



Titania Nipper User Guide

Software Version: 3.6.0

Last updated: October 28, 2024

© Titania Ltd. 2024. All Rights Reserved

Contents

Titania Nipper User Guide	1
Nipper v3.x User Guide	3
System Requirements	4
Downloading Nipper v3.x	5
Installing Nipper	7
How to update Nipper	9
Adding a license to Nipper	11
Offline Activation Steps	12
Navigating around Nipper	14
Creating your first report with Nipper	16
Saving Your Reports	24
Creating NIST SP 800-53 reports	25
Creating STIG reports	27
Creating PCI DSS 4.0 Reports	30
Creating CIS Benchmark reports	35
Conclusion	38

Nipper v3.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 v3.x 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 3.6.0

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 Ltd., publisher of this work.

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

System Requirements

Below are the basic system requirements needed to operate Nipper:



Operating System: Microsoft Windows 10 or greater

Processor: 1 gigahertz (GHz) or faster with two or more cores on a compatible 64-bit processor or system on a chip (SoC).

Memory: 4 gigabytes (GB) or greater.

Storage: 1 GB or greater available disk space.

Graphics card: Compatible with DirectX 12 or later, with a WDDM 2.0 driver.

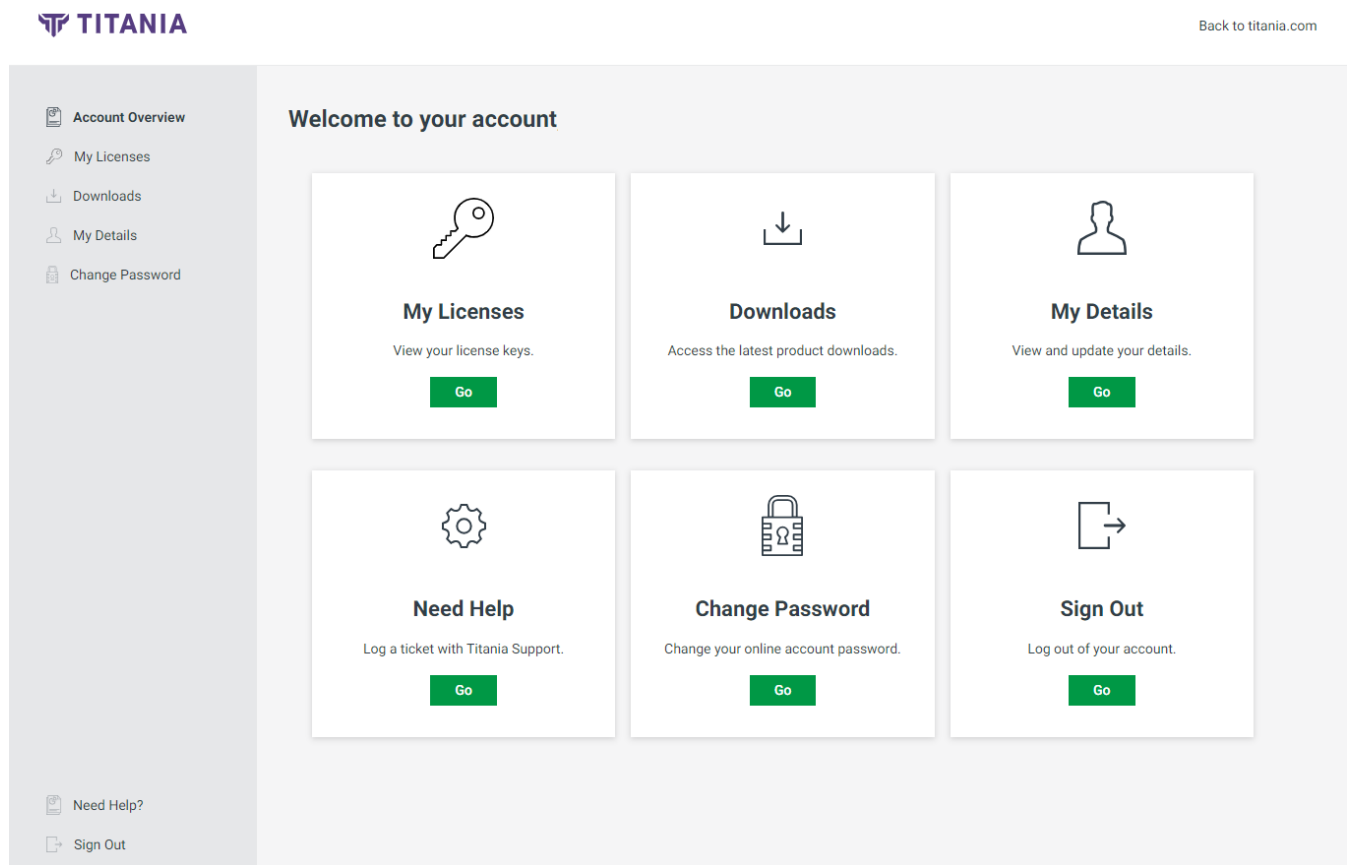
Display: High definition (720p) display, 9" or greater monitor.

Downloading Nipper v3.x

Nipper v3.x can be downloaded on the Windows platform.

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.

- 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 section gives detailed instructions on how to install Nipper on Windows operating systems.



Please note that Nipper v3.0 is currently only supported for Windows operating systems.



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



Note: Nipper v2.x.x and Nipper v3.0 can be installed and run alongside each other on a machine.

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



Note: We installed Nipper on Windows 11 x64 for this explanation. Other versions of Microsoft Windows may be compatible with Nipper v3.0.0 but may have limited functionality.

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; tick the box next to '**I accept the terms in the License Agreement**' and click **Next** 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. When you have chosen where to install Nipper and pressed **Install**, the software will install to your specifications and you will be taken to the final installation screen. To complete, select **Finish**.

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 **Updates** section on the left-hand panel.
2. Next click on **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 will 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.

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 18.04 x64	2.13.2	104.86 MB	Download

- After logging in, you will be redirected to the [Dashboard](#). Select the [Download Area](#).
- Inside the Download Area, select **View Download**. This will take you to the [latest available installs](#) where you can select the correct file.
- 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, visit "Installing Nipper" on page 7

Adding a license to Nipper

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

1. From the Nipper home screen click **Licensing**.
2. When the Manage Licenses screen appears click **Add** to add a new license.
3. After you click **Add**, 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, account.titania.com by logging into your account and then going to **Your account**.

You will need to have registered for this account before accessing it. An email with your registration details will have been sent to you when you purchased the license or you can request an account by visiting account.titania.com and selecting **Request an Account** (license holders only).



