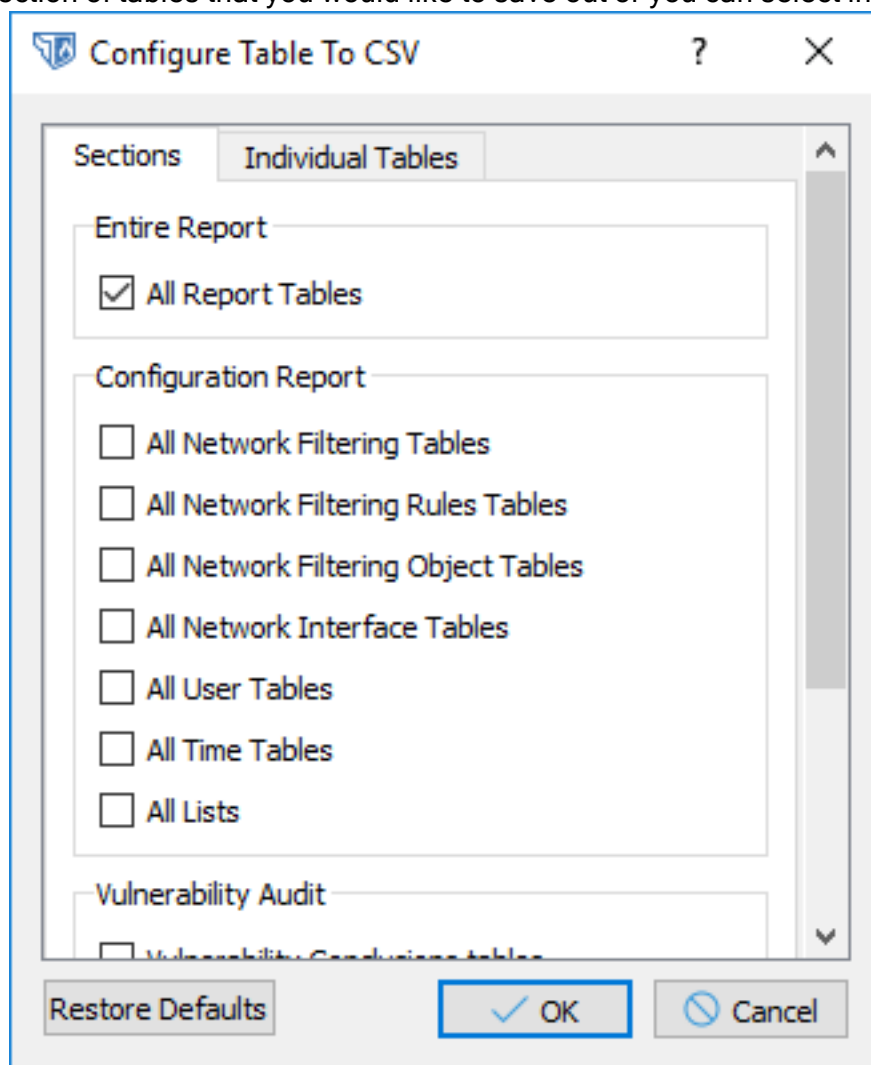
    below).

