NIPPER OmniSight
BY TITANIA

Nipper OmniSight Standalone Documentation

v4.0.0

[DOCUMENT CLASSIFICATION: CONFIDENTIAL]

Contents

1. Welcome to Nipper OmniSight

Welcome to the Nipper OmniSight Documentation.

This guide is designed to help customers install, set up, and run Nipper OmniSight successfully.

While Titania makes every effort to ensure the accuracy and relevance of the information in this guide, customers are encouraged to contact Titania Support if further assistance is required.

2. Getting Started with Nipper OmniSight

2.1 Purpose of this Guide

This document provides step-by-step guidance for administrators responsible for installing and managing Nipper OmniSight in a virtualized environment.

3. Administrator Guide

3.1 Setup and Installation

3.1.1 Recommended System Specifications

To ensure optimal performance and stability, Nipper OmniSight should be deployed using the following minimum hardware specifications:

RAM	Processor	Storage
16 GB	4 Core	300 GB

Recommended hardware specifications:

RAM	Processor	Storage
32 GB	8 Core	300 GB

Important:

Running Nipper OmniSight below the recommended specifications may result in:

- Installation issues
- Reduced performance
- Slower processing times

For the best experience, always adhere to the minimum system requirements.

3.1.2 Provided by Titania

- Base OVA - Including Nipper Resilience installer file: nipper-omnisight-<version>.ova
- Activation Code

Once these are received, save in a directory as they will be needed later.

3.1.4 Initial Set Up

Nipper OmniSight is distributed as an OVA file: **nipper-omnisight-<version>.ova**

Important Notes:

- Do not rename or modify any Titania-provided files unless explicitly instructed to do so. Changing filenames can cause installation failures.
- The installation has been tested on VMWare Workstation Pro using an OVA image, if you are using a hypervisor using a different disk format, please refer to the following article.

3.1.5 Importing the Virtual Machine

Follow the steps below to import and configure the Nipper OmniSight virtual machine.

Step 1: Import the OVA File

1 Open ESXi Host Client management console
2 From the top menu, select "**Create/Register VM**"
3 On the Select Creation Type page choose "**Deploy Virtual Machine from OVF or OVA**" Click "**Next**"
4 Enter a name for your new VM
5 Click to browse for the OVA image or drag & drop it to the import box. Click "**Next**"
6 Choose / Confirm the storage location for the new VM. Click "**Next**"
7 Confirm Deployment Options:
   - Network Mappings – Bridged is recommended, NAT is also supported
   - Disk provisioning – Thick / Thin, as preferred
   - Auto Power On – as preferred

Click "**Next**"

8 Verify selections & click "**Finish**" (Note warning about not refreshing browser)
9 Watch for import completion in the Recent Tasks panel.

Step 2: Configure Virtual Machine Settings

Once the import is complete, the VM is configured with the following default settings, please adjust to your hardware and network requirements as necessary:

- **Memory:** 32 GB
- **Processors:** 8
- **Hard Disk:** 300 GB
- **Network Adaptor:**
  - Recommend set to **Bridged**
  - Enable **Replicate physical network connection state**
  - This configuration allows SSH access to the VM

Step 3: Power On the Virtual Machine (if auto power on not selected during import)

Click **Power on this Virtual Machine.**

Allow several minutes for the VM to fully boot.

3.2 First Login and Installation

Step 1: Log In

Once the VM has booted, click the Console menu to access the CLI.

Log in using the default credentials:

Username: titania

Password: FradNik7

You will be prompted to change the password immediately after logging in. Follow the prompts to enter the default password and create new password. The system will then display the welcome message. This includes details of the network interface card required in the next step.

Optional step: Configuring a Static IP Address

To configure a static IP address for the host Network Interface Card (NIC) not the docker instance, run the following command:

sudo set-static-ip

Follow the on-screen prompts to complete the configuration.

Step 2: Locate the Installer

Navigate to the Nipper OmniSight installation directory by entering the following command:

cd /opt/app/nipper-omnisight

Step 3: Run the Installer

Start the installation by running:

sudo ./install.sh

Step 4: Respond to Installation Prompts

During installation, you will be asked several questions:

1 **Extend Logical Volume (LV):**
- Prompt: *"Do you want to extend the LV to use all remaining free space?"*
- Select: Y

2 **Host Name:**
- Accept the default value.
- Press: Enter

3 Enable 2FA:
- Prompt: *"Enable Two-Factor Authentication (2FA)"*
- If you select Y, you will need a device that has a 2FA app

4 Standalone or Integrated:
Prompt: *"Are you using an external configuration storage e.g. CMDB or Git Repository? [y/n]"*
- Select N if you are Standalone
- Select Y if you are looking to integrate with an external repository

5 **Number of Sensors:**
- Accept the default value of **5**
- Press: Enter

3.3. Configuring SSL

3.3.1 SSL setup

Nipper OmniSight includes a default self-signed certificate if no certificate is provided at first startup. This certificate is generated for the hostname defined in HOST_NAME within /opt/app/nipper-omnisight/.conf. The corresponding Root CA (RootCA.crt) is stored in /opt/app/nipper-omnisight/docker/provisioning/ssl/ca/ and must be trusted by any browser accessing the system.

Self-signed certificates cannot be generated for IP addresses using this automatic process. If HOST_NAME is an IP address, please follow the manual self-signed certificate instructions in 3.3.3.

For production environments, Titania recommends using certificates issued by your organisation's PKI rather than the default self-signed certificate.

If you plan to use your own SSL certificates, configure them before starting Nipper OmniSight for the first time. If the system is already running, ensure it is stopped before making SSL changes.

3.3.2 Using Certificates from Your Organisation's PKI

If your organisation has a PKI, you can supply your own SSL certificate signed by your internal CA. Place the required files in the following locations:

File name	File location	File description
public.crt	/opt/app/nipper-omnisight/docker/provisioning/ssl/	Public certificate with SANs for all hostnames/IPs used to access the system
private.key	/opt/app/nipper-omnisight/docker/provisioning/ssl/	Private key matching public.crt
dhparam.pem	/opt/app/nipper-omnisight/docker/provisioning/ssl/	Diffie-Hellman parameters
RootCA.crt	/opt/app/nipper-omnisight/docker/provisioning/ssl/ca/	CA certificate that public.crt chains to
RootCA.pem	/opt/app/nipper-omnisight/docker/provisioning/ssl/ca/	Copy of RootCA.crt in .pem format
CA distinguished name hash}.0	/opt/app/nipper-omnisight/docker/provisioning/ssl/ca/	Symlink created using the CA's distinguished name hash

Most browsers will already trust your organisation's CA. If not, ensure the CA used to sign public.crt is trusted.

3.3.3 Generating Your Own Self-Signed Certificate

- If you need to generate your own self-signed certificate, follow the steps below. Replace the placeholder values (such as country, organisation, and SAN entries) with details appropriate for your environment.
  Navigate to the SSL directory
  cd /opt/app/nipper-omnisight/docker/provisioning/ssl/
- Generate the Root CA private key (minimum 2048-bit recommended):
  openssl genrsa -out ca/RootCA.key 2048
- Create the Root CA certificate, supplying your chosen country and common name:
  openssl req -x509 -new -nodes -key ca/RootCA.key -sha256 -subj "/C={Country}/CN={Common Name}" -days 1024 -out ca/RootCA.crt
- Copy the CA Certificate to the required PEM format:
  cp ca/RootCA.crt ca/RootCA.pem
- Create the distinguished-name hash symlink required by the system:
  syslog_ng_link_name=$(echo $(openssl x509 -noout -hash -in ca/RootCA.crt).0)
  ln -s ca/RootCA.pem ca/${syslog_ng_link_name}
- Generate the private key for the server certificate:
  openssl genrsa -out private.key
- Create a certificate signing request (CSR), supplying your organisation details and SAN entries for all hostnames/IPs the certificate should cover

openssl req -new -sha256 -key private.key -subj "/C={Country}/ST={State}/
L={Locality}/O={Organisation}/CN={Common name}" -reqexts SAN -config <(cat /etc/ pki/tls/openssl.cnf
<(printf "\n[SAN]\n{SAN Content}")) -out cert.csr

- Example SAN content
  subjectAltName=DNS:tes-at-my-org,DNS:alt-host-name,IP:10.50.10.123
- Generate the server certificate using the CSR and Root CA
  openssl openssl x509 -req -in cert.csr -CA ca/RootCA.crt -CAkey ca/RootCA.key - CAcreateserial -days
  1024 -sha256 -extfile <(printf "authorityKeyIdentifier=keyid,issuer\nbasicConstraints=CA:FALSE\nkeyUsage
  = digitalSignature,nonRepudiation,keyEncipherment, dataEncipherment\n{SAN Content}") -out public.crt
- Generate the Diffie-Hellman parameters (minimum 2048-bit recommended):
  openssl dhparam -out dhparam.pem 2048

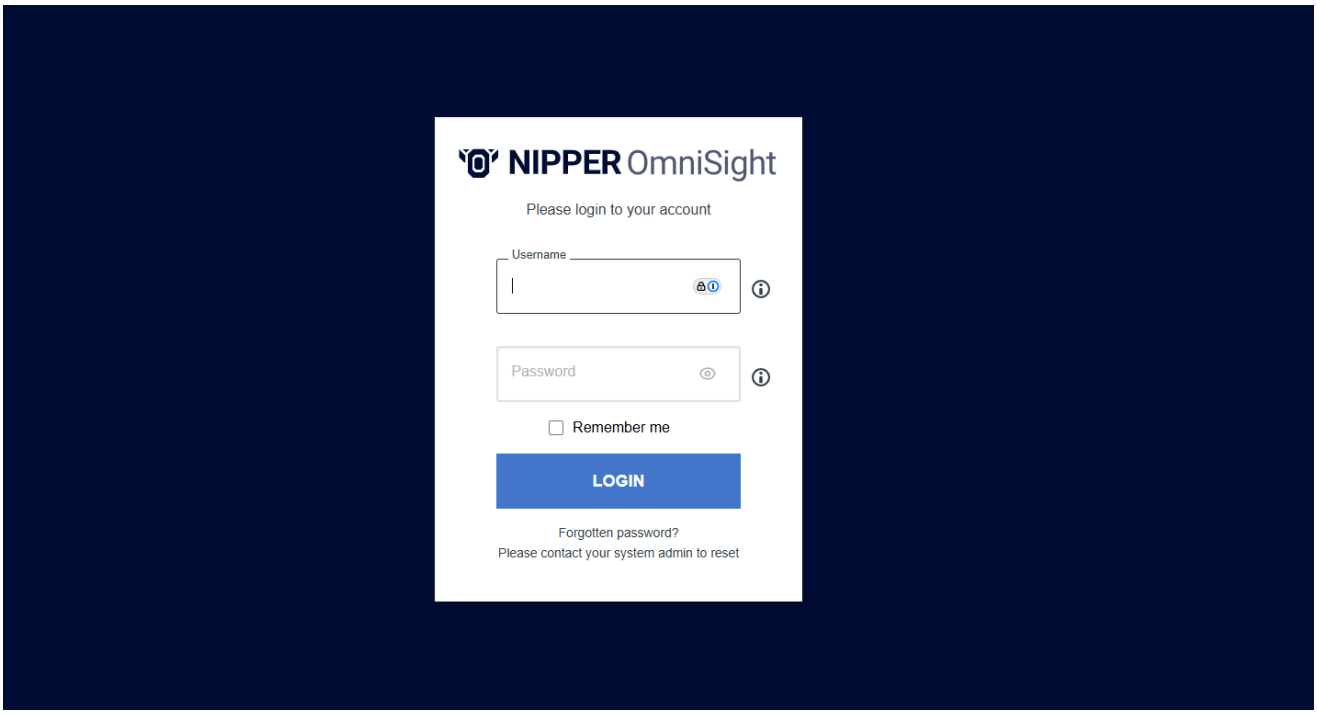
4. Accessing Nipper OmniSight for the first time

Once Nipper OmniSight has successfully been installed and all setup has been completed you will be able to access the login page of the system, this can be done in your browser (we support these browser versions and later **Chrome** - 140.0.7339.185, **Firefox** – 143.0.1, **Edge** – 140.0.3485.94) and going to https://(address) where the (address) is the IP or hostname of the machine that currently hosts Nipper OmniSight.

5. User Guide

5.1 Login

Upon navigation to the Nipper OmniSight URL, you will be presented with the login page.



Once you have reached the login page you will be shown a login prompt, you can use the default login:

Username: admin

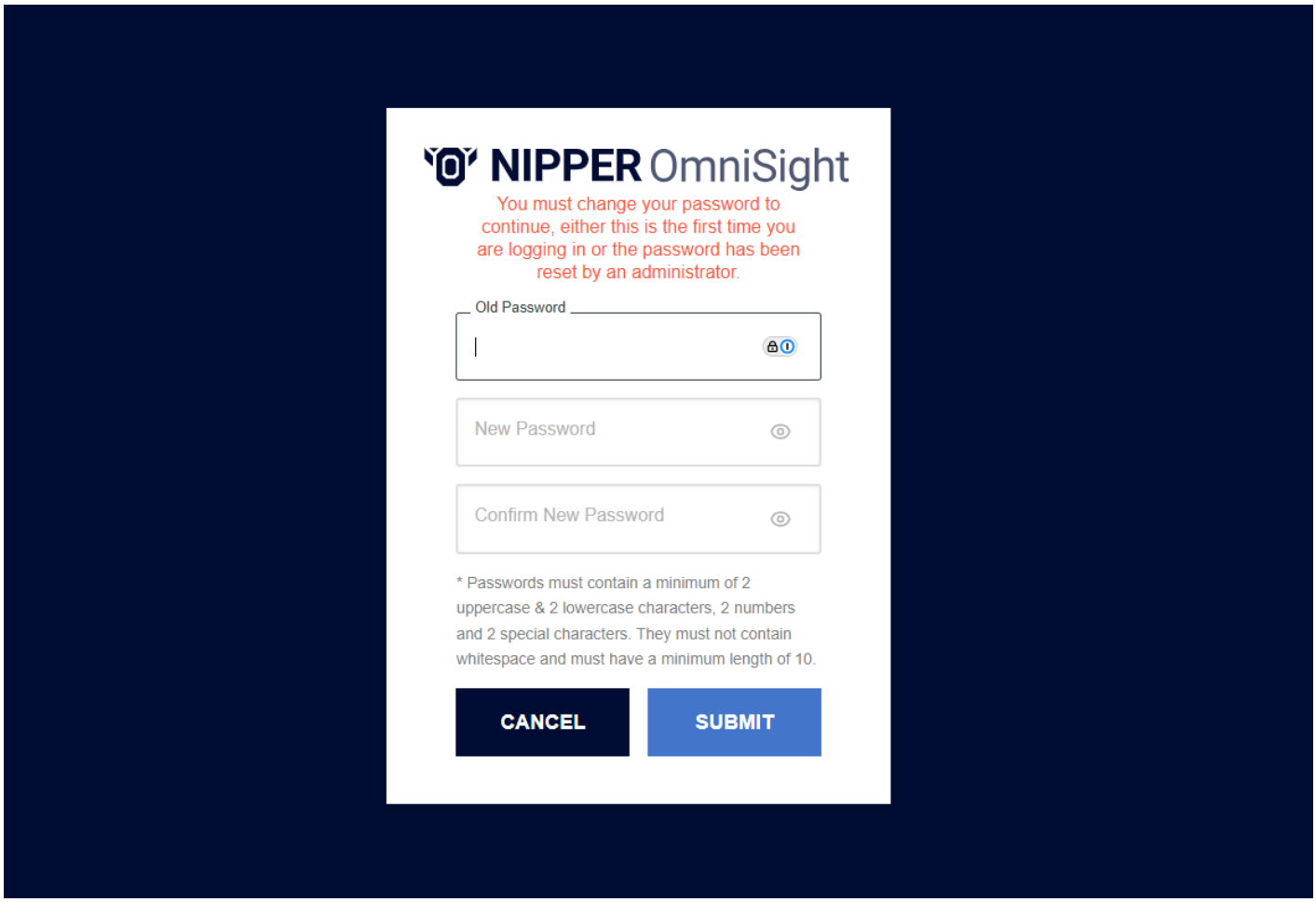
Password: pass

Once the first step has been completed, you will be prompted to change the password on the next screen.

5.1.1 Changing your Password

The Change Password screen is shown either:

1. Following the initial login to the Nipper OmniSight product
2. Following a password reset by an Administrator
3. Following the user selecting to change their own password



Old Password: Enter your old password here.

Clicking on the Eye icon within the password input box, will allow you to see the password entered.

New Password: Enter your new password here. Your new password must contain a minimum of 2 upper case and 2 lower case characters as well as 2 numbers and 2 special characters. No spaces should be included, and it must be a minimum of 10 characters long. Clicking on the visibility eye icon within the password input box will allow you to see the password entered.

Confirm New Password: Re-enter your newly created password here. Clicking on the Eye icon within the password input box, will allow you to see the password entered.

Once you've completed the screen, clicking **Submit** will save your new password and you will be redirected back to the login screen.

Clicking on **Cancel** will take you back to the previous login screen.