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 toggling the required license on or off.

4. Enter the Serial Number and Activation Code details into the relevant boxes and click **Next**.
5. 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**.
6. You will then be asked if you want to activate the license using either Online or Offline modes. The default is Online and will be pre-ticked. Click **Next** to continue.
7. 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. From the Nipper home screen click **Licensing**.
2. When the Manage Licenses screen appears click **Add** to add a new license.
3. After you click **Add**, 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, account.titania.com by logging into your account and then going to **Your account**.

You will need to have registered for this account before accessing it. An email with your registration details will have been sent to you when you purchased the license or you can request an account by visiting account.titania.com and selecting **Request an Account** (license holders only).



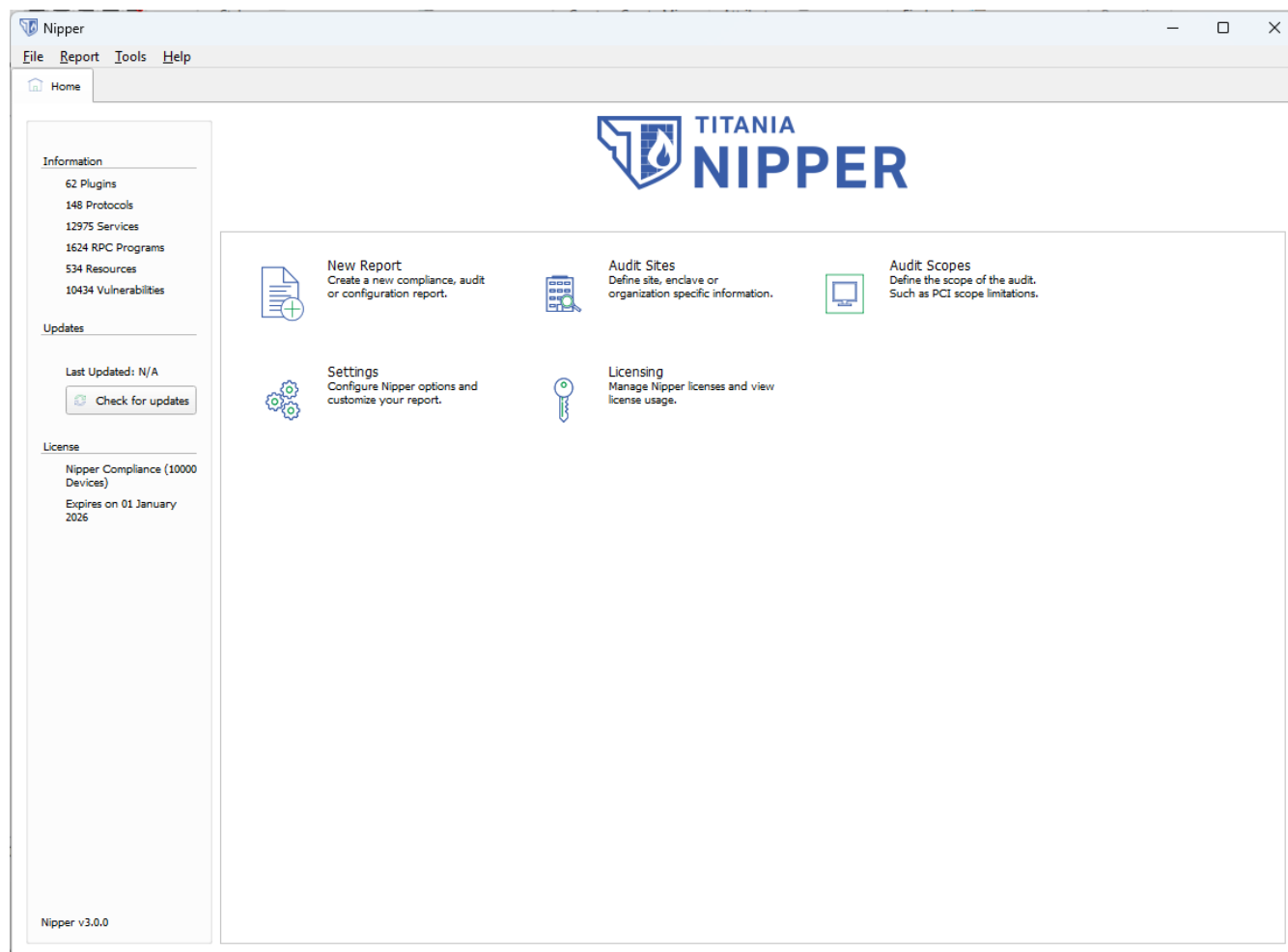
Note: Nipper allows you to add multiple licenses and will set the most recently added license active by default. If you wish to change which license is currently in use this can be amended within **Tools -> Manage Licenses** (or **Ctrl & L**) and toggling the required license on or off.

4. Enter the Serial Number and Activation Code details into the relevant boxes and click **Next**.
5. 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**.
6. You will then be asked if you want to activate the license using either Online or Offline modes. Select **Offline** then click **Next**.
7. 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.
8. Transfer the License Activation Request on to a system that has internet connectivity and go to <https://activate.titania.com/> and upload the Activation request.
9. 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.
10. Click the **Load License Activation Response** button and load the titania-response.nlr file.
11. Click **Next** to complete the license activation process.

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

Navigating around Nipper

This is the homepage:



From the homepage, you have multiple options available for selection.

The Left-Hand Panel displays general Nipper information which is dynamically updated on start-up. You are able to check for any Nipper updates by clicking **Check for updates**. License information is shown at the bottom of the panel.

In the main section:

- **New Report** will allow you to generate a new report within Nipper.
- **Audit Sites** allows you to define site, enclave or organization specific information.
- **Audit Scopes** lets you define the scope of the audit, such as which IP addresses to include/exclude.