2. 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:
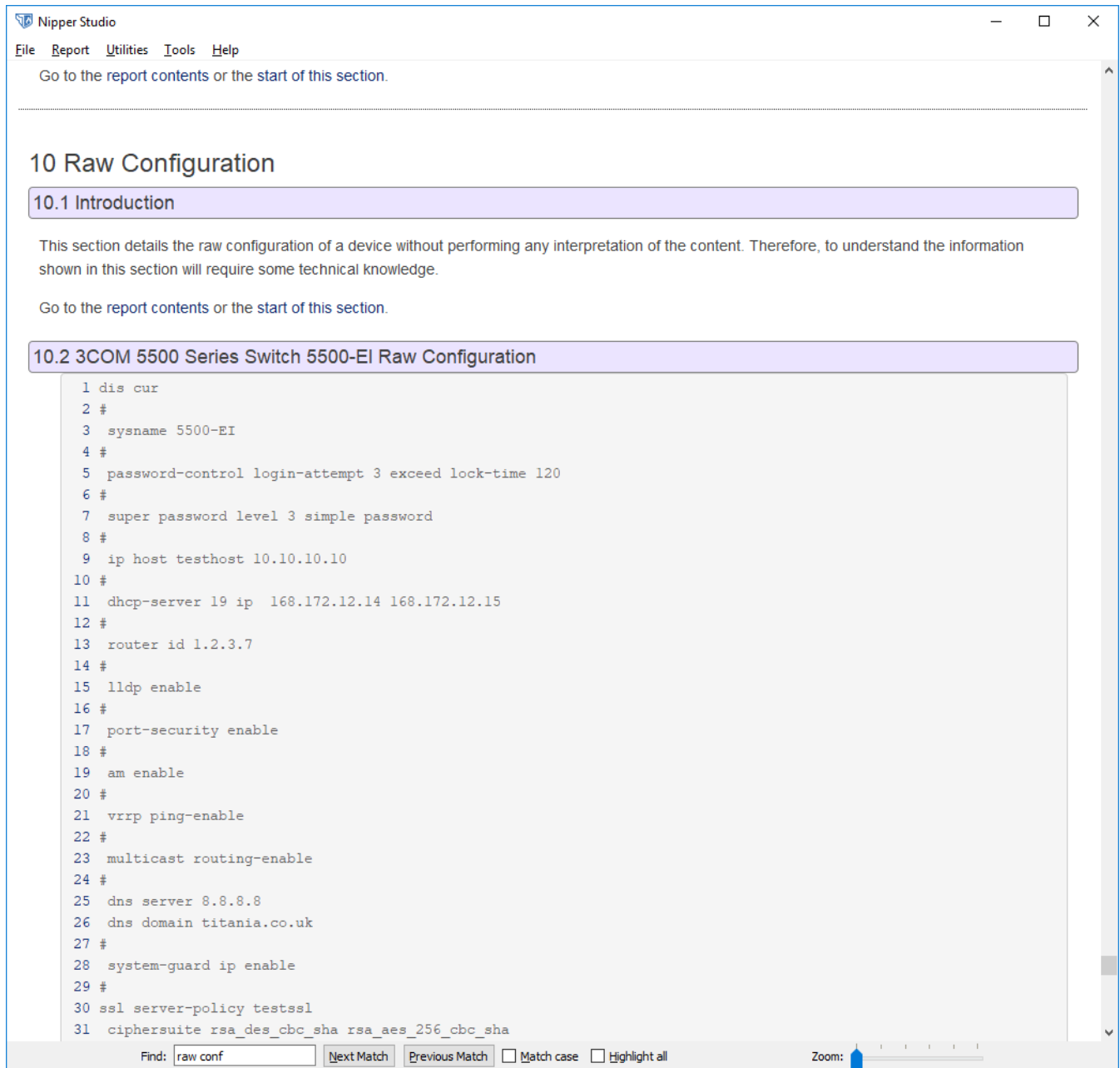
In order to make a comparison, first audit your device using Nipper, selecting either **Security Audit** or **Raw Configuration**, and save the result as an XML file. When you later come to re-audit the report, if you select either **Security Audit** or **Raw Configuration Changes**, you will be asked 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 tabs along the top of the window are: **Overview**, **Options**, **Licensee** and **License**.

The **Overview** tab lists 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 labeled 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 Active** and **Remove** buttons at the base of this license and may note that the **Make Live**button could be 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 Nipper" on page 12 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.

How to update Nipper

We continually enhance the accuracy of our configuration auditing tool, Nipper. Each new release builds the support it provides. Developments include enhanced device support, new plugins, additional features, and bug fixes, as well as updates to the vulnerabilities it detects from the National Vulnerability Database.

This guide provides step-by-step instructions for updating your software to the latest version.

Checking for updates

From the Nipper Home Screen you can see when your last check for updates was run. If this was not recently, you should follow the steps below to find out what version of Nipper you are using and how to access the latest release.