5.1.2 Two-factor Authentication (2FA)

If you have requested to enable two-factor authentication, you will need to complete a two-factor authentication (2FA) process in order to access the product

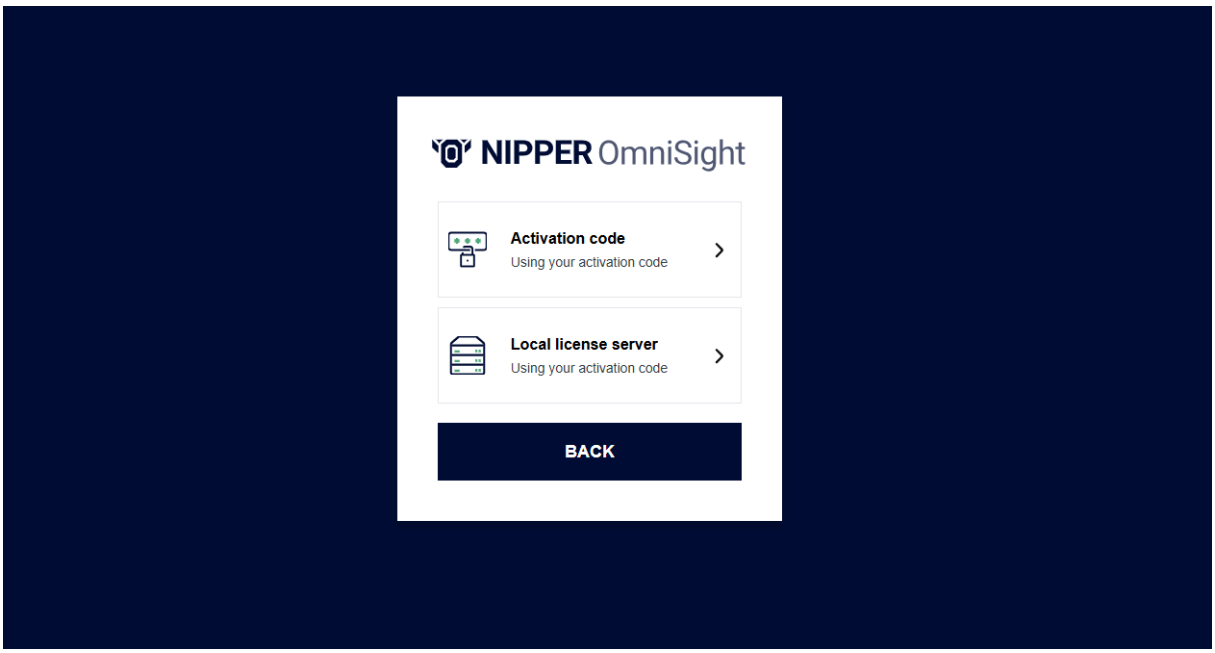
Two-factor authentication (2FA) is used by Nipper OmniSight to provide an extra layer of security when accessing the product. It requires you to have access to an authentication application in order to generate a time-sensitive authentication code.

The 2FA screen is displayed, either following the first successful login to the Nipper OmniSight product or following a successful password reset. Using your chosen authentication application, scan the QR code displayed on screen, creating a Nipper OmniSight account, then click Continue to Login to be redirected to the code input screen. By hovering over the Information icon, additional information is provided to assist with the 2FA process. Enter the code shown on your authentication application, then click Next to complete the login process.

Note: You have a limited number of attempts to successfully enter the authentication code. Following three consecutive incorrect entries, you will be redirected back to the start of the login screens. To reset your 2FA, please contact your system administrator.

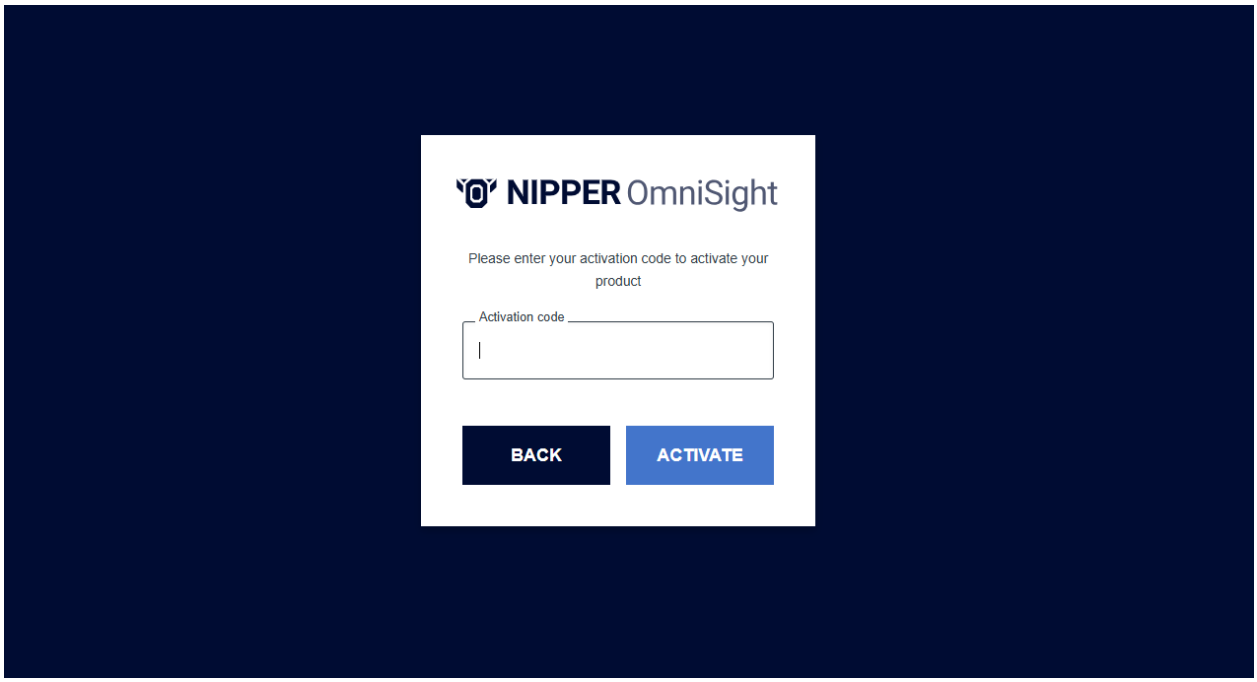
5.2 Activation Code

You will now be presented with a screen to enter either an Activation Code or to connect to the Local License Server (if operating offline).



Activation Code

If you are operating in an online environment, you can select Activation Code, and enter the code that was provided in the file activation_code.txt.

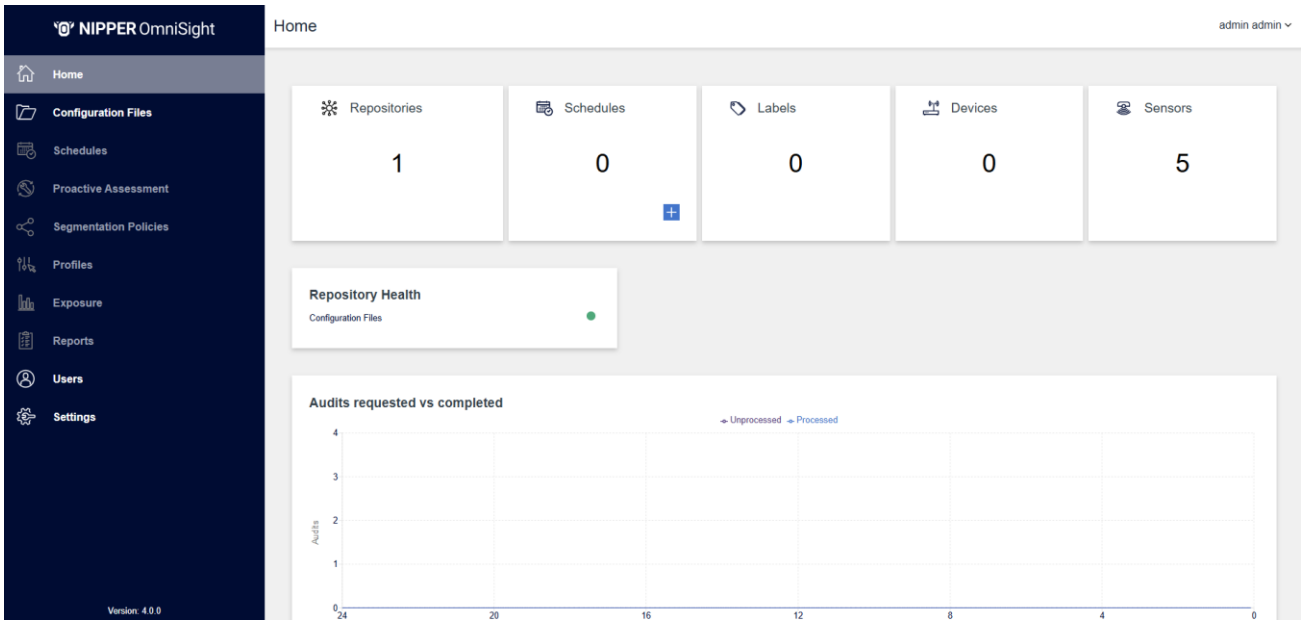


Local License Server

If you are operating in an offline environment, you will not be provided with an Activation Code. Instead, when you receive your OVA, it will contain a local license server that is pre-activated with your entitled licenses. After deploying and starting this local license server within your environment, you should then be able to enter your Activation Code, along with the URL of the local license server, in this screen. Once this information is submitted, OmniSight will validate against the local server and become fully licensed, functioning in the same way as it would with an online activation.

5.3 Home Screen

Once you have entered the activation code, you will be presented with the Home Screen.



You will be able to navigate to the Users, and Settings screens, as well as the Configuration Files screen. To set up any reporting within Nipper OmniSight, you must first add your configuration files.

5.4 Configuration Files

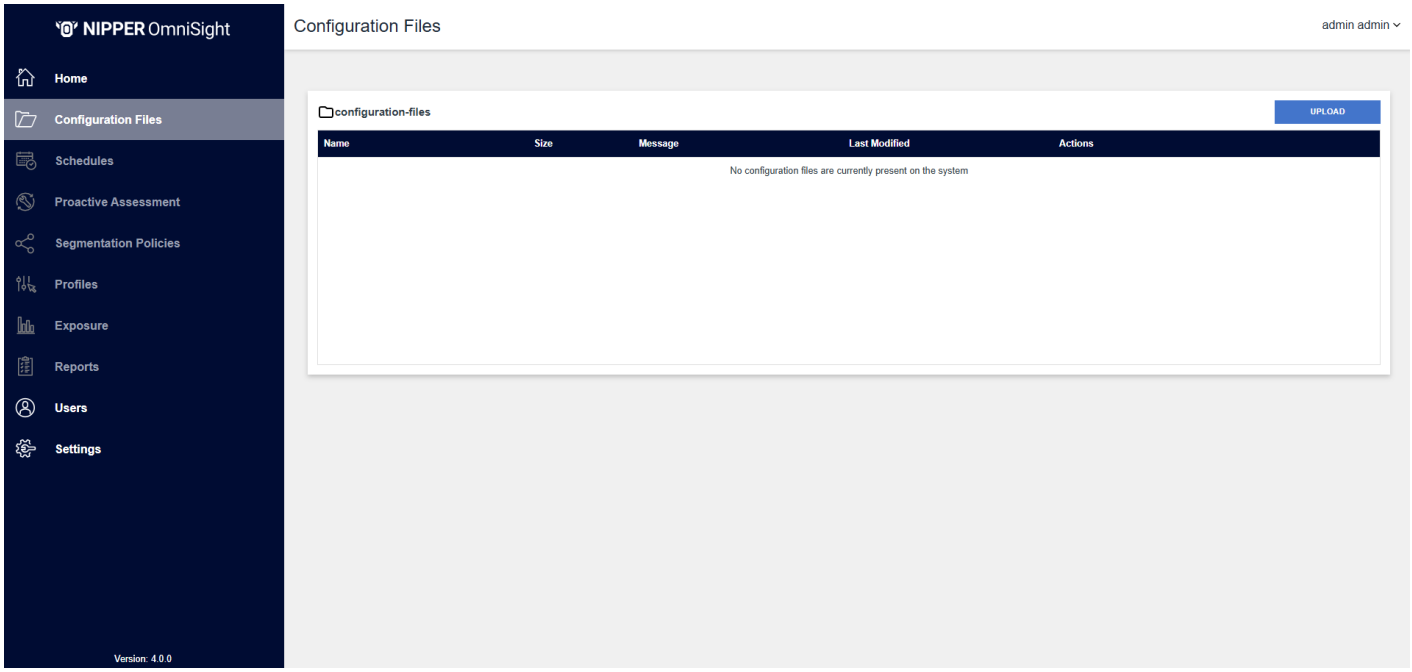
The Configuration Files page provides the ability to upload configuration files directly into Nipper OmniSight. These configuration files do not persist to disk, instead they are stored in memory for 24 hours, however this duration can be updated in the Settings page. Once the TTL expires the files will be automatically deleted.

Configuration files can be re-uploaded at any time

Note: Configuration Files is only available to users in the Administrators group or the NOC group.

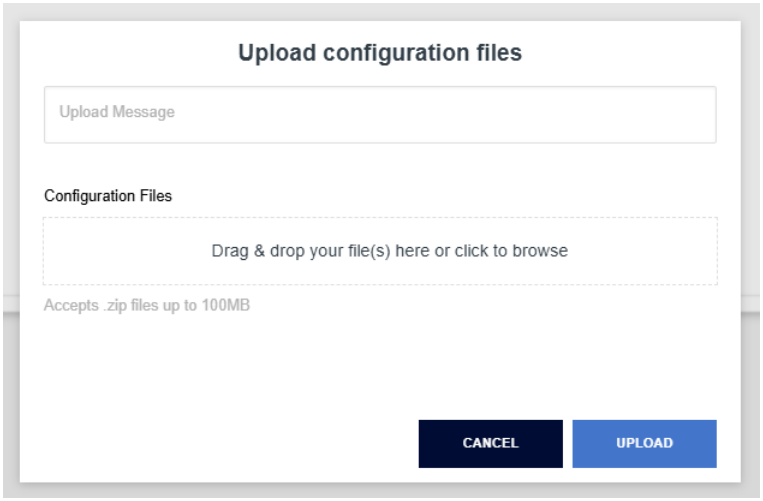
5.4.1 Uploading Configuration Files

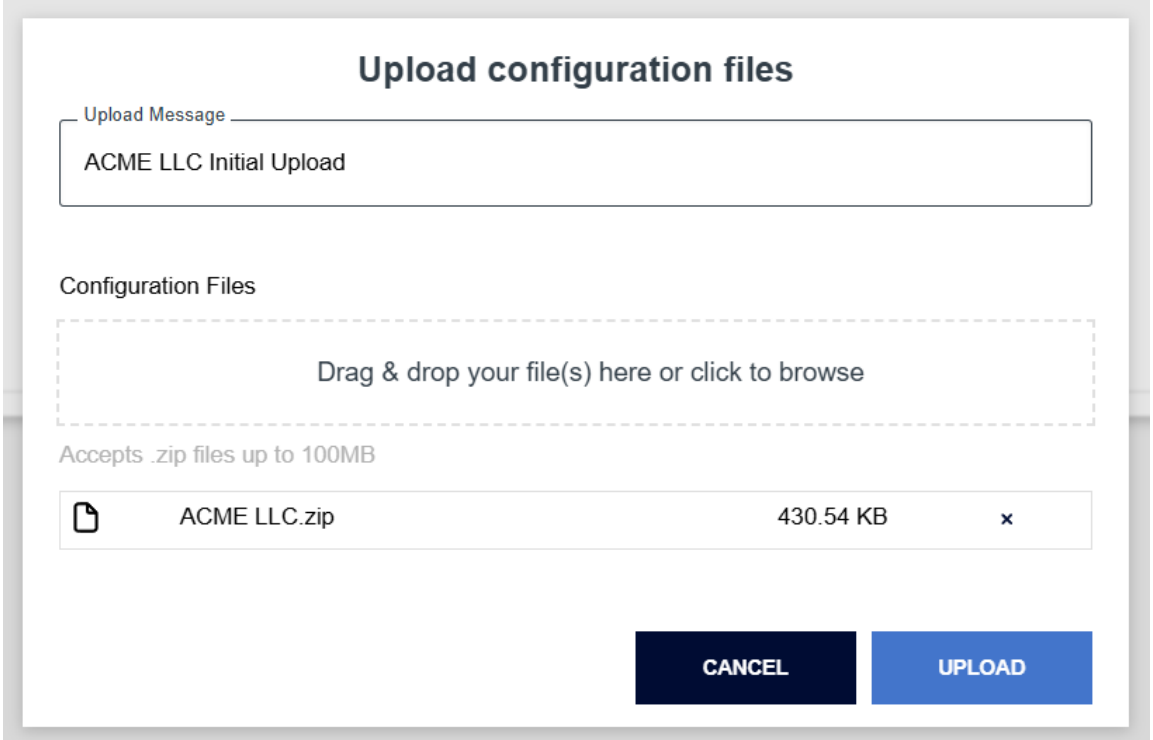
Clicking on the **Configuration Files** link on sidebar menu, you will be navigated to the upload configuration files page.