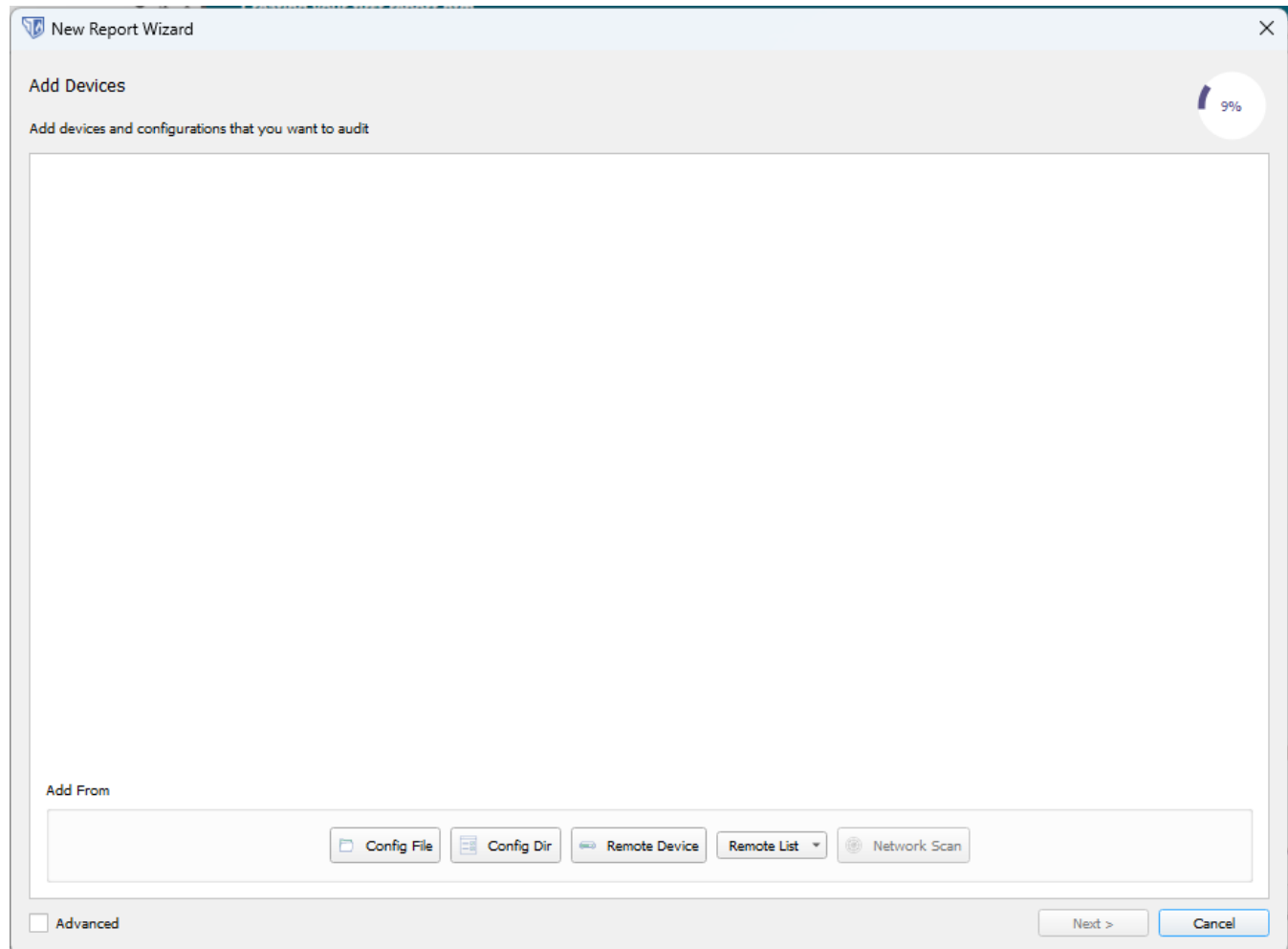
- **Settings** provides configuration options for Nipper, allowing you to tailor the experience to your specific requirements.
- **Licensing** lets you add new licenses and manage existing ones.

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 options:

- **Config File** looks for a single, manually exported device configuration file.
- **Config Dir** looks for a directory containing one or more manually exported device configuration files.

- **Remote Device** will allow you to add the configuration files of supported devices remotely.
- Under Remote List there are three options:
 - **Import from NMAP XML** will enable you to add multiple devices via an XML input.
 - **Import from CSV** will enable you to add multiple devices via a CSV input.
 - **Export to CSV** generates a CSV from the networks that are available in the format that can be re-imported using 'Import from CSV'.

Config File

1. Selecting **Config File** allows you to navigate to the location on your computer where the required configuration file is stored.
2. Once selected, you will be returned to the **Add Devices** screen. Your configuration file will be displayed in the window.



Note: You are able to add multiple device configuration files.

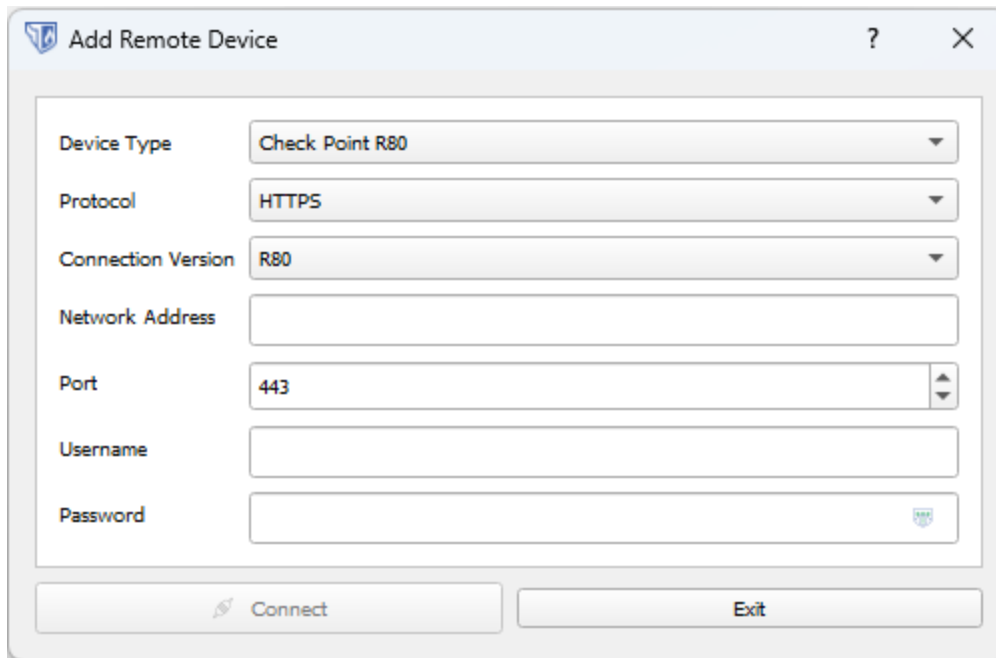
3. Click on **Next** to proceed to the **Select Report(s)** screen.

Config Dir

1. Selecting **Config Dir** allows you to navigate to the location on your computer where the required configuration directory is stored.
2. Once selected, you will be returned to the **Add Devices** screen. All selected configurations will be displayed.
3. Click on **Next** to proceed to the **Select Report(s)** screen.