Visit the Support section of our website to find what the latest version of Nipper is and read the release notes for it.

Updating to the latest version from the Nipper Home Screen

You can update your current version of Nipper within the software in a few simple steps:

1. Firstly, open Nipper and locate the **Help** section on the top navigation bar.

2. Clicking **Help** will open the drop-down menu, then select **Check For Updates**.

> ✅ Shortcut: Hit Ctrl + U on your keyboard to open *Check For Updates*

3. You will then be able to see which version of Nipper you are currently running. Select the **Check for Updates** button to run a check against the Titania servers.

4. Next, you we see the release notes with a description of what is new in the latest version of the software.

5. Select **Download & Install** and follow the on-screen instructions to update to the latest version.

Installing the latest version of Nipper from the Titania website

1. Firstly, visit the Log in area on the Titania website and enter the email address and password associated with your account.

2. After logging in, you will be redirected to the Dashboard. Select the Download Area.

3. Inside the Download Area, select **View Download**. This will take you to the latest available installs where you can select the correct file for your operating system.

4. After clicking **Download**, the installer will download. Once this is downloaded, you will be able to install Nipper. For details on how to install Nipper on each OS, visit "Installing Nipper" on page 8

Updating NVD Resources

The National Vulnerability Database (NVD) is a U.S. government repository of data relating to vulnerability management. The National Vulnerability Database files stored within Nipper are updated with each release. However, users who want to have absolutely up-to-the-minute updates can add NVD files manually through Nipper's Resource Manager.

To add an NVD file manually, you will first need to have the file on your machine or device. NVD files can be downloaded from the United States National Institute of Standards and Technology, at the following URL:

- https://static.nvd.nist.gov/feeds/json/cve/1.1/[filename].zip.

For example the file nvdcve-1.1-2022.json is found at:

- https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-2022.json.zip
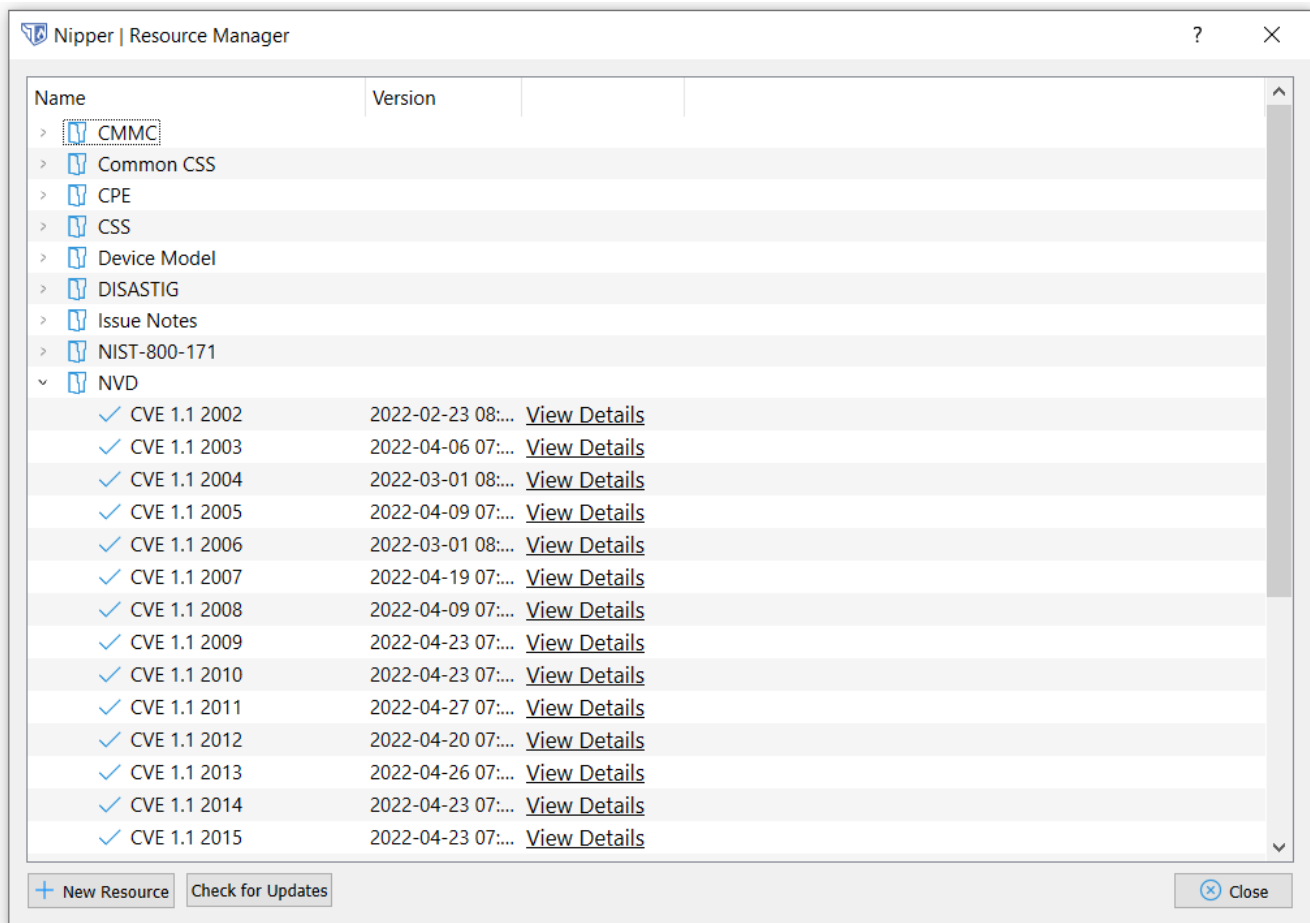
This will download a zip file containing only the NVD file in question.