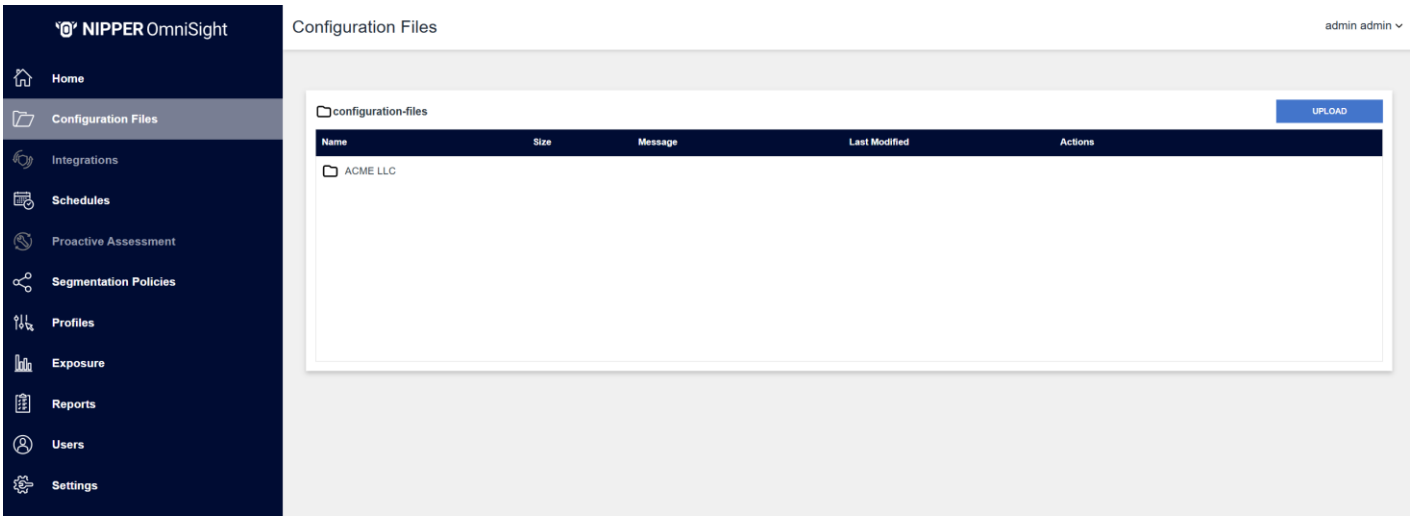
Click the Upload **button** to add configuration files. A pop-up window will appear, allowing you to select a file and provide an upload message.

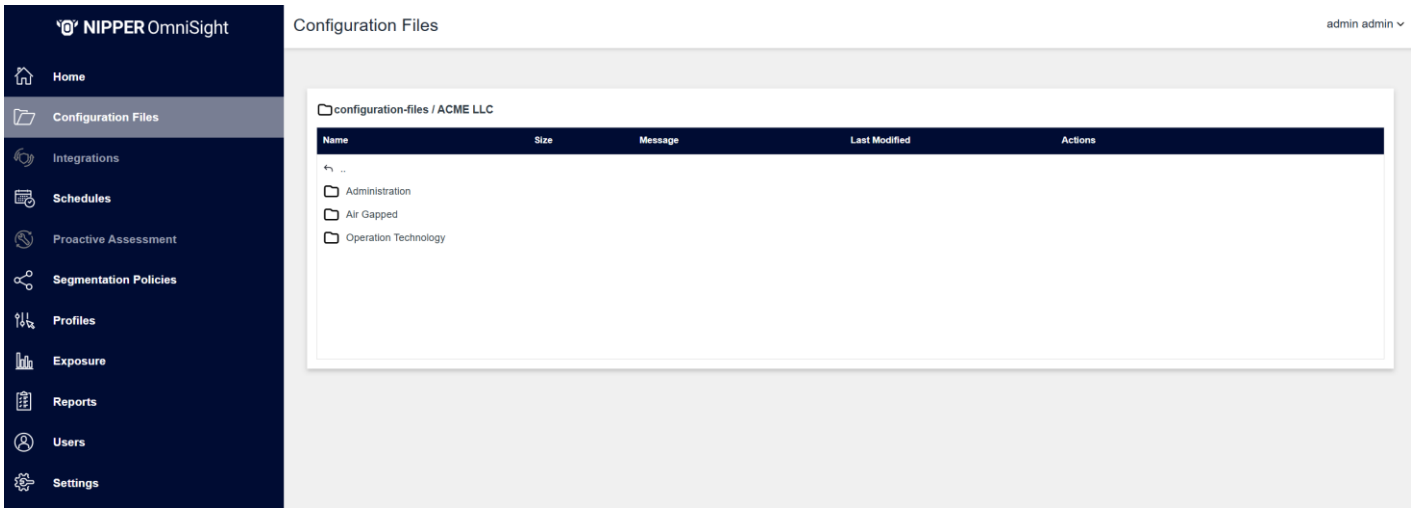
Note: Uploads are restricted to ZIP files with a maximum file size of 100 MB. A ZIP file containing multiple files must contain a folder structure as this is used to Label the configuration files, see Section 5.4.3. You must supply an Upload Message to upload the files. Multiple file uploads are not supported at this time.

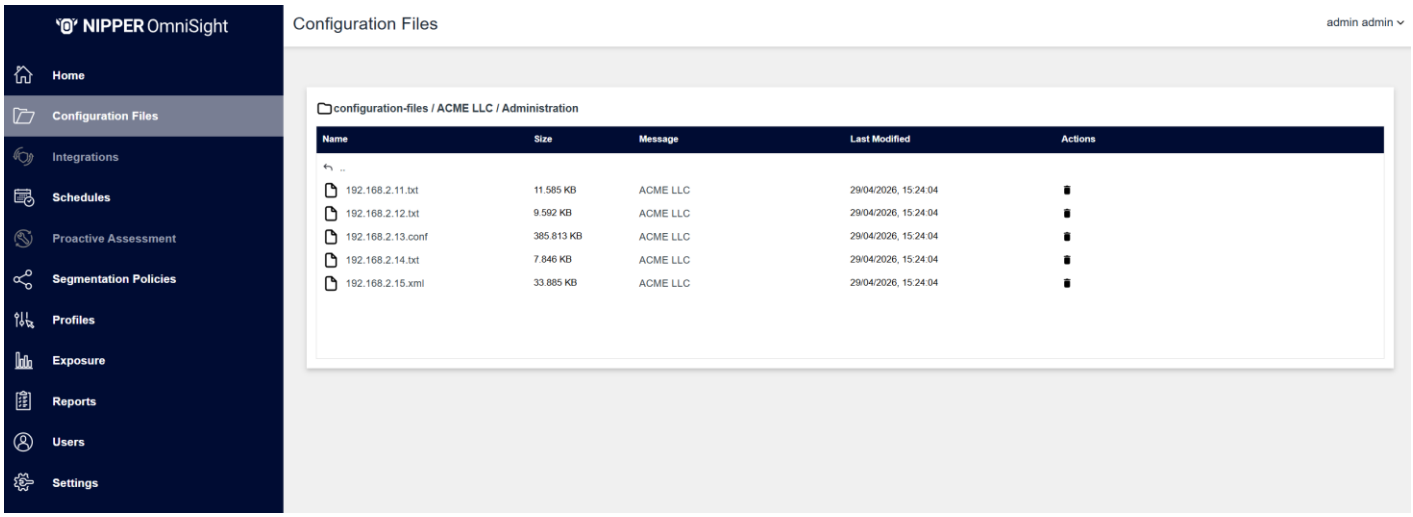




Once the upload is complete you can view a folder structure containing the configuration files.







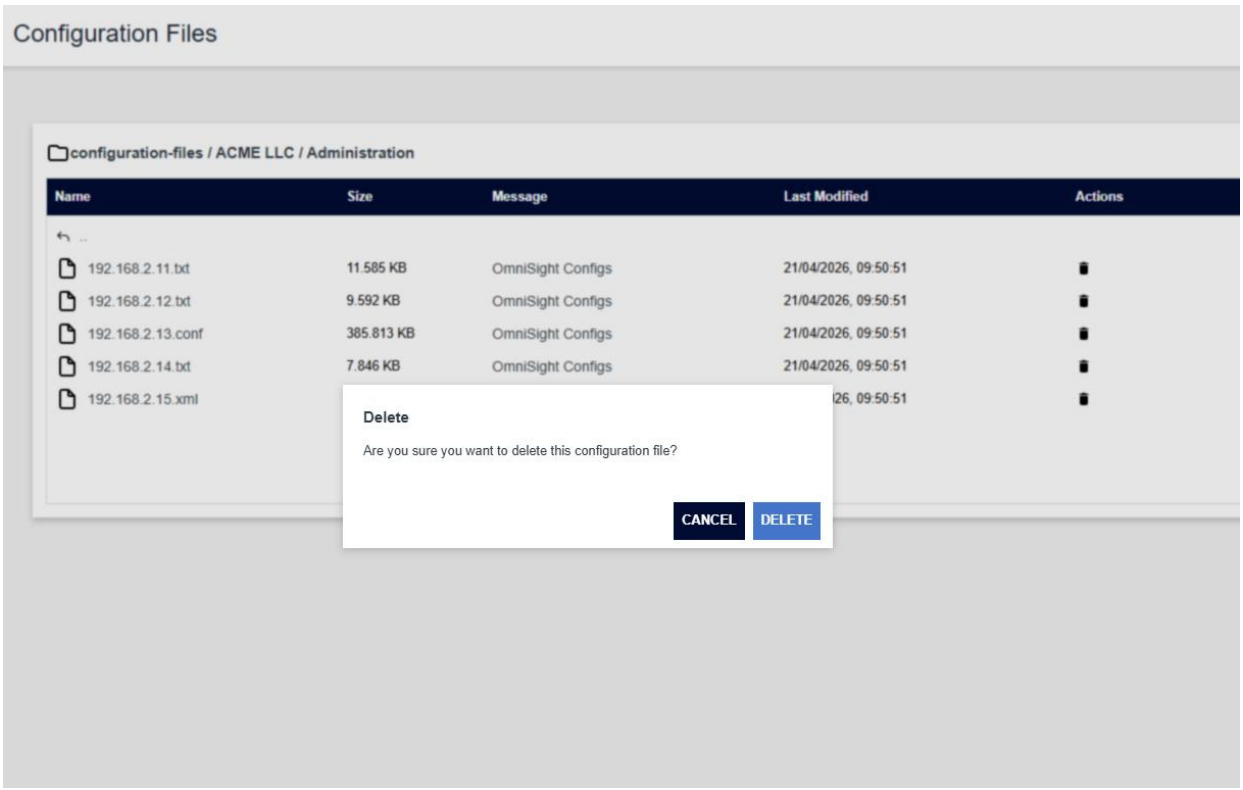
Once you have added in your configuration files, the sidebar will become active, except for Integrations and Proactive Assessment, as this functionality is not available within Standalone.

If the repository appears disconnected, this is due to it resyncing, whilst the connection status is orange no labels are returned. This is a temporary state and the files will be available after the synchronisation completes.

5.4.2 Deleting Configuration Files

To delete a configuration file, click the **Delete** icon under the "Actions" column on the row for the corresponding file that is to be deleted.

Clicking this delete button will prompt a deletion confirmation dialog, clicking **Delete** will remove the file, whereas clicking **Cancel** will navigate back to the folder view.

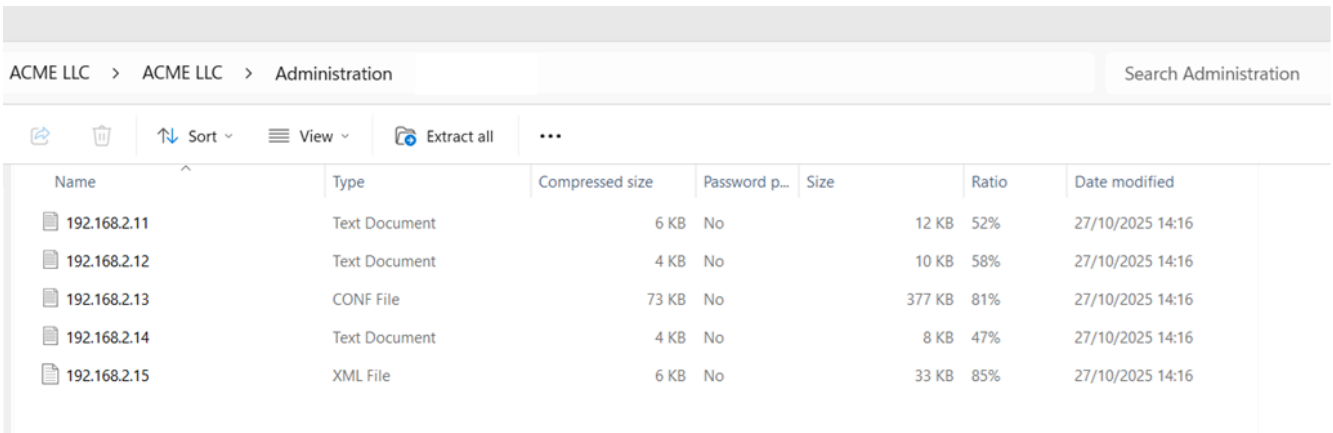


5.4.3 Labels in Configuration Files

Nipper OmniSight is configured to treat the Configuration File folders as labels.

Later, when creating Schedules, when prompted to select a label, the name of each folder within Configuration Files will be the label you select.

If a file is within nested folders, then that device will have the labels of all folders in its structure. In this example, the configuration file named 192.168.2.11 has the labels of Administration and ACME LLC:

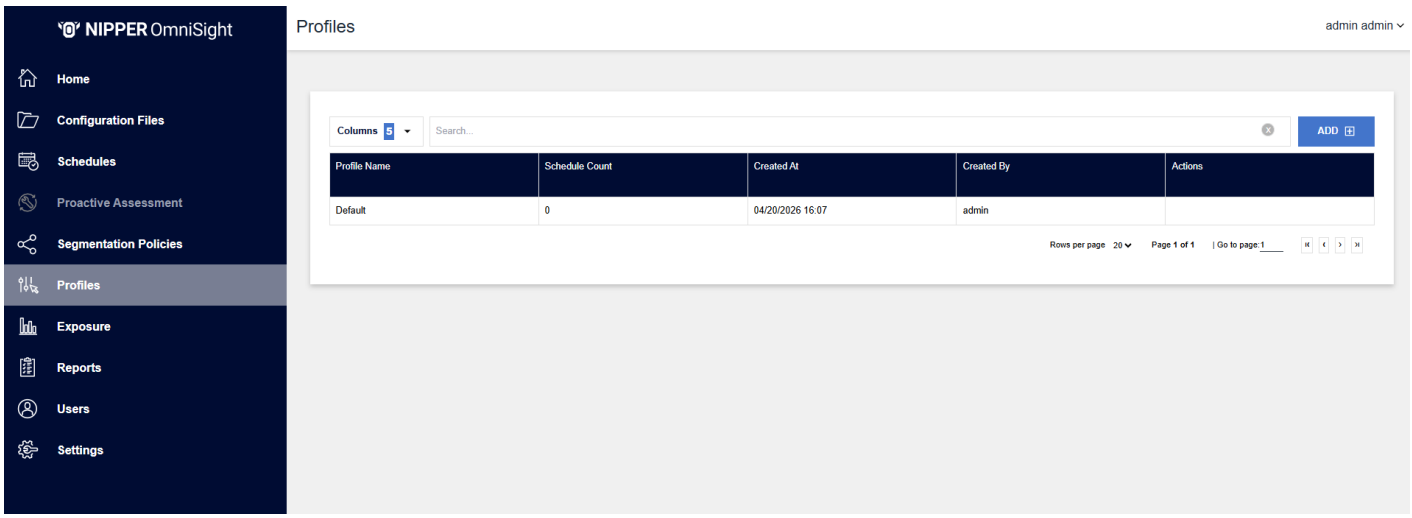


Note that label names are **case-sensitive**.

5.5 Profiles

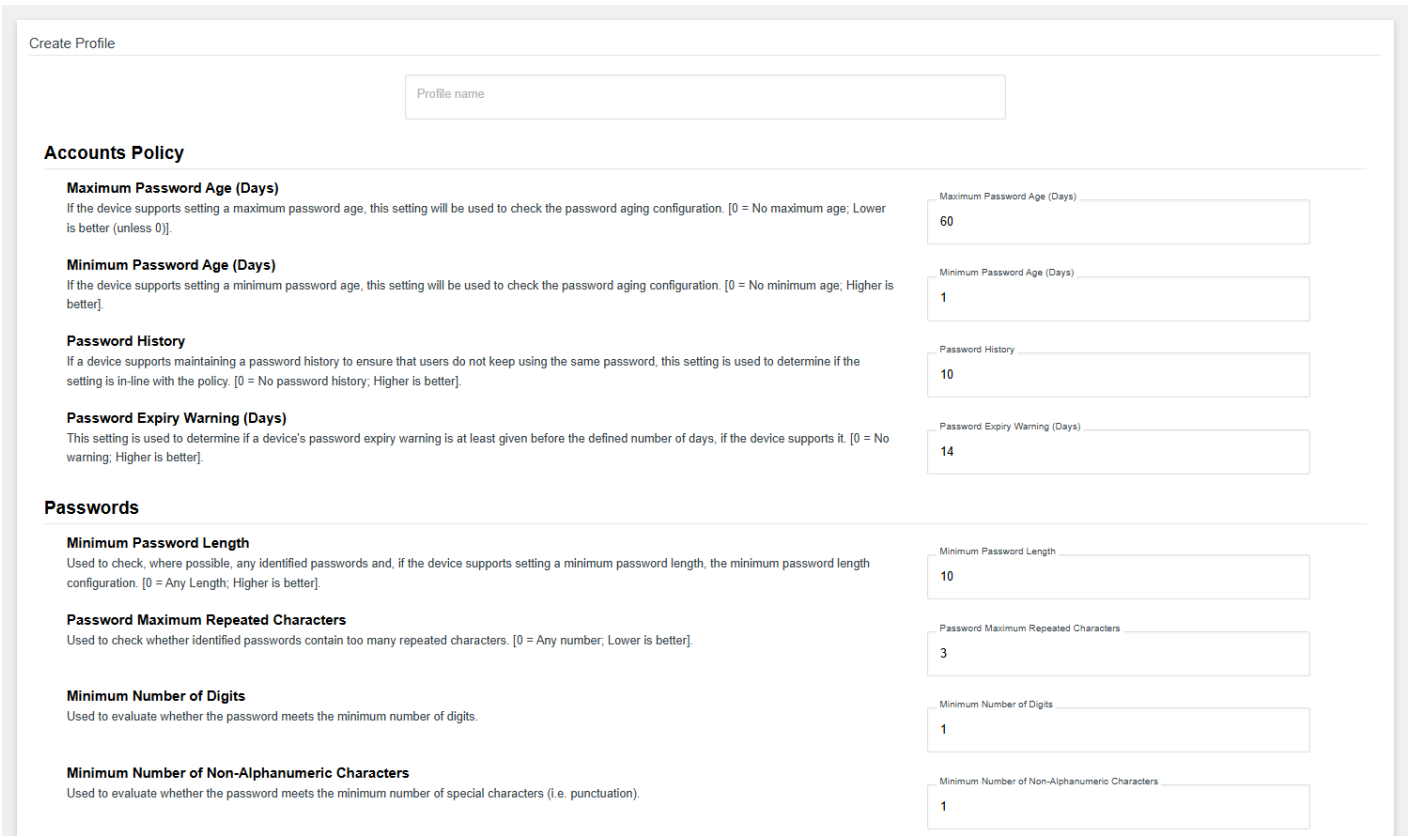
Profiles allow you to fine-tune the report output Nipper OmniSight will generate.