Remote Device

Selecting **Remote Device** 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 **Connection Version** field can be left as default; this is included for future functionality.

The **Network Address** section requires you to enter the basic information for your device. The **Port** section allows you to enter the port, along with the **username** and **password** required to elevate privilege in order to obtain access to the configuration file.

Remote List

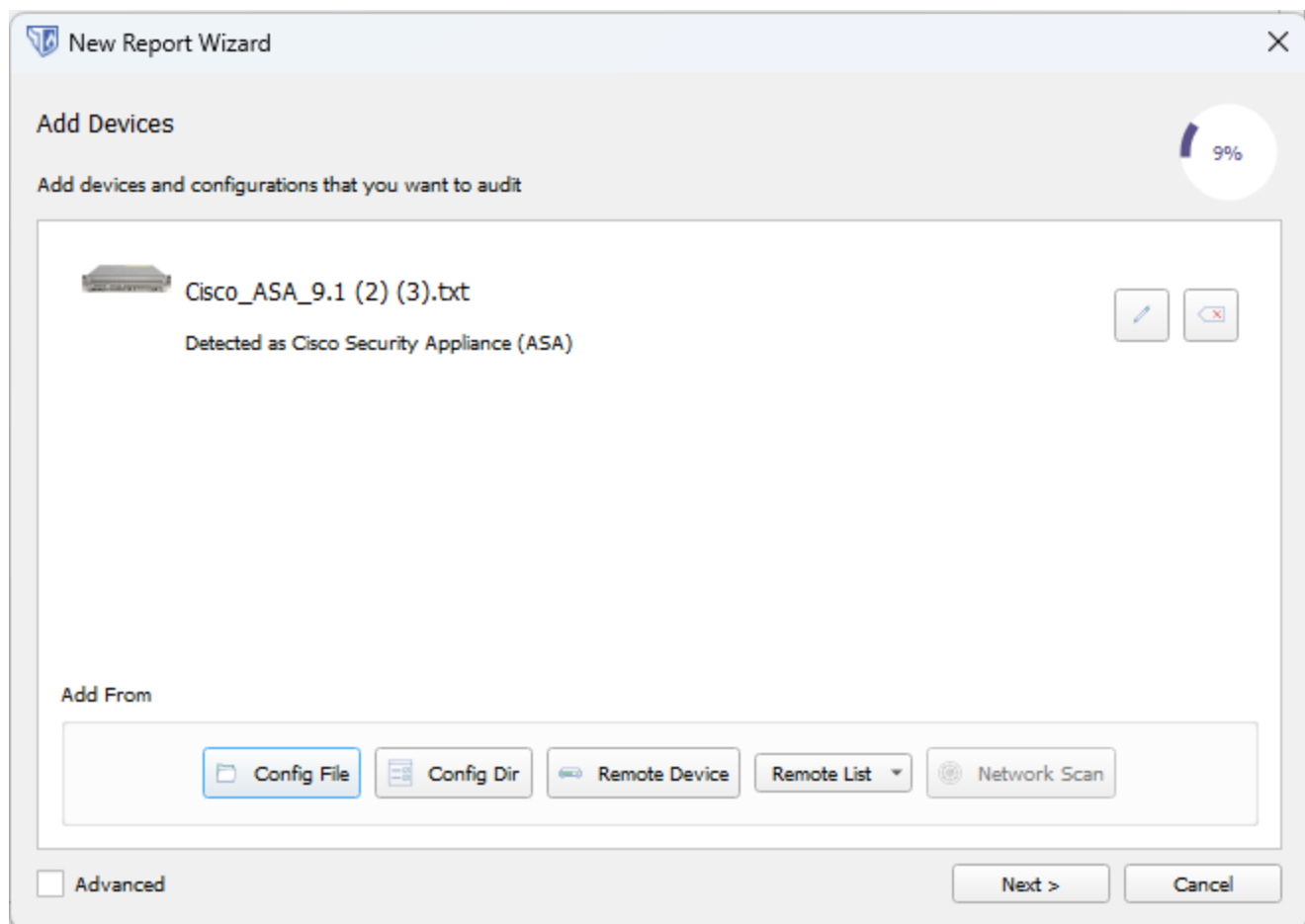
Within **Remote list** there are two available options:

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

Export to CSV generates a CSV file from the available networks in a format that can be re-imported using 'Import from CSV'.