Alternatively, a list of each NVD can be found here.

1. To add the NVD file to Nipper, open the Resource Manager by clicking on **Manage Resources** in the **Tools** menu. The NVD files currently included are listed in the resource manager in the NVD group.

Name	Version		
> [ ] CMMC			
> [ ] Common CSS			
> [ ] CPE			
> [ ] CSS			
> [ ] Device Model			
> [ ] DISASTIG			
> [ ] Issue Notes			
> [ ] NIST-800-171			
∨ [ ] NVD			
✓ CVE 1.1 2002	2022-02-23 08:...	View Details	
✓ CVE 1.1 2003	2022-04-06 07:...	View Details	
✓ CVE 1.1 2004	2022-03-01 08:...	View Details	
✓ CVE 1.1 2005	2022-04-09 07:...	View Details	
✓ CVE 1.1 2006	2022-03-01 08:...	View Details	
✓ CVE 1.1 2007	2022-04-19 07:...	View Details	
✓ CVE 1.1 2008	2022-04-09 07:...	View Details	
✓ CVE 1.1 2009	2022-04-23 07:...	View Details	
✓ CVE 1.1 2010	2022-04-23 07:...	View Details	
✓ CVE 1.1 2011	2022-04-27 07:...	View Details	
✓ CVE 1.1 2012	2022-04-20 07:...	View Details	
✓ CVE 1.1 2013	2022-04-26 07:...	View Details	
✓ CVE 1.1 2014	2022-04-23 07:...	View Details	
✓ CVE 1.1 2015	2022-04-23 07:...	View Details	

If you are replacing an NVD file, you will first need to remove the old one, as the Resource Manager will not let you add a new file with the same name. Click on **View Details** for the file in question and click **Remove**.

2. To add the new file, click on **New Resource** to open the **Add Resource** wizard.

3. Select the **NVD** resource type and click **Next**.

4. From here, you can select **Add File** or **Add Directory**. Add File will open a file explorer dialog and allow you to select the single NVD file you wish to add to Nipper. **Add Directory** will open a file explorer dialog and allow you to select a folder of NVD files to be added to Nipper.

5. Once you have added the NVD files you require, click **Next** to begin adding these files to Nipper. The end screen should then appear.

6. Click **Finish** to end this process.

Vulnerability Audits run from Nipper will now include your custom NVD files.

Conclusion

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

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