To access **Profiles**, you must click the “Profiles” button on the left-hand sidebar. A “Default” profile will already be listed and is automatically applied to assessments if no other profile is specified.



5.5.1 Creating a Profile

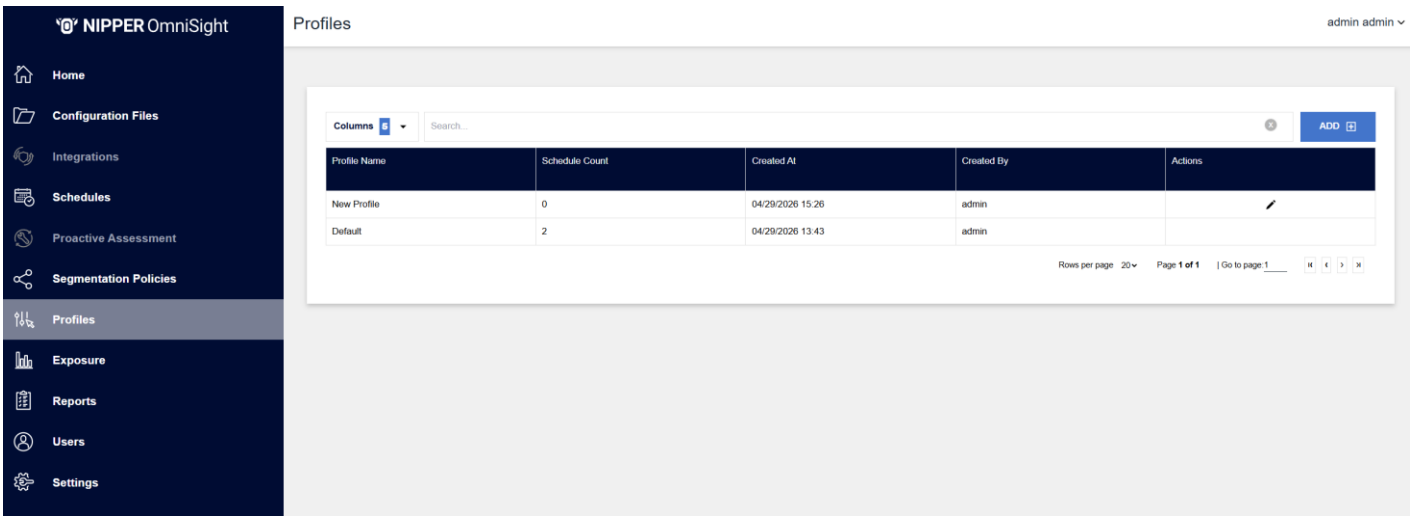
Clicking the “Add” button to the top right of the table will open the Create Profile page where you will be presented with an empty Profile Name field and a series of settings split between various categories. The pre-defined values are based off the Default profile.



Various input fields are visible on this page:

- **Numerical**: Will only accept an integer number.
- **Toggle**: Can be activated/deactivated.
- **Dropdown**: When clicked a dropdown menu of options will appear.

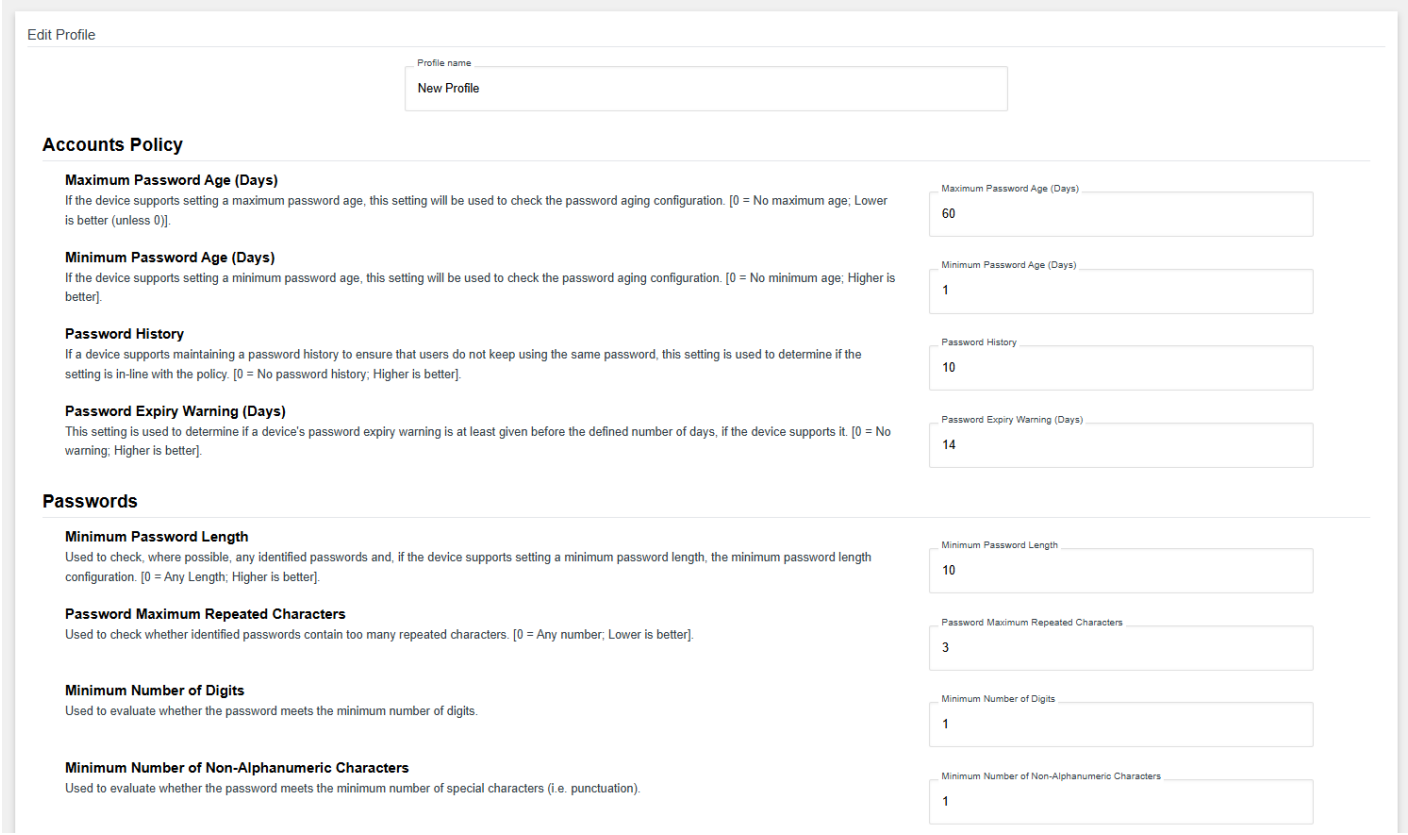
Once the required preferences have been set the Profile can be saved and added to a Schedule rule. It will now appear in the Profiles list.



5.5.2 Edit Profile

To edit an existing profile, navigate to the Profiles page, and click the **Edit** (pencil) icon under "Actions" on the row for the corresponding profile that is to be changed.

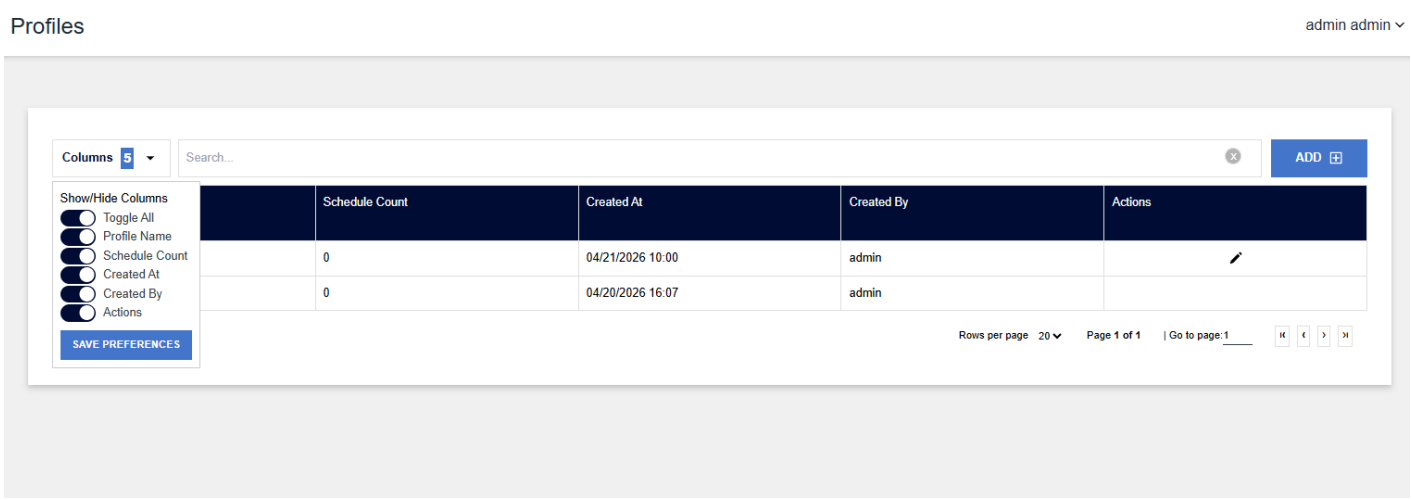
Clicking this will navigate to the Edit Profile page, where profile settings can be changed as desired



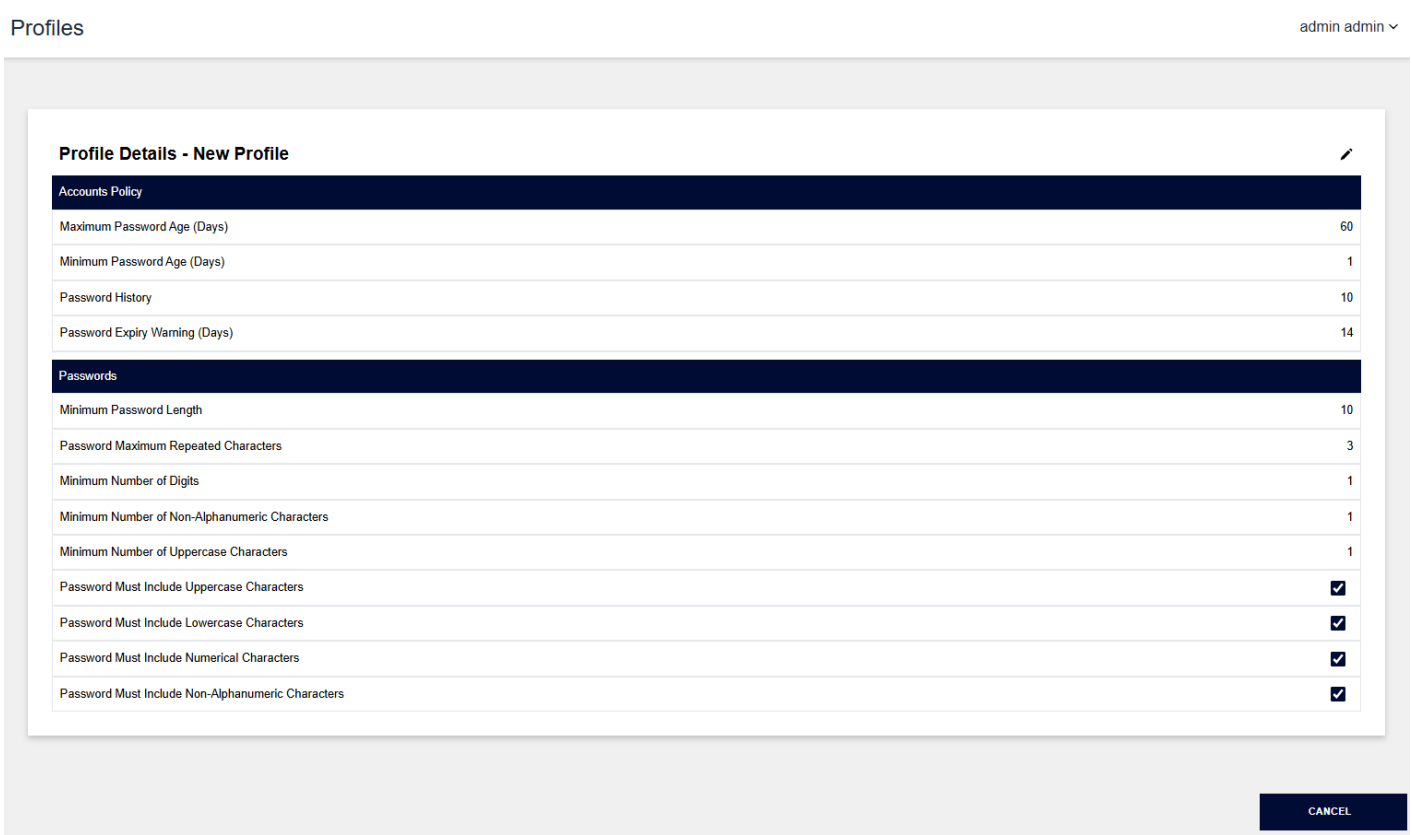
Once the edits have been made, scroll to the bottom of the page and click “Save”. You will be navigated back to the Profiles list page.

5.5.3 Viewing Profiles

The Profiles table has several columns that can be shown/hidden to the user or ordered by if clicking on the table column title.



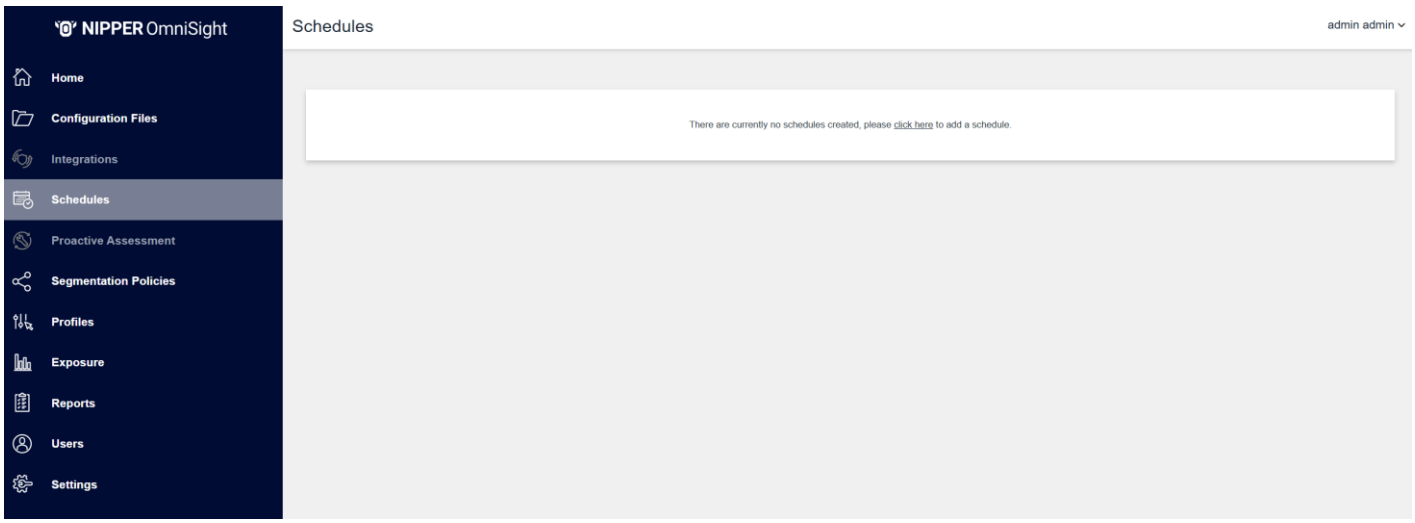
A user can also view the profiles by clicking on the profile row in the table. The profile settings cannot be changed on this page, but the user can be taken to the edit profiles page by clicking the **Edit** (pencil) icon in the top right corner of the View Profile page.