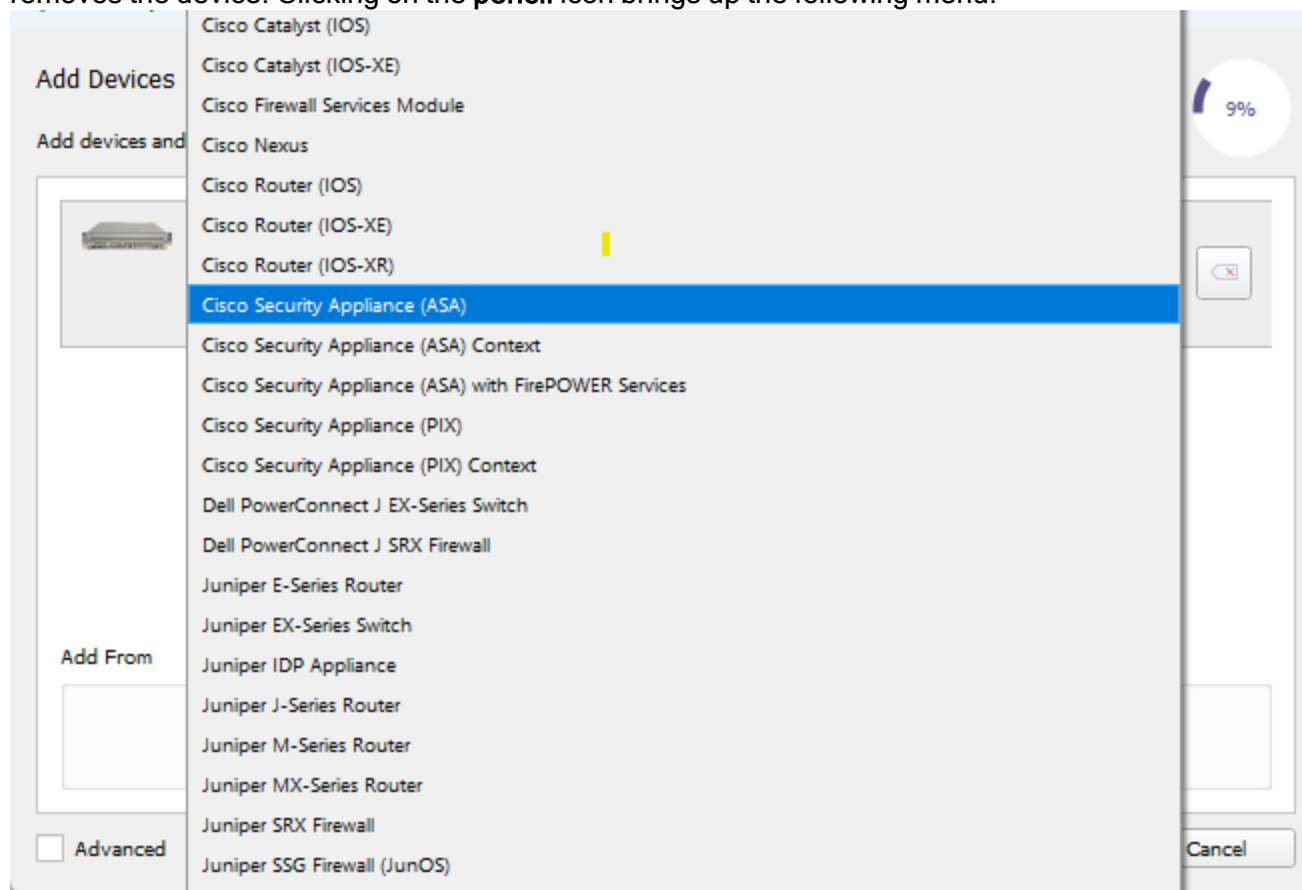
Report options

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:

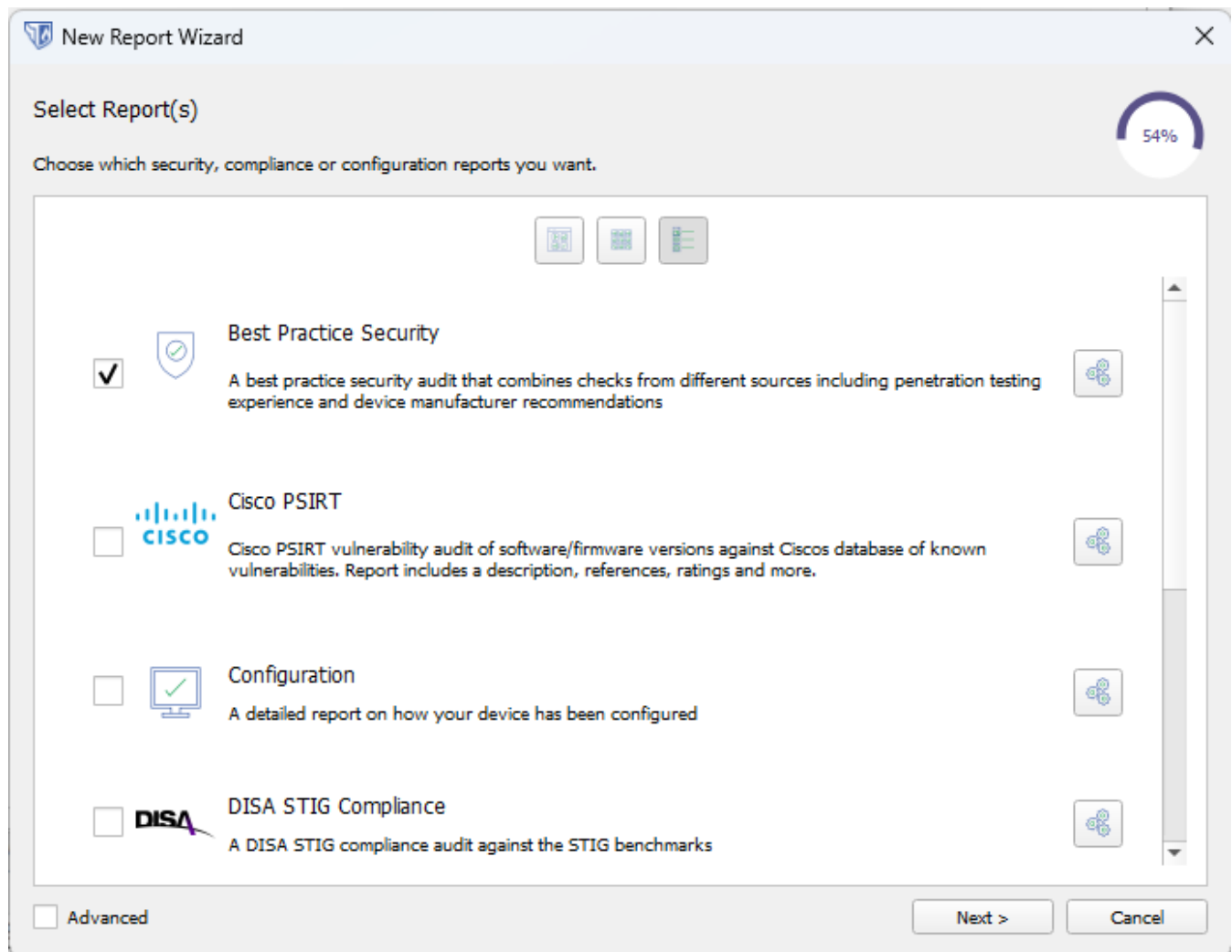


You will see in this case (as is normal) Nipper has automatically detected the device type. The dropdown list that appears allows you to manually set the device type.



Note that, if this is altered from the device type identified by Nipper from the config file, audit findings may not be 100% accurate.

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 **Select Report(s)** 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 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 will allow you to run a comparison against a previous report:

New Report Wizard

Report Comparison (Optional)

72%

Select a previous report to perform a comparison

Note: Before you can perform a comparison to a previous report you first must have saved the report you want to perform a comparison with to a JSON file.

Select the report (below) that you want to perform a comparison to.

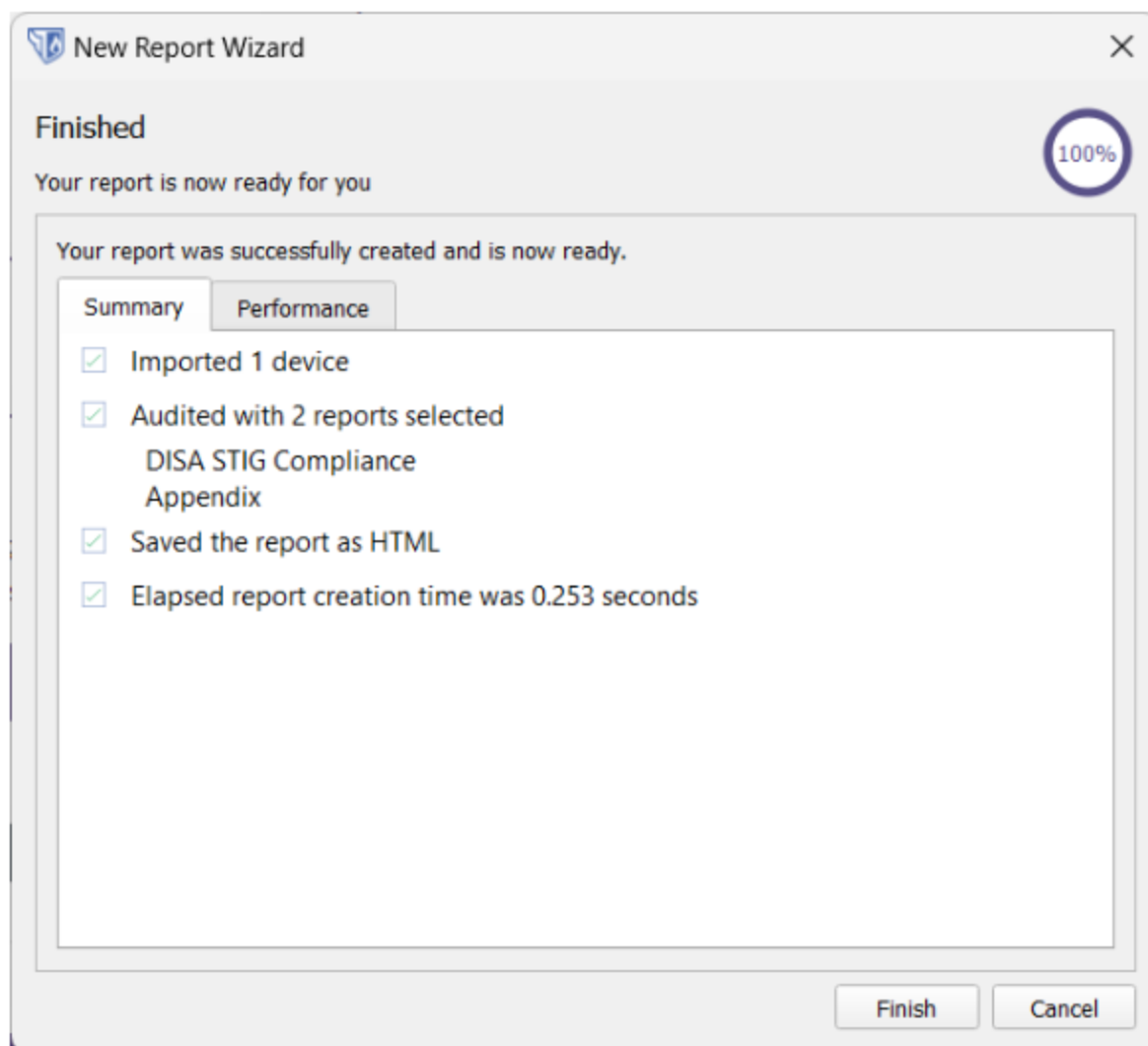
When selecting a previous report the previously audited devices will automatically be matched against the current selected devices. If no devices from the previous report can be automatically matched, or the "Advanced" option is checked, you will be asked to confirm the matching of the devices.

☐ Advanced

Next >

Cancel

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.

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 As**.

You can save out all or some of the tables in the Nipper report.

1. Go to the **Save As** 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
2. Check the boxes you want to save and then simply click **OK** and save the files.



Note: There are additional options available for STIG reports allowing XCCDF exports for use with the DISA STIG Viewer tool.

Creating NIST SP 800-53 reports

The National Institute of Standards and Technology's (NIST) Special Publication 800-53 comprises operational, technical, and management security controls that are designed to secure and enhance the resilience of US government networks and federal IT systems. Titania Nipper can automate the compliance assessment of up to 49 of the NIST SP 800-53 controls and control enhancements, related to devices, across the following 8 control families:

- Access Control (AC)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification & Authentication (IA)
- Maintenance (MA)
- System & Communications Protection (SC)
- System & Information Integrity (SI)

For further information on the NIST SP 800-53 Titania mapping, see the guide <https://www.titania.com/resources/compliance/nist-800-53-mapping-document>

Note: The NIST SP 800-53 report is available as part of the Nipper Compliance suite of reports. For more information, contact your Solutions Advisor, or sales@titania.com.

The report provides a risk based evidentiary Pass and Fail assessment, mapped to STIGs, based on the CCI references. Findings shown within the report are based on the STIG risk-based categorization of CAT I, CAT II and CAT III and sorted by severity, allowing you to focus on the most critical vulnerabilities first.

Creating the NIST SP 800-53 Report

1. To begin, go to **File, New Report**.
2. Add one or more devices to the audit using **Config File**, **Config Dir**, **Remote Device** or **Remote List** methods.
3. On the Reporting Options screen, select the **NIST 800-53** report check box. If this is not available, your active license does not support the NIST SP 800-53 feature.
4. On the Report Comparison screen, if you wish to perform a comparison with a previously generated report, select the report here.

5. Begin the report generation by pressing the **Next** button.
6. After a short time generating, your report is then available.

Viewing the NIST 800-53 report

The NIST 800-53 report will be displayed in HTML format by default, within the Nipper report Browser. From here, you can scroll through the report, navigate to key sections via the navigation window shown to the right of the screen and search for key text or phrases within the report. You also have the option to save the report in several formats.

Creating STIG reports

[Security Technical Implementation Guides](#) (STIGs) are configuration standards developed by the Defence Information Systems Agency (DISA). They are designed to make device hardware and software as secure as possible, safeguarding the Department of Defence (DoD) IT network and systems.

Compliance with STIGs is a requirement for DoD agencies, or any organization that is a part of the DoD information networks (DoDIN). This includes defence contractors that connect to the DoD network or system.

Note: The STIG reports are available as part of the Nipper Compliance suite of reports. For more information, contact your Solutions Advisor, or sales@titania.com.

The reports provide a risk prioritized evidentiary Pass and Fail assessment report, for both Device specific and generic NDM, RTR, VPN, IDPS, Firewall and L2S STIGs (where applicable). Findings shown within the report use the STIG risk-based categorization of CAT I, CAT II and CAT III and sorted by severity, allowing focus on the most critical vulnerabilities first.