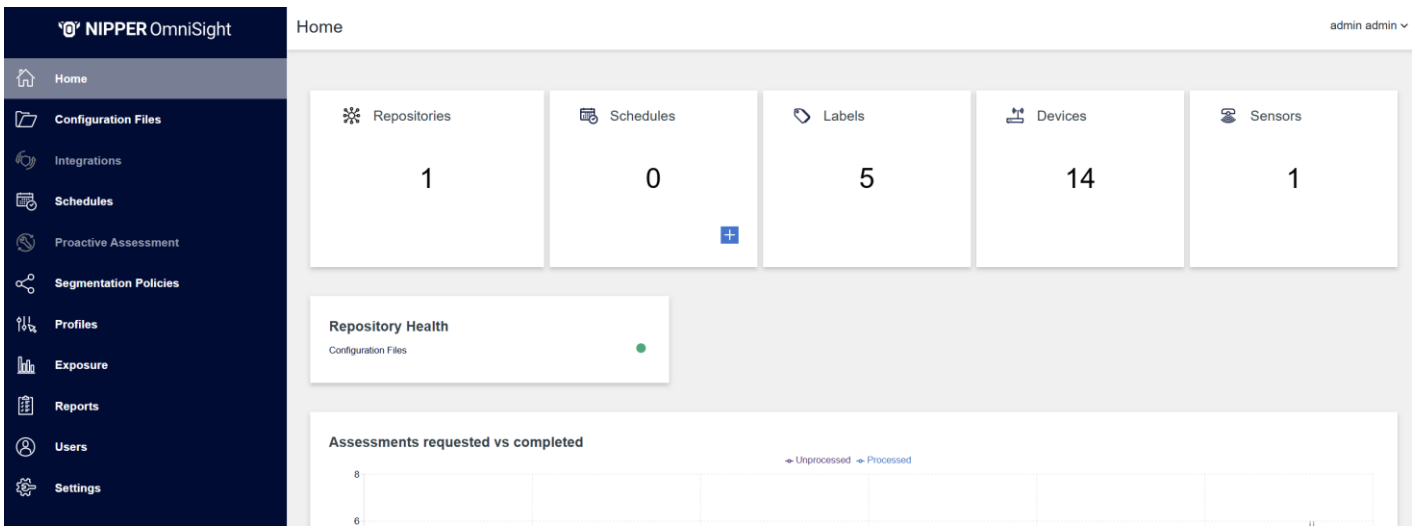
5.6 Scheduling

Scheduling allows fine-grained control over when a set of one or more pre-defined assessments are run, and with what frequency they should occur.

To access the Schedules screen, you can either click on the Schedules link in the sidebar menu, and navigate to the **Create Schedules** screen by clicking on the **click here** link:

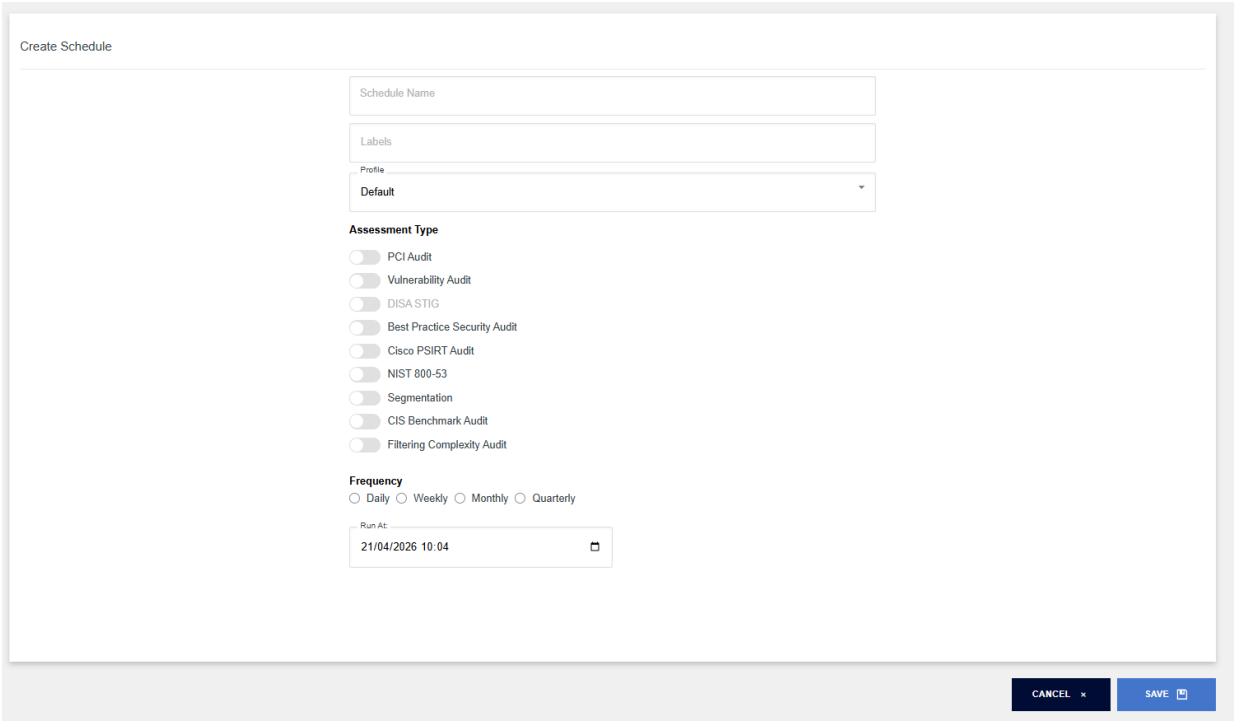


or click on the blue **Add** icon in the Schedules widget on the dashboard, which will take you straight to the Create Schedules screen.



5.6.1 Creating a Schedule

Once on the Create Schedules page you will be presented with a series of input fields.



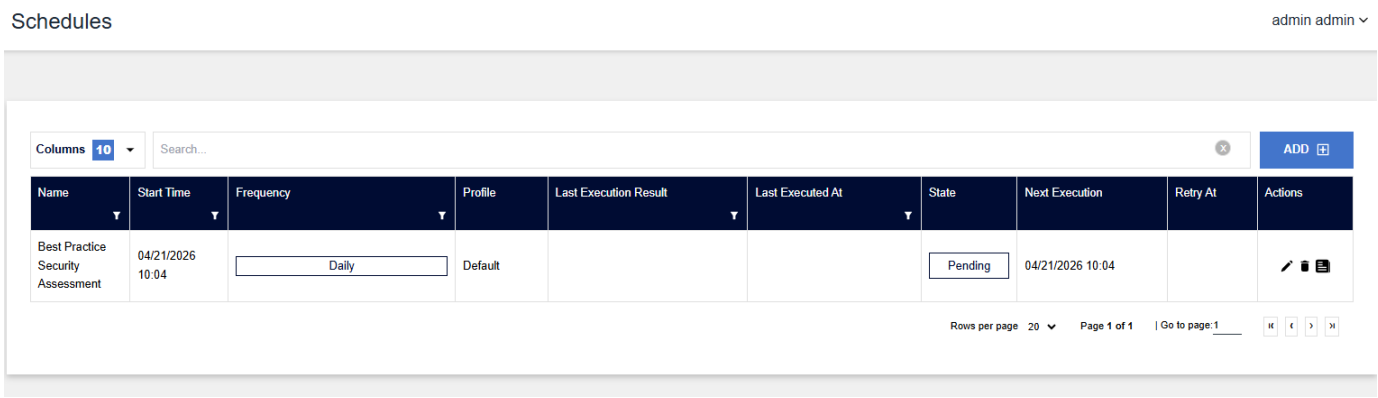
Some of these assessment and schedule options will only be visible if they have been enabled for your specific license. If you believe you should have access to certain options but don't see them, please contact Titania Support for assistance.

- **Schedule Name (Text Box):** An identifier for the Assessment Schedule to be created.
- **Labels (Text Box):** The folder name within Configuration Files where the configs you would like to assess are stored. This will assess all devices with the associated label, this is a logical AND operation not a logical OR operation. Note: Autocomplete of known labels will start once you type the first letter.
- **Profile:** Either the default profile or a custom one you have created
- **Assessment Type:** Each standard that can be assessed against has an ON/OFF radio switch to select which types apply to this schedule. The Assessment Types that can be selected are dependent upon your licensed options.
- **Frequency:** A set of mutually exclusive radio buttons to select the interval which governs how often the Assessment Schedule should run. The exact frequency options available is dependent upon your licensed options.
- **Run At:** A date/time selector to control the start date and time of this Assessment Schedule.

Segmentation assessments are dependent upon a Segment having been created with matching labels, if you wish to select Segmentation Assessment, please create a Segment in the Segmentation Policies screen first.

Once the form has been satisfactorily completed, the Assessment Schedule can be finalized and created with the **Save** button at the bottom right of the page. Alternatively, the **Cancel** button at the bottom of the page can be used to navigate back to the Schedules page.

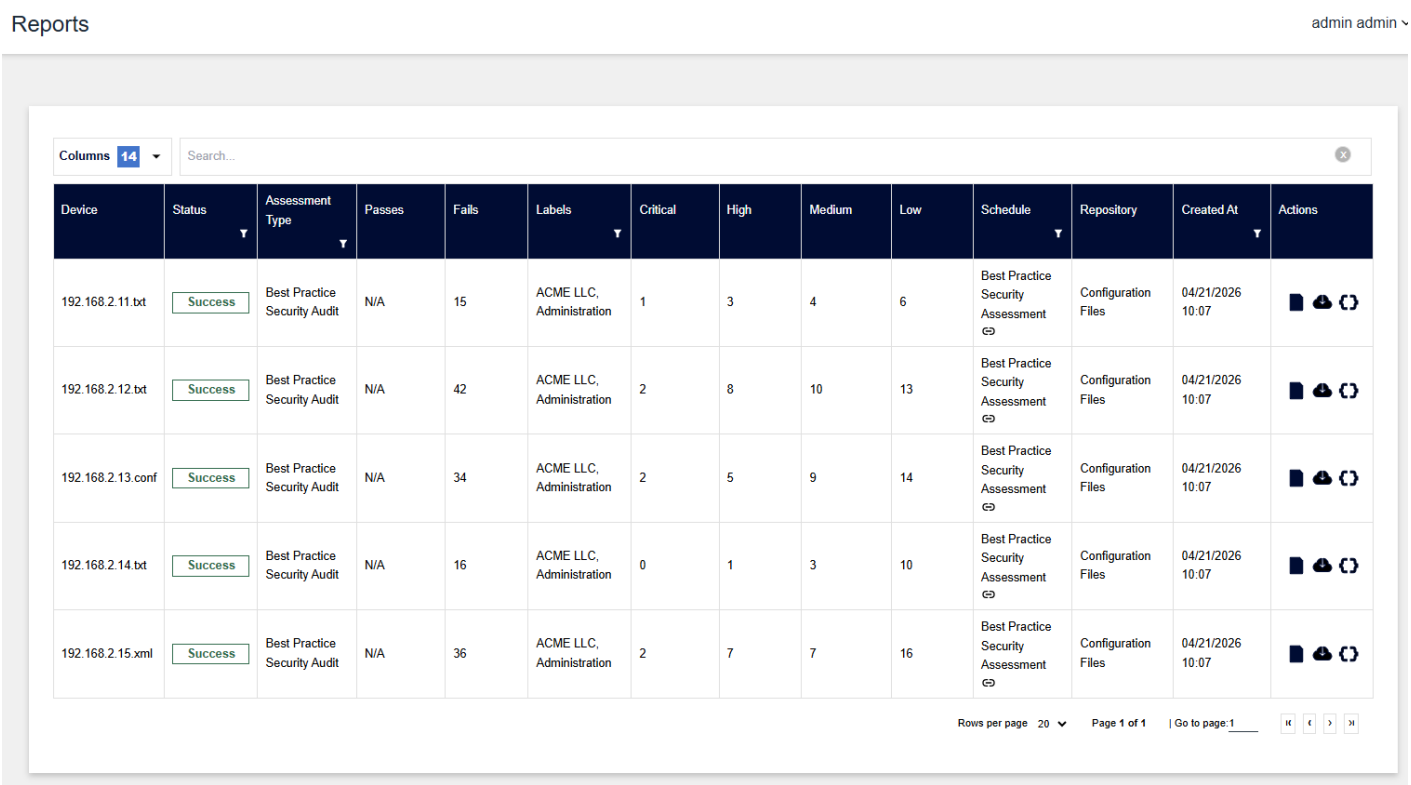
Upon successfully saving, the newly created Assessment Schedule should be visible within the Schedules table.



You can create further Schedules by clicking on the **Add** button.

5.6.2 Viewing Schedule Reports

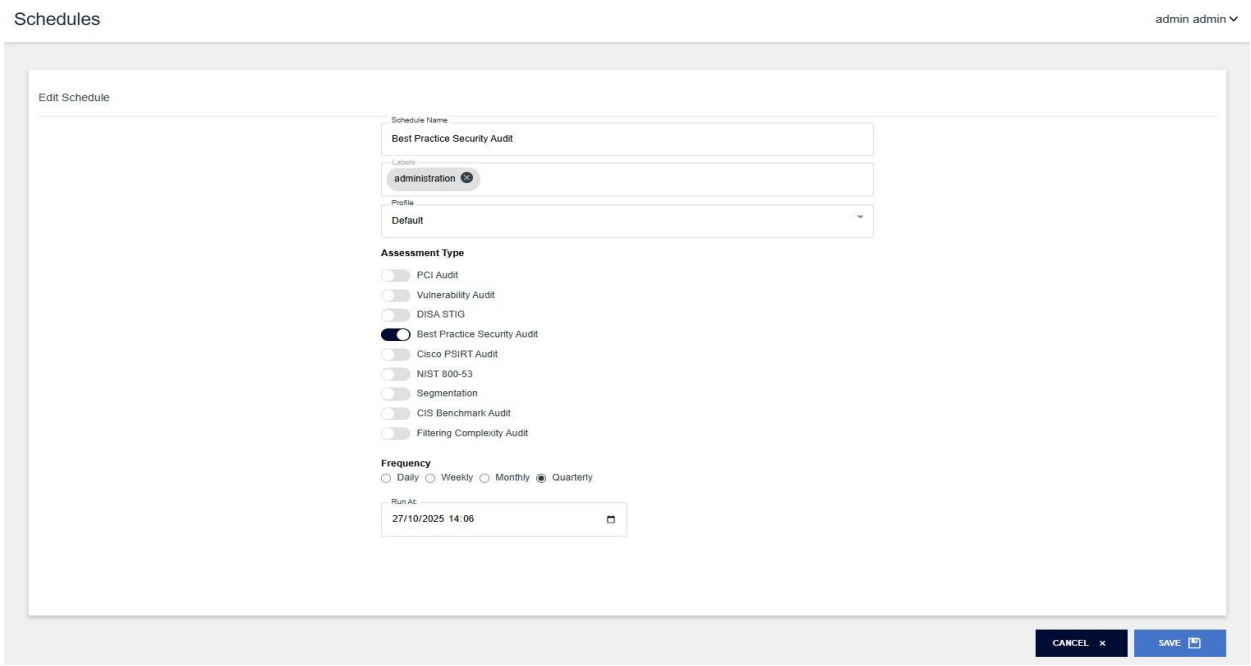
To view the reports generated from a schedule, you can click on the **View Reports** icon in the “Actions” column on the row for the schedule you would like to view. You can also click on the Report option in the side bar. This takes you to the Reports screen where the view will be pre-filtered to only show the reports for that schedule.



5.6.3 Editing an existing Schedule

To edit an existing schedule, navigate to the Schedules table, and click the **Edit** (pencil) icon under "Actions" on the row for the corresponding assessment that is to be changed.

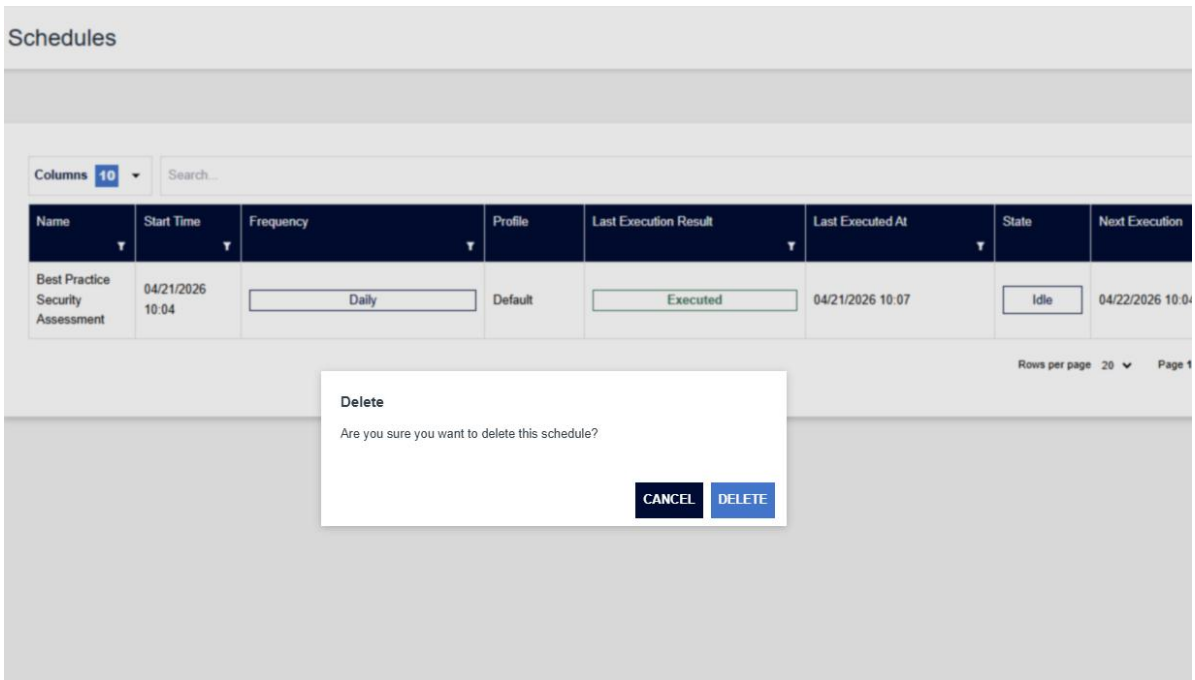
Clicking this will navigate to the Edit Schedule page, where settings for the Schedule can be changed as desired.



5.6.4 Deleting an existing Schedule

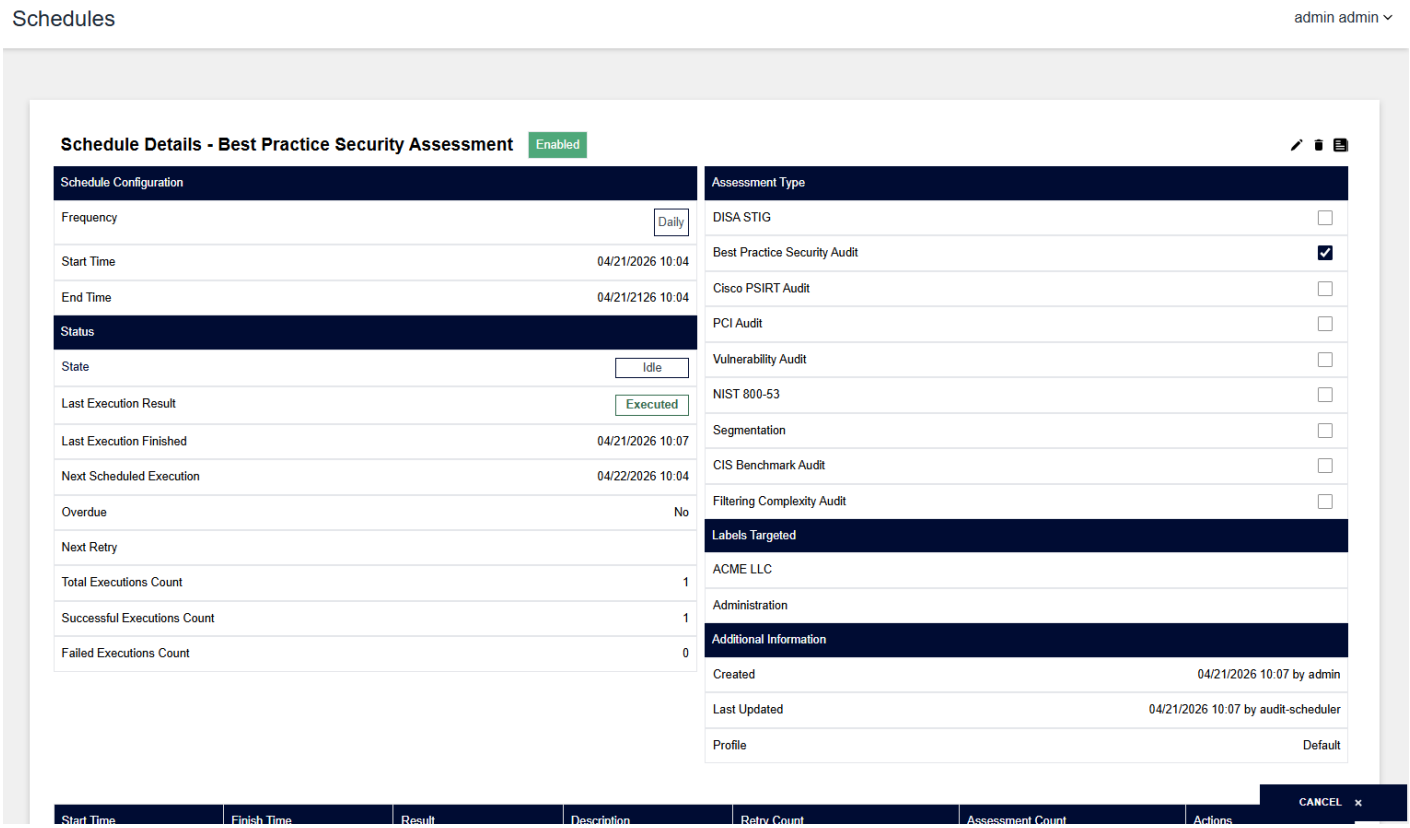
To delete an existing schedule, navigate to the Schedules table, and click the **Delete** icon under "Actions" on the row for the corresponding assessment that is to be deleted.

Clicking this delete button will prompt a deletion confirmation dialog, clicking **Delete** will remove the schedule, whereas clicking **Cancel** will navigate back to the Schedule table.



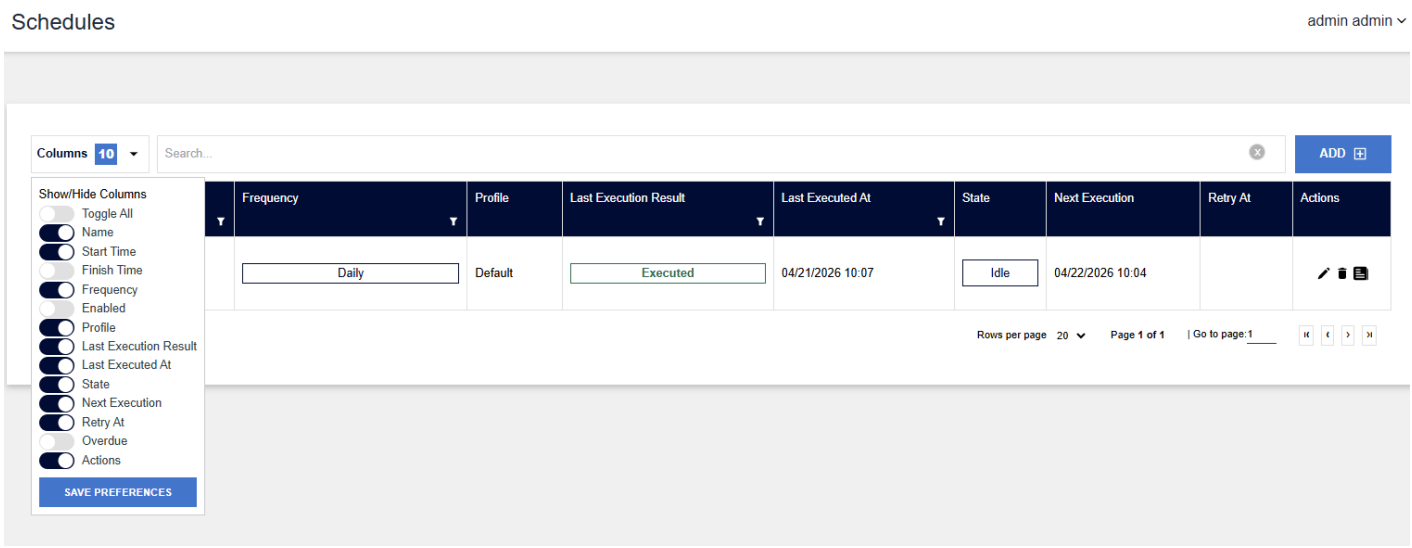
5.6.5 Schedule Details

To view the details of a schedule, click anywhere on the row in the table for the schedule you wish to view. From here you can view the settings applied to that schedule, the status of the schedule and navigate to the Reports screen. You can also edit and delete a schedule from here and see the different executions of the schedule at the bottom table and view reports specific to the schedule runs.



5.6.6 Viewing the Schedules table

The columns on display as default can be amended by simply clicking on the Columns drop down menu and selecting or deselecting the columns from the list.



You can also order the table based on the data in any of the columns by clicking on the column title.

5.7 Segmentation Policies

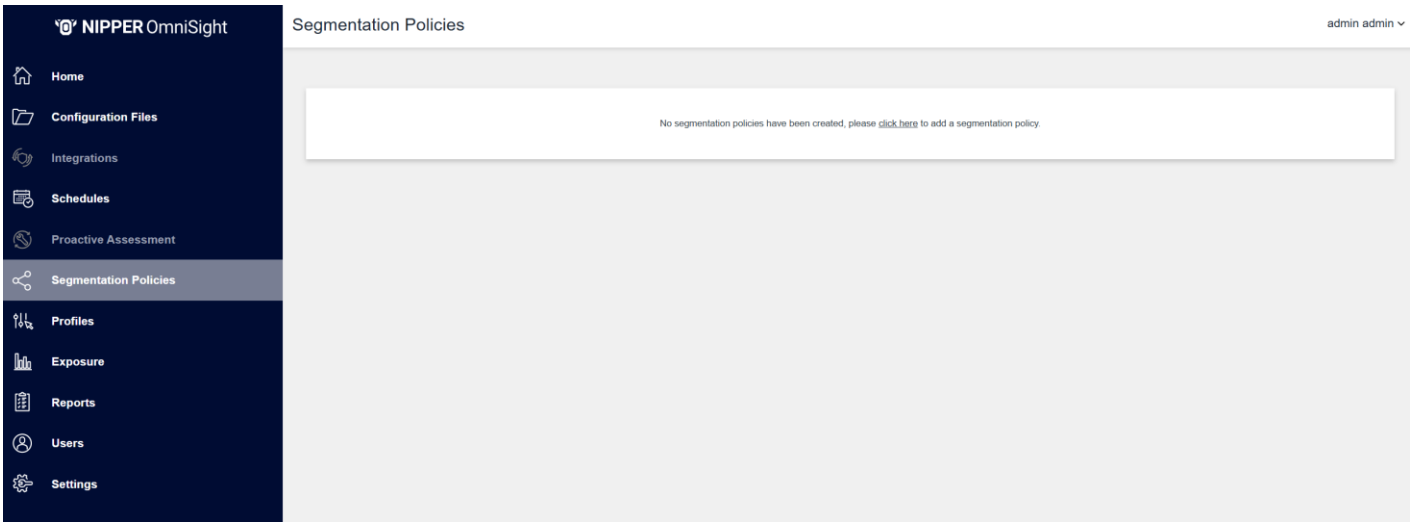
Nipper OmniSight helps organisations strengthen the security of their network infrastructure by ensuring that critical segments remain properly isolated, reducing the overall attack surface and limiting potential blast radiuses. Within the platform, you can define Segmentation Policies that establish precise Allow Lists for each segment, specifying which IP addresses, ranges, services, and local user accounts are permitted, along with the privilege levels required to maintain Least Privilege Access. Once these policies are in place, scheduled segmentation assessments automatically verify that your live network configuration continues to align with the defined Allow Lists, supporting ongoing operational hardening and sustained assurance.

Because the Allow Lists contain sensitive information, Nipper OmniSight securely one-way encrypts this data so it cannot be retrieved in its original form. When a device configuration is later assessed, the platform applies the same encryption process to the relevant fields and compares the results to confirm whether the segmentation policy is being correctly enforced.

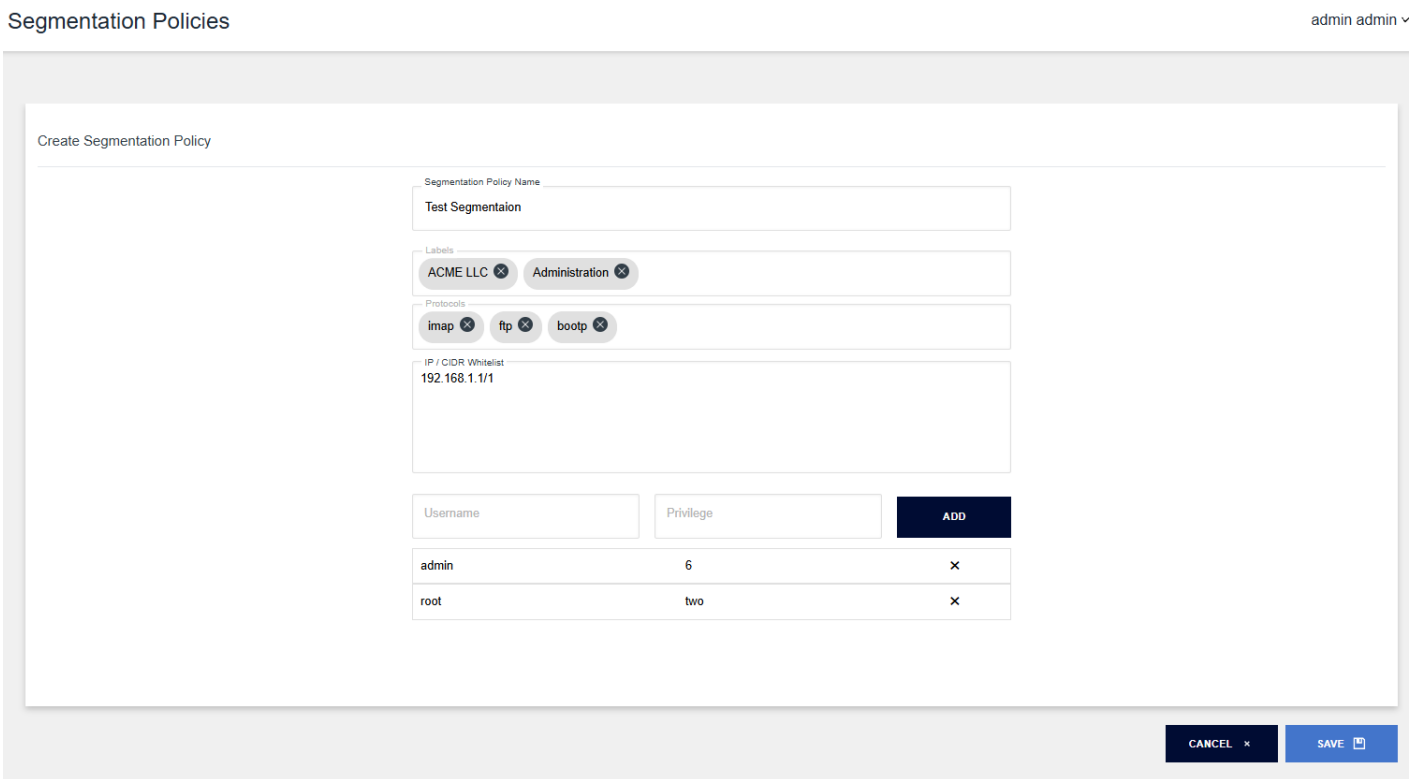
To get started, simply create a new Segmentation Policy, associate it with a segment by selecting the appropriate labels, and provide the required Allow List information. Once complete, you can then construct schedules for that segment to automate ongoing assessments.

5.7.1 Creating a Segmentation Policy

To create a new Segmentation Policy, navigate to the **Segmentation Policies** page using the sidebar menu. If this is your first time creating a policy, the page will display an introductory prompt inviting you to create your initial Segmentation Policy.



This section is where you define the details of your Segmentation Policy.



Assign the policy a clear, unique name that provides meaningful context for its purpose.

Define the segment by selecting the labels that uniquely identify it; any devices matching this label structure will automatically be included in scope for assessment against the policy.

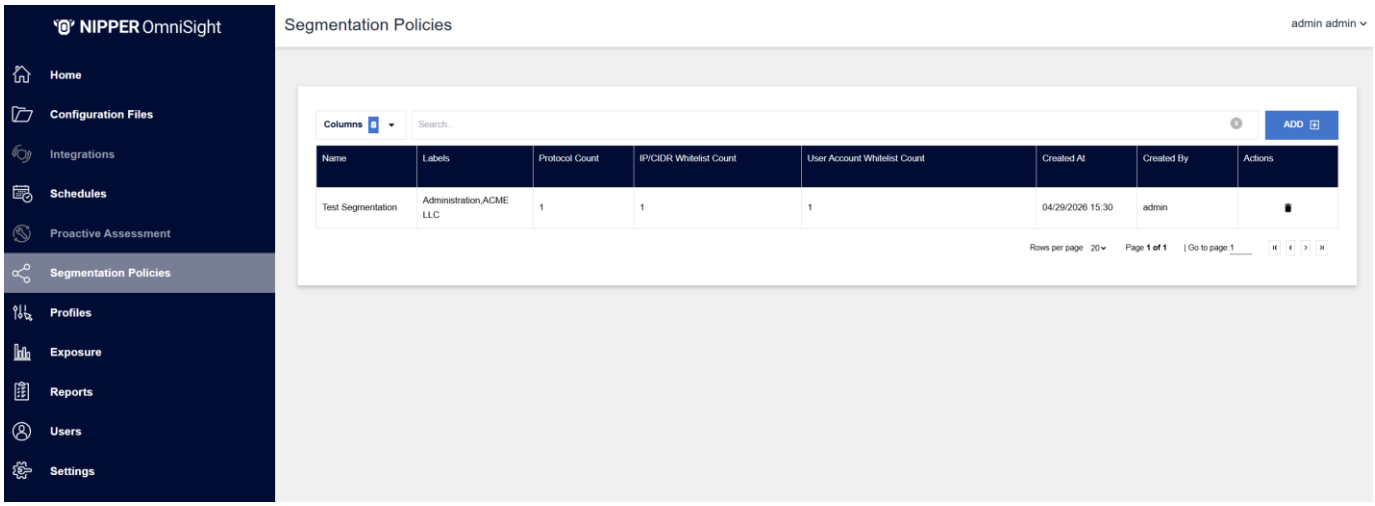
Specify an Allow List of authorised protocols by typing into the field, matching protocol options will appear for selection, and if no match exists, you can create a new protocol entry.

Define an Allow List of authorised IP addresses and CIDRs for communication to and from the segment, using any combination of fixed IPs and ranges. Entries must be comma-separated, and pre-prepared lists can be pasted directly into the field.

Define an Allow List of authorised Local User Accounts and their associated privilege levels that should have access to networking devices within the segment.

Once all required fields have been completed, you can save the policy to apply your changes, or cancel to discard them and return to the Segmentation Policies page.