Creating the STIG Report

1. To begin, go to **File, New Report**.
2. Add one or more devices to the audit using **Config File, Config Dir, Remote Device** or **Remote List** methods.
3. On the Reporting Options screen, select the **DISA STIG Compliance** report check box. If this is not available, your active license does not support the STIG compliance feature.
4. On the Report Comparison screen, if you wish to perform a comparison with a previously generated report, select the report here.
5. Begin the report generation by pressing the **Next** button.
6. After a short time generating, your report is then available.

Viewing the STIG report

The STIG report will be displayed in HTML format by default, within the Nipper report Browser. From here, you can scroll through the report, navigate to key sections via the navigation window shown to the right of the screen and search for key text or phrases within the report. You also have the option to save the report in several formats.

STIG Report settings

Within Nipper, there are report-specific settings allowing you to tailor reports to your requirements.

1. From the Nipper Home Screen, select **Settings**.
2. On the Settings screen choose **Reports**.
3. From the Reports screen options, select **DISA STIG Compliance**.

You will be presented with several configuration options for your STIG reports:

Audit

Automatically Select Benchmarks. Benchmarks selected for auditing a device are unique to that device and its configuration. By selecting this option, Nipper will automatically use the benchmarks configured for the selected device from within the site's settings.

Default Profile sets the default benchmark profile to be used for the audits.

Report Devices that could not be audited will return a CAT I finding requiring investigation for any devices which cannot be audited.

Interactive Auditing will cause prompts to appear for any compliance issues that could not be automated. Note, the core interactive audit setting will override any preference here.

Add Device Configuration When Asking Interactive Questions will add the device configuration to the interactive question that asks about a specific device.

Compact Interactive Mode will prompt Nipper to show all questions for a specific benchmark at the same time, in a compact list.

DoD or DoD Approved CA (Certificate Authority) allows you to enter host addresses that are DoD or DoD Approved CAs.

Deny MSDP (Multicast Source Discovery Protocol) Peer Sources allows you to enter any addresses here that should be blocked in multicast MSDP peer sources.

Deny MSDP Peer Destinations allows you to enter addresses that should be blocked in multicast MSDP peer destinations.

Reporting

Order Findings By lets you define the order in which you want the findings shown.

Include CCI References will include CCI references within the STIG report.

Summarize Each Benchmark will show a summary of the findings for each benchmark, prior to the detailing findings being displayed for each one.

Include Rule ID will include the rule ID within the summary table.

Include CCI (ident) will include the CCI within the summary table.

Heatmaps

Include Heatmap In Summary will include a ratings heatmap within the report summary section.

Include Heatmap Section includes a section for a heatmap within the report.

Include Passed / NA Findings in the Heatmap will include any passes or N/A results within the heatmap.

Heatmap Table Title allows you to specify a name for the heatmap to be shown in the report.

Horizontal Heatmap Rating System allows you to specify which rating system to use as the default within the heatmap.

Heatmap Horizontal Axis allows you to specify which rating data should be used for the horizontal axis.

Vertical Heatmap Rating System allows you to specify which rating system to use as the default within the heatmap.

Heatmap Vertical Axis allows you to specify which rating data should be used for the vertical axis.

Creating PCI DSS 4.0 Reports

The PCI DSS (Payment Card Industry Data Security Standard) 4.0 comprises security requirements that are designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Titania Nipper can automate the compliance assessment of a number of the PCI DSS 4.0 Security Requirements and testing procedures. For further information on the PCI DSS 4.0 Titania mapping, see the guide [here](#).

The Nipper Compliance suite includes a PCI DSS 4.0 report module which provides a risk prioritized evidentiary Pass and Fail assessment report of compliance with specified PCI DSS 4.0 security requirements. Findings shown within the report and sorted by risk severity, allowing focus on the most critical vulnerabilities first. Each requirement is given a status to indicate the outcome of the analysis for that audit. Three statuses are returned within the report; **'Pass'**, **'Fail'**, **'Investigate'** or **'N/A'**.

- **Pass** - The check has passed all its required elements. For example, If the check states that the Telnet service should be disabled, and it is, then it will be marked as having passed. Alternatively, a 'Pass' status will be shown if a check is determined not applicable to a device. For example, if the test requires HTTP to be disabled, but the device does not support HTTP, then it will be not applicable and therefore marked as having passed.
- **Fail** - The check has failed to meet some or all the requirements. For example, the check may specify that support for only SSH protocol version 2 must be configured, yet the test finds version 1. In this instance, the check would be marked as having failed.
- **Investigate** - The check requires further investigation to determine its status. For example, the test may require port security to be enabled on a network switch port or physically secured. If the check is unable to verify this through the device configuration provided, then investigation of the physical security would need to be carried out. In this case, the check would be marked as requiring further investigation.
- **N/A** - The check is not applicable to the device being audited. For example, where a security control is testing functionality that is not available on the device.

The Risk severity returned will be **Critical**, **High**, **Medium**, **Low** or **No Rating Available**.

- **Critical** - These findings can pose a very significant security risk. The findings that have a critical impact are typically those that would allow an attacker to gain full administrative access

to the device.

- **High** - These findings pose a significant risk to security but have some limitations on the extent to which they can be abused. User level access to a device and a DoS vulnerability in a critical service would fall into this category.
- **Medium** - These findings have significant limitations on the direct impact they can cause. Typically, these findings would include significant information leakage findings, less significant DoS findings or those that provide significantly limited access.
- **Low** - These findings represent a low-level security risk. A typical finding would involve information leakage that could be useful to an attacker, such as a list of users or version details.
- **No Rating Available** - The findings are returned when an additional report is used to determine the outcome of the Check For example, where a configuration report needs to be examined by an Auditor to determine a setting, the report will be included in the report, but Nipper will not be able to determine a rating.

Generating the PCI DSS 4.0 Compliance Report:

1. From the home screen, select the **New Report** option.
2. On the following pop-up screen, you will be prompted to select any devices and configurations that you wish to run the audit against. Select the configuration file(s), directories, or remote devices that the report is to be generated for.
3. Click **Next** to progress to the next screen.
4. From the 'Select Report(s)' screen, ensure the PCI DSS 4.0 option is chosen and click **Next** to proceed.
5. Nipper provides the ability to compare the report being run with one previously generated. If this option is required, navigate to the location of the report to be compared and click **Open** to return to this screen. Clicking on **Next** will progress to the final screen in the report wizard.
6. Depending on the device being audited, Nipper will display options prior to generating the report. These settings allow you to specify the status of specific features/confirm the setup of the device which help Nipper determine the outcome of any related checks used in the audit.

7. A summary 'Finished' screen is displayed, confirming number of devices imported along with report selection, save details and elapsed creation time. Clicking on **Finish** will take you to the generated report.

Viewing the PCI DSS 4.0 Compliance report

The PCI DSS 4.0 report will be displayed in HTML format by default, within the Nipper Report Browser. From here, the user can scroll through the report, navigate to key sections via the navigation window shown to the right of the screen and search for key text or phrases within the report. The user also has the option to save the report in several formats.

The report is broken down into several sections:

Summary

This section lists the device(s) audited and provides a high-level visual summary of the findings, broken down by status. Each control is then detailed within tables based on status (Failures first, followed by Passes and then Investigates). Within the table itself, each finding is given a STIG Risk rating (CAT I, CAT II, CAT III) and the table is prioritized based on these (most severe to least).

Status	Total
Pass	5
Fail	6
Investigate	22
N/A	5

Table 4: Overall PCI DSS 4.0 Assessment summary findings table

	Informational	Low	Medium	High	Critical
Trivial	0	0	0	0	1
Easy	0	0	1	0	2
Moderate	0	0	1	0	4
Challenging	0	1	0	0	2

Table 5: Nipper "Impact" to Nipper "Ease"

Title	Testing Procedure	Status	Devices	Risk
Testing Procedure 2.2.7.a	2.2.7.a	FAIL	Example-Cisco-ASA	Critical
Testing Procedure 8.3.2.a	8.3.2.a	FAIL	Example-Cisco-ASA	Critical
Testing Procedure 2.2.7.c	2.2.7.c	FAIL	Example-Cisco-ASA	Medium
Testing Procedure 2.2.1.c	2.2.1.c	FAIL	Example-Cisco-ASA	No Rating Available

Contents

Clickable list of report contents.

	Contents
Your Report	
Report Conventions	
Compliance Status	
Nipper Ratings	
Network Filtering Actions	
Network Filter Objects	
PCI DSS 4.0 Assessment	
Introduction	
Requirement 1: Install and Maintain Network Security Controls	
Requirement 2: Apply Secure Configurations to All System Components	
Requirement 8: Identify Users and Authenticate Access to System Components	
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	

Your Report

Section providing information around conventions used, compliance statuses and STIG Ratings.

Main Report Body

The main report is made up of the relevant requirement families - for example, Requirement 1: Install and Maintain Network Security Controls). Within these, individual requirements that can be audited in Nipper are detailed, under the following headings:

- **Defined Approach Requirements and Defined Approach Testing Procedures** - describes the method for implementing and validating PCI DSS using the requirements and testing procedures defined in the standard.
- **Affected Devices** - Tabular view of the device audited, together with the specific, defined testing requirements carried out and the overall result and rating.
- **Findings** - Tabular view of the check(s) carried out, with description(s), finding(s) and result(s) for each one. Where the requirement is assessed using an additional audit (e.g. configuration report) the report includes a link to the specific section.

Appendix

Glossary providing details of Protocols, IP Options, Services, Logging Severity Level, Common Time Zones, and Abbreviations used in the report.

Saving the report

All reports within Nipper can be saved in several formats:

- ASCII Text
- HTML
- JSON
- LaTeX
- Table to CSV, Excel, JSON, SQL, XML
- XML

For more information on saving Nipper reports, please see "Saving Your Reports " on page 24.

Creating CIS Benchmark reports

The CIS Benchmarks are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks. Mapped to the CIS Critical Security Controls (CIS Controls), the CIS Benchmarks elevate the security defenses for network devices.

The CIS reports provide a risk prioritized evidentiary Pass and Fail assessment report, against device specific benchmarks.

Creating the CIS Report

1. To begin, go to **File, New Report**.
2. Add one or more devices to the audit using **Config File, Config Dir, Remote Device** or **Remote List** methods.
3. On the Reporting Options screen, select the **CIS** report check box.
4. On the Report Comparison screen, if you wish to perform a comparison with a previously generated report, select the report here.
5. Begin the report generation by pressing the **Next** button.
6. After a short time generating, your report is then available.

Viewing the CIS Benchmark report

The CIS report will be displayed in HTML format by default, within the report browser. From here, you can scroll through the report, navigate to key sections via the navigation window shown to the right of the screen and search for key text or phrases within the report. You also have the option to save the report in several formats.

The CIS report provides a risk prioritized evidentiary Pass and Fail assessment report of compliance against the selected CIS Benchmark. Findings shown within the report and sorted by risk severity, allowing focus on the most critical vulnerabilities first. Each requirement is given a status to indicate the outcome of the analysis for that audit. Three statuses are returned within the report; '**Pass**', '**Fail**', '**Investigate**' or '**N/A**'.

- **Pass** - The check has passed all its required elements. For example, If the check states that the Telnet service should be disabled, and it is, then it will be marked as having passed.
Alternatively, a 'Pass' status will be shown if a check is determined not applicable to a device. For example, if the test requires HTTP to be disabled, but the device does not support HTTP, then it will be not applicable and therefore marked as having passed.

- **Fail** - The check has failed to meet some or all the requirements. For example, the check may specify that support for only SSH protocol version 2 must be configured, yet the test finds version 1. In this instance, the check would be marked as having failed.
- **Investigate** - The check requires further investigation to determine its status. For example, the test may require port security to be enabled on a network switch port or physically secured. If the check is unable to verify this through the device configuration provided, then investigation of the physical security would need to be carried out. In this case, the check would be marked as requiring further investigation.
- **N/A** - The check is not applicable to the device being audited. For example, where a security control is testing functionality that is not available on the device.

The Risk severity returned will be **Critical, High, Medium, Low** or **No Rating Available**.

- **Critical** - These findings can pose a very significant security risk. The findings that have a critical impact are typically those that would allow an attacker to gain full administrative access to the device.
- **High** - These findings pose a significant risk to security but have some limitations on the extent to which they can be abused. User level access to a device and a DoS vulnerability in a critical service would fall into this category.
- **Medium** - These findings have significant limitations on the direct impact they can cause. Typically, these findings would include significant information leakage findings, less significant DoS findings or those that provide significantly limited access.
- **Low** - These findings represent a low-level security risk. A typical finding would involve information leakage that could be useful to an attacker, such as a list of users or version details.
- **No Rating Available** - The findings are returned when an additional report is used to determine the outcome of the Check For example, where a configuration report needs to be examined by an Auditor to determine a setting, the report will be included in the report, but Nipper will not be able to determine a rating.

Saving the report

All reports within can be saved in several formats:

- ASCII Text
- HTML
- JSON
- LaTeX
- Table to CSV, Excel, JSON, SQL, XML
- XML

For more information on saving reports, please see "Saving Your Reports " on page 24.

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