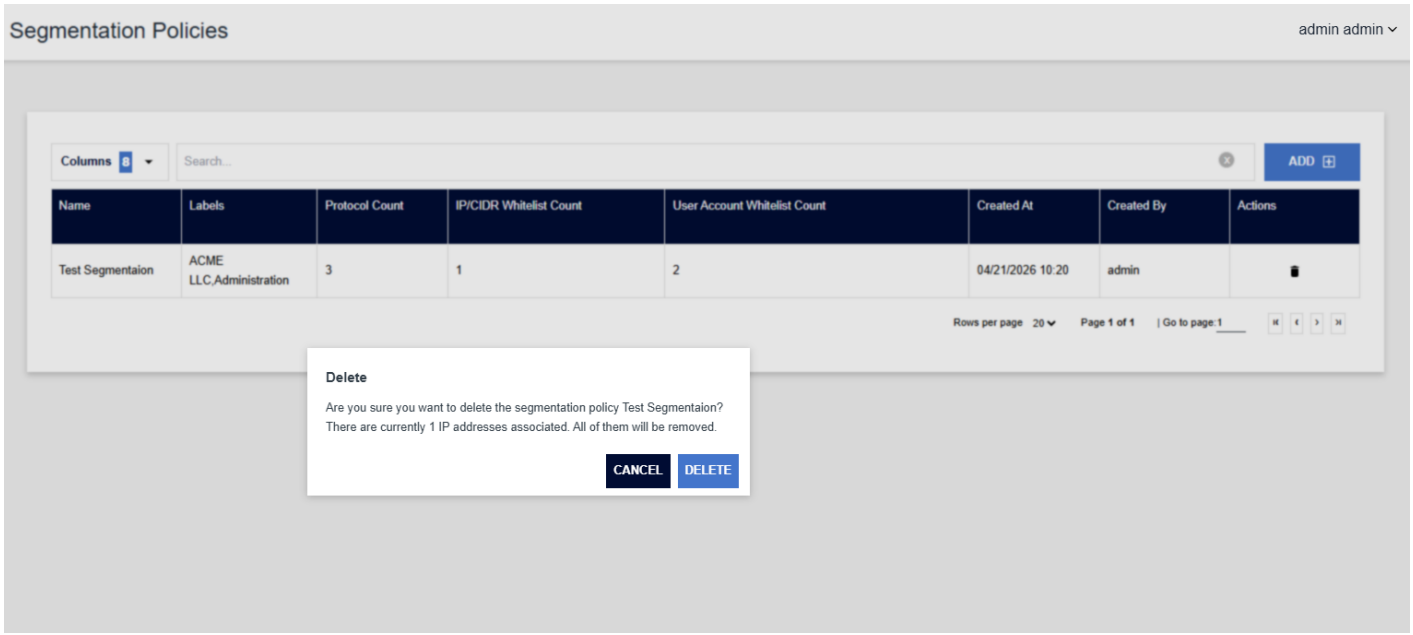
Your newly created Segmentation Policy will now appear in the list, as shown below:



This list displays all Segmentation Policies that have been created and are ready for assessment; because the stored data contains sensitive information and is securely non-retrievable, policies cannot be amended, but you may remove an existing policy and create a replacement if changes are required.

5.7.2 Deleting a Segment

Segmentation Policies can be removed by selecting the Delete icon in the Actions column of the Segmentation Policies list. You will then be prompted to confirm that this is the policy you intend to remove before the deletion is completed.



5.8 Exposure

Exposure Page Overview

The **Exposure** page in Nipper OmniSight provides a high-level visual summary of your device assessment results. It is designed to help you quickly understand the overall security and compliance posture of your environment.

Key Capabilities

- At-a-glance insights into:
  - Number of devices assessed
  - Total findings
  - Critical and high vulnerabilities
- Interactive dashboards covering:
  - Vulnerabilities
  - Compliance frameworks (CIS, PCI, DISA STIG, NIST 800-53)
  - Vendor advisories (e.g., Cisco PSIRT)
- Trend analysis
  - View how your security posture changes over time with 6-month trend charts
- Drill-down functionality
  - Click any chart to navigate directly to detailed reports

Filtering Results

Use labels and match conditions to refine the data displayed:

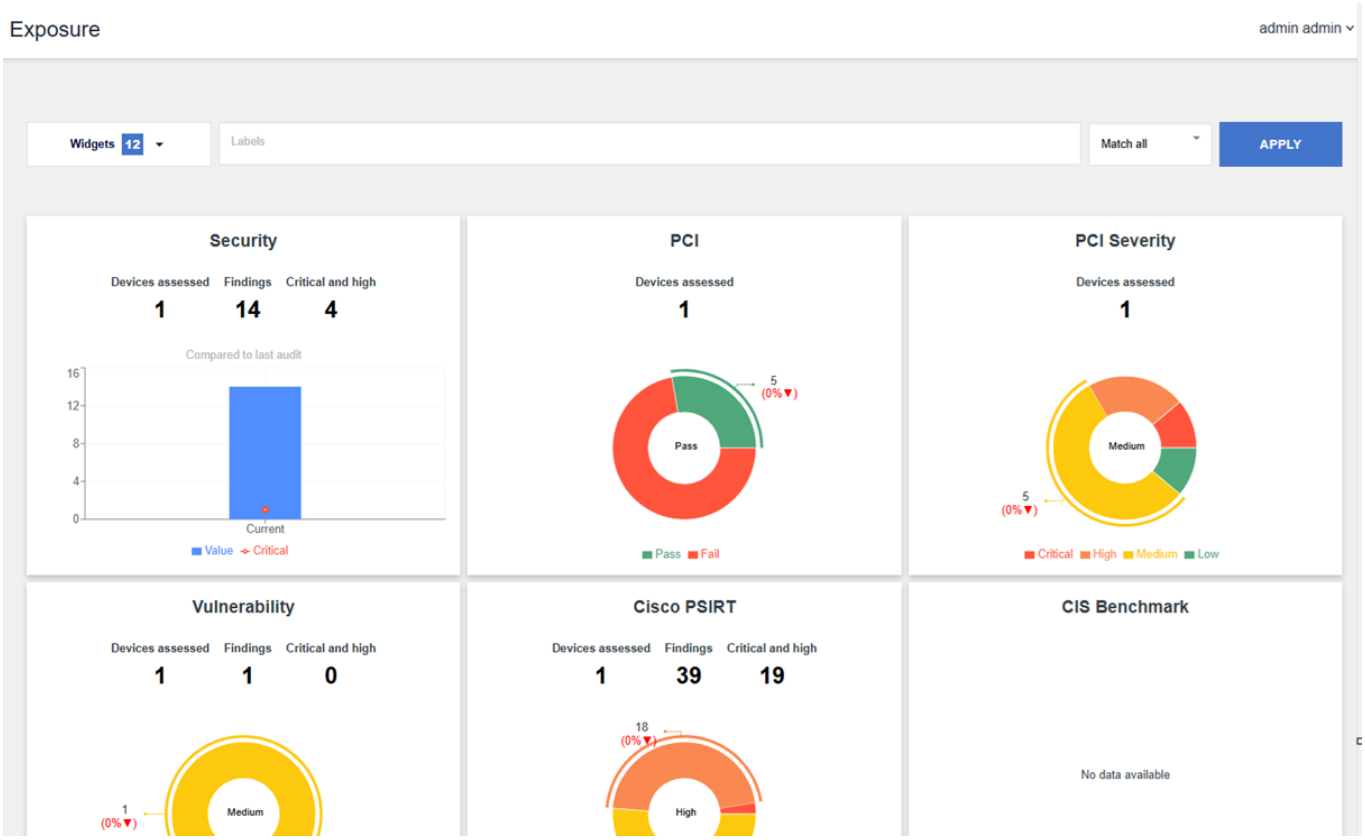
- **Match all** – Shows results containing all selected labels
- **Match any** – Shows results containing at least one selected label
- **Match exact** – Shows results matching the exact label set

Apply filters to focus on specific devices, environments, or assessment scopes.

The Exposure page helps you:

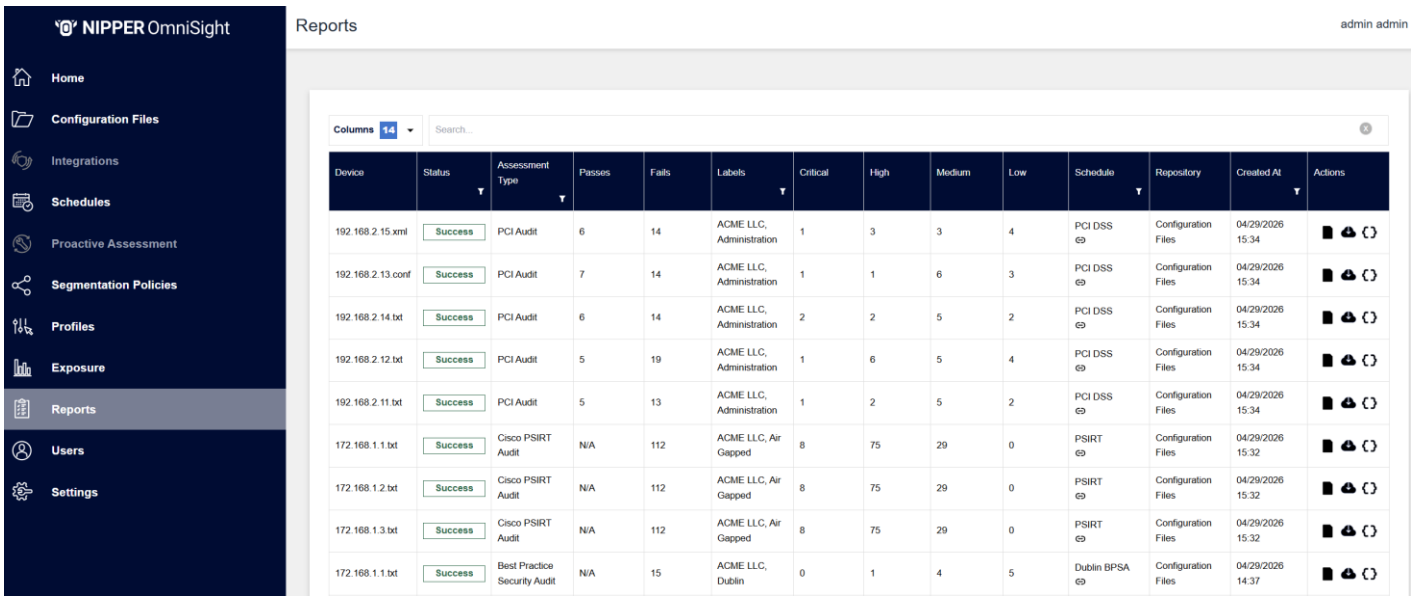
- Quickly identify critical risks
- Monitor compliance status
- Track improvements or regressions over time
- Navigate efficiently to detailed device reports

For more information into these reports, please refer to the following article.



5.9 Reports

The Reports page lists all reports generated from Schedules. From here you can filter, search and view reports generated from device assessments.



Clicking on the **View Reports** icon in the “Actions” column will open that device's assessment report.

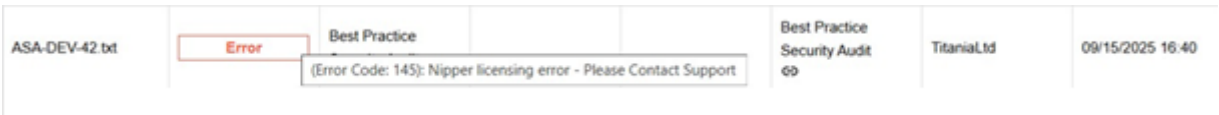
Clicking on the **Download Report** icon in the “Actions” column will download the HTML report file

Clicking on the **Download JSON** icon in the “Actions” column will download the JSON report file

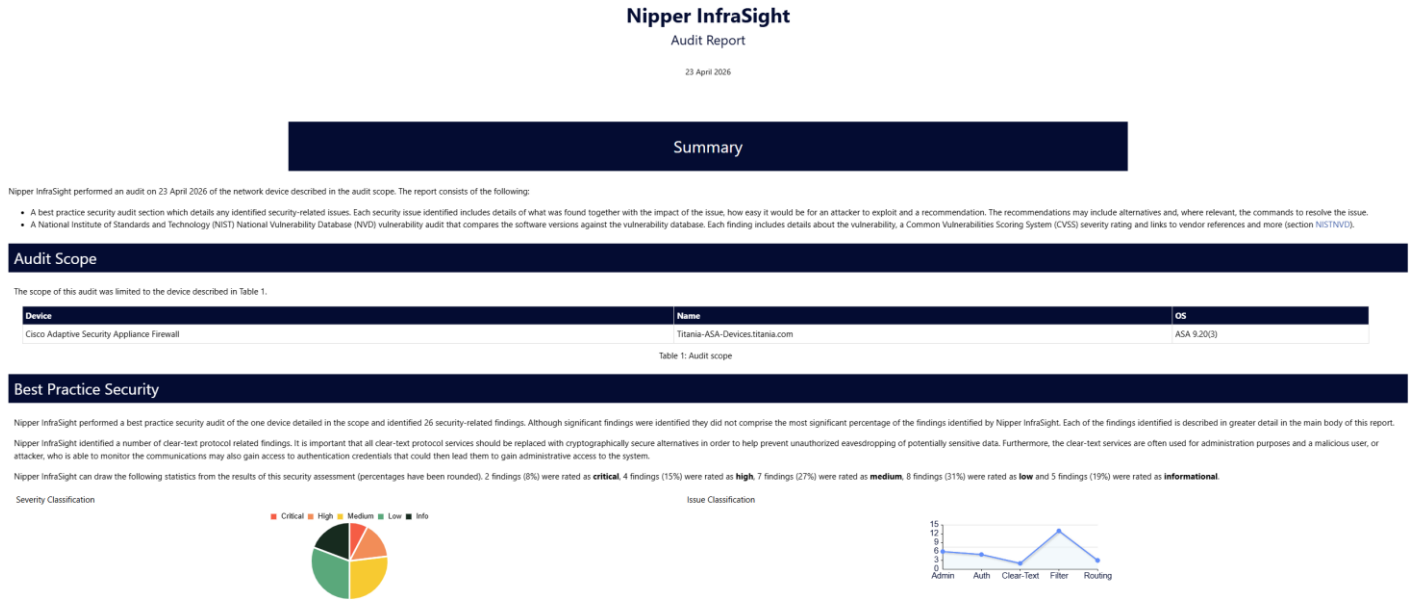
Note: Absence of these buttons indicates the report is not yet generated or has been removed due to a more recent version of the report being available elsewhere within the reports list.

If the assessed device is not detected, an error or feedback message will be displayed under the

'Results' column, which is hidden by default. This column can be toggled using the 'Toggle Column' option on the Report List page. Additionally, users can hover over the status to view the full message in a tooltip



The HTML report will display the complete findings from the assessment performed on the device. Following the top section with the assessment summary is the main body of the report that lists the findings and ways on fixing the issue.



Nipper InfraSight

Audit Report

23 April 2026

Summary

Nipper InfraSight performed an audit on 23 April 2026 of the network device described in the audit scope. The report consists of the following:

- A best practice security audit section which details any identified security-related issues. Each security issue identified includes details of what was found together with the impact of the issue, how easy it would be for an attacker to exploit and a recommendation. The recommendations may include alternatives and, where relevant, the commands to resolve the issue.
- A National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) vulnerability audit that compares the software versions against the vulnerability database. Each finding includes details about the vulnerability, a Common Vulnerabilities Scoring System (CVSS) severity rating and links to vendor references and more (section NISTNVD).

Audit Scope

The scope of this audit was limited to the device described in Table 1.

Device	Name	OS
Cisco Adaptive Security Appliance Firewall	Titania-ASA-Devices.titania.com	ASA 9.20(3)

Table 1: Audit scope

Best Practice Security

Nipper InfraSight performed a best practice security audit of the one device detailed in the scope and identified 26 security-related findings. Although significant findings were identified they did not comprise the most significant percentage of the findings identified by Nipper InfraSight. Each of the findings identified is described in greater detail in the main body of this report.

Nipper InfraSight identified a number of clear-text protocol related findings. It is important that all clear-text protocol services should be replaced with cryptographically secure alternatives in order to help prevent unauthorized eavesdropping of potentially sensitive data. Furthermore, the clear-text services are often used for administration purposes and a malicious user, or attacker, who is able to monitor the communications may also gain access to authentication credentials that could then lead them to gain administrative access to the system.

Nipper InfraSight can draw the following statistics from the results of this security assessment (percentages have been rounded). 2 findings (8%) were rated as **critical**, 4 findings (15%) were rated as **high**, 7 findings (27%) were rated as **medium**, 8 findings (31%) were rated as **low** and 5 findings (19%) were rated as **informational**.

Severity Classification

Issue Classification

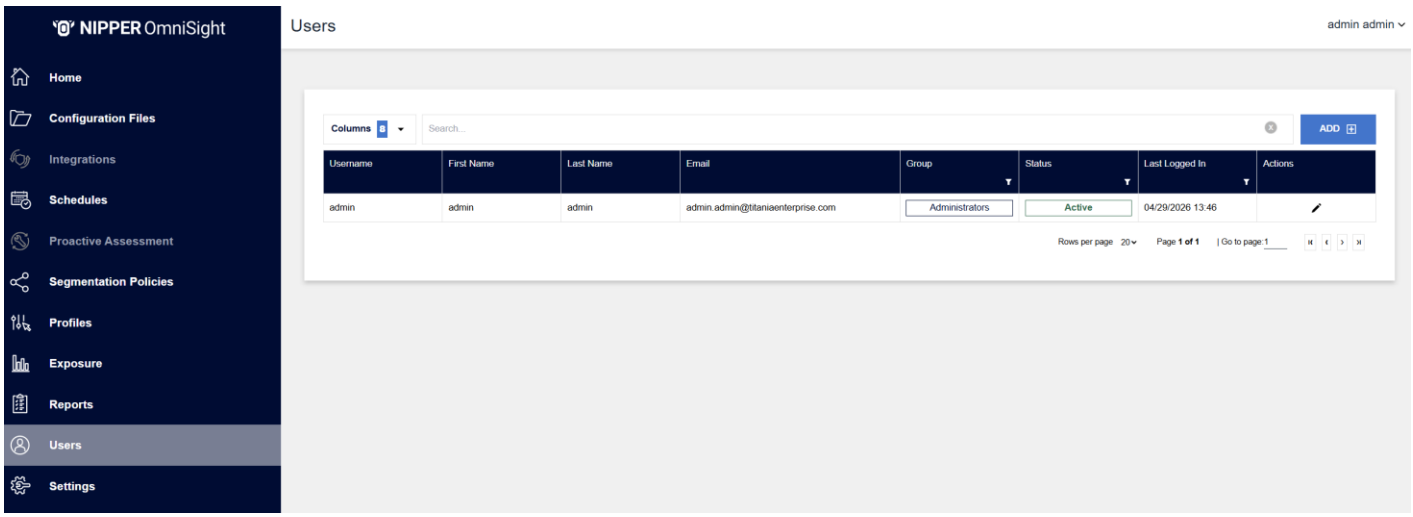
The JSON report contains the same findings information in a JSON structure.


```
{
  "auth": null,
  "id": "2c31808b994d2def01994d9e7431037b",
  "auditOutcome": "SUCCEEDED",
  "errorString": "",
  "metadata": {
    "startTime": 1757943854196,
    "endTime": 1757943857790,
    "product": "Nipper",
    "productVersion": null
  },
  "repositoryDevice": {
    "name": "ASA-DEV-42.txt",
    "description": "Cisco Adaptive Security Appliance Firewall",
    "operatingSystemName": "ASA",
    "operatingSystemVersion": "9.19(1)",
    "repositoryId": "2c31808f994d2c2001994d31bb6a0000",
    "repositoryName": "gitrepository"
  },
  "reportAuditTypes": [
    {
      "type": "Generic",
      "findings": [
        {
          "id": null,
          "auth": null,
          "findingId": "1.4.3",
          "reportTitle": "PCIDSS40Assessment",
          "requirement": "Requirement 1: Install and Maintain Network Security Controls",
          "compliance": "Fail",
          "title": "Testing Procedure 1.4.3",
          "product": "Nipper",
          "description": "Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted
network.",
          "rating": {
            "easeOfExploit": "trivial",
            "easeOfExploitScore": 10,
            "easeOfFix": "quick",
            "easeOfFixScore": null,
            "impact": "high",
            "impactScore": 7,
            "rating": "high",
            "titaniaRating": "Nipper",
```

5.10 User Management

To access the **User Management** section of Nipper OmniSight, click on the Users link in the sidebar menu.

Here you will be presented with a table containing each of the configured users on the system.

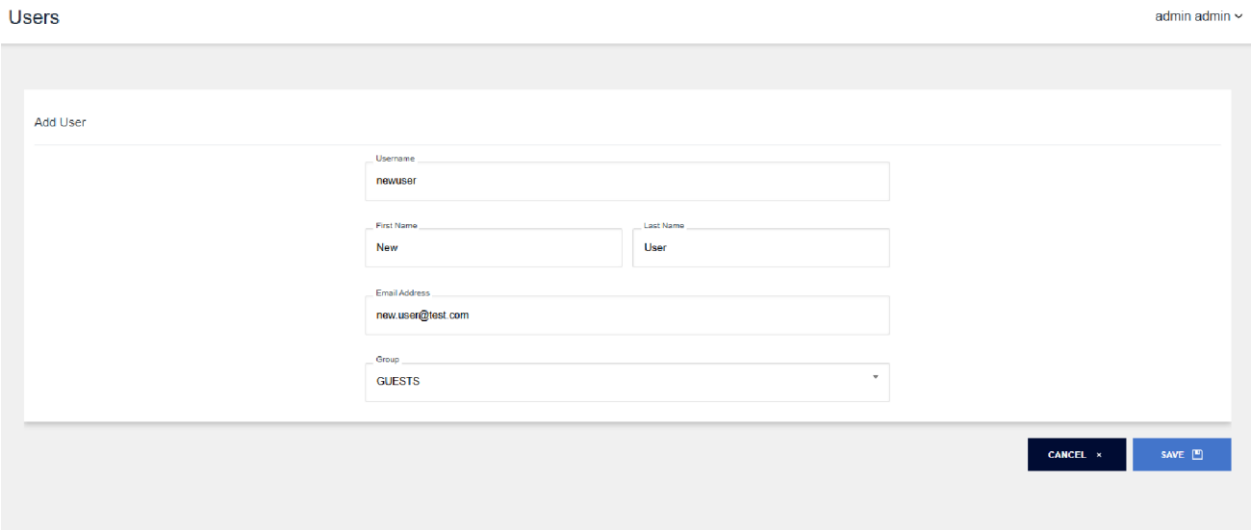


Note: User Management is only available to users in the Administrators group.

5.10.1 Adding a new user

To add a new user to the system, click on the **Add** button.

Once on the Add User page you will be presented with a series of input fields.



You have the option to choose which user group this new user belongs to, the chosen group will determine the privileges the user has.

A user in the **Guest** group:

- May change their own password
- Has read-only access to Configuration Files, Schedules, Segmentation Polices, Profiles, Exposure and Reports

A user in the **Users** group:

- Has the same permissions as a "Guest" user, in addition they have the following permissions
- Has write access to Schedules, Segmentation Polices and Profiles
- Can configure instant and scheduled assessments

A user in the **Administrators** group:

- Has the same permissions as a "Users" user, in addition they have the following permissions.
- Has write access to Configuration Files, Schedules, Segmentation Polices, Profiles and Reports
- Has the ability to view and manage other users' information.
- Has the ability to view and manage settings.

A user in the **NOC** group:

- Has write access to Configuration Files only

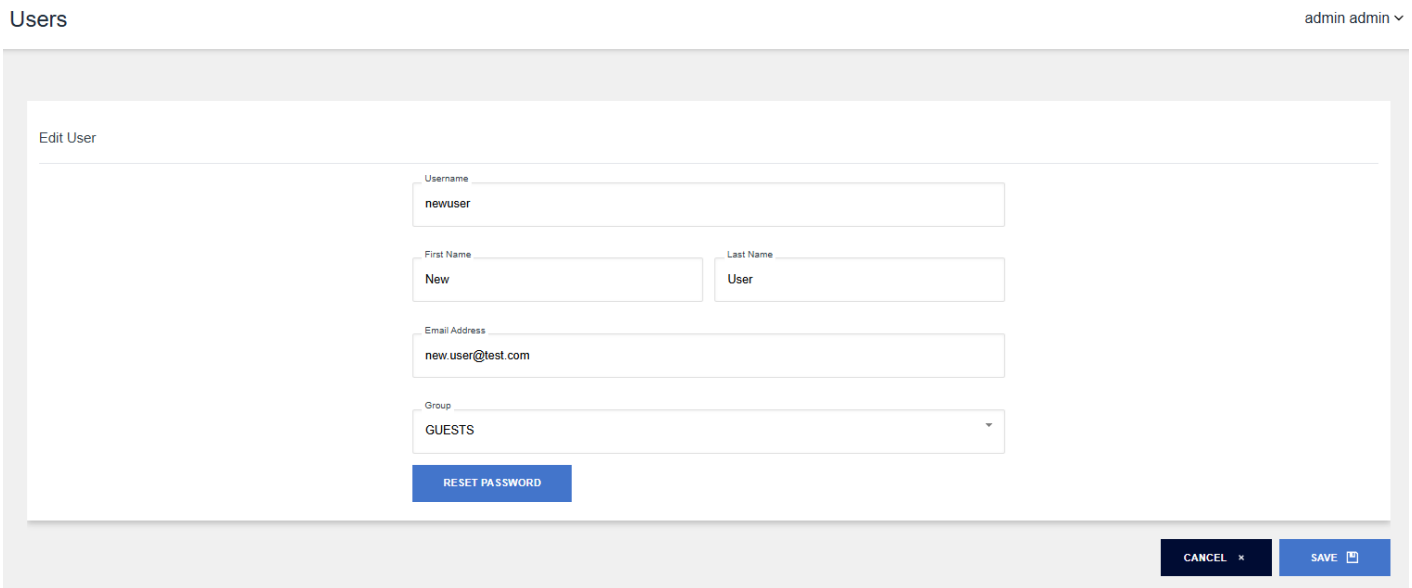
Once all fields have been completed, click **Save**. A window will be displayed showing a generated password for that user. You can copy the username and password to your clipboard by clicking on the **Clipboard** icons to the right of the fields.

Note: when a new user logs into the system for the first time they will be required to change their password.

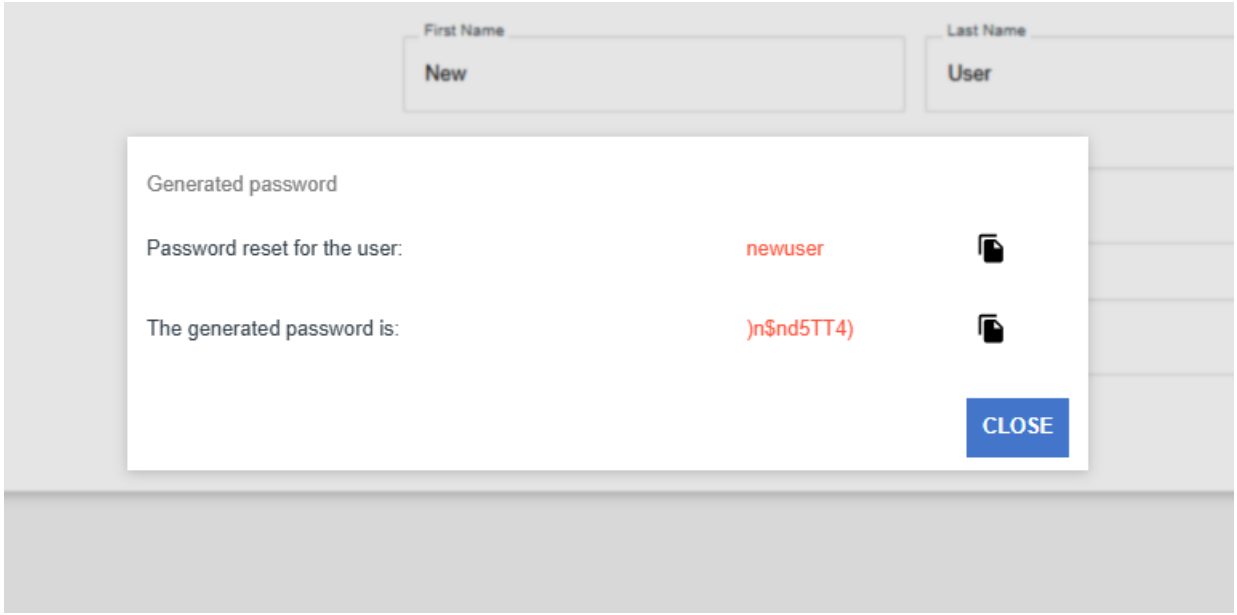
5.10.2 Editing an existing user

To edit an existing user, navigate to the Users table, and click the **Edit** (pencil) icon under "Actions" on the row for the corresponding User that s to be changed.

Here you can change the name or email of the user, the group the user belongs to, or allow the user to reset their password or generate a new two-factor authentication code.



If you reset a user's password, you will see a window with a generated password. Here you can copy the username and password to your clipboard by clicking on the **Clipboard** icons to the right of the fields.

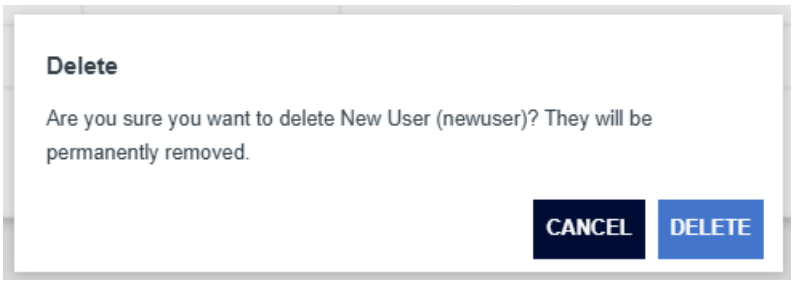


The user will then be prompted to change their password when they next login.

5.10.3 Deleting an existing user

To delete a user from the system, click the **Delete** icon under the "Actions" column on the row for the corresponding User that is to be deleted.

Clicking this delete button will prompt a deletion confirmation dialog, clicking **Delete** will remove the user, whereas clicking **Cancel** will navigate back to the Users table.



Note: Once a user has been deleted, you will no longer be able to add another user with the same username.

5.11 Manage Resources

Nipper OmniSight regularly updates NVD (National Vulnerability Database) and KEV (Known Exploited Vulnerabilities) resources during each product release.

However, the Manage Resources section gives users the ability to upload their own resources, ensuring that Nipper OmniSight is using the most up-to-date vulnerability information available.

Note: Manage Resources is only available to users in the Administrators group.

5.11.1 Resource Types

NIST NVD (CVE) JSON Download

The National Vulnerability Database (NVD) is a U.S. government repository of data relating to vulnerability management. Provided by the National Institute of Standards and Technology (NIST), these files aggregate data from the Common Vulnerabilities and Exposures (CVE) system and include comprehensive vulnerability information such as descriptions, severity ratings (e.g., CVSS scores), affected software versions, and potential remediation steps.

CISA Known Exploited Vulnerabilities (KEV) Catalog

Known Exploited Vulnerability (KEV) files are a curated list of vulnerabilities actively exploited in the wild. Maintained by trusted organizations like the U.S. Cybersecurity and Infrastructure Security Agency (CISA), they focus on quickly highlighting risks that require immediate attention rather than providing exhaustive technical details.

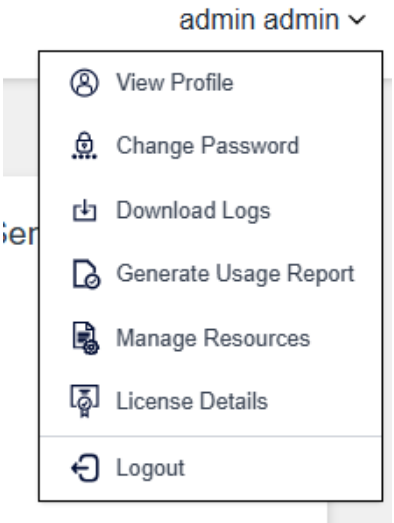
CIS to MITRE ATT&CK Mappings

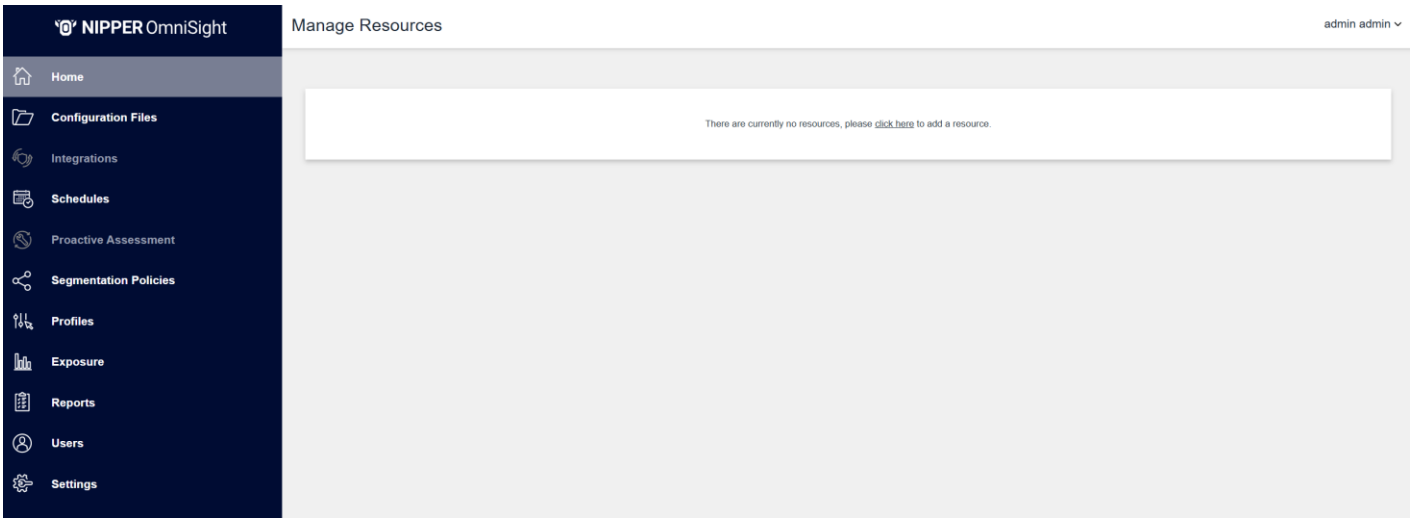
CIS to MITRE ATT&CK Mapping files allow users to upload mappings between CIS Controls and MITRE ATT&CK techniques. These mappings help associate security controls with relevant adversary tactics and techniques, enabling better visibility into how implemented controls support threat detection, mitigation, and defensive coverage analysis.

5.11.2 Adding a New Resource

To upload a resource file, click your username in the top right corner and select Manage Resources.

The Manage Resources page will allow you to upload a resource file into Nipper OmniSight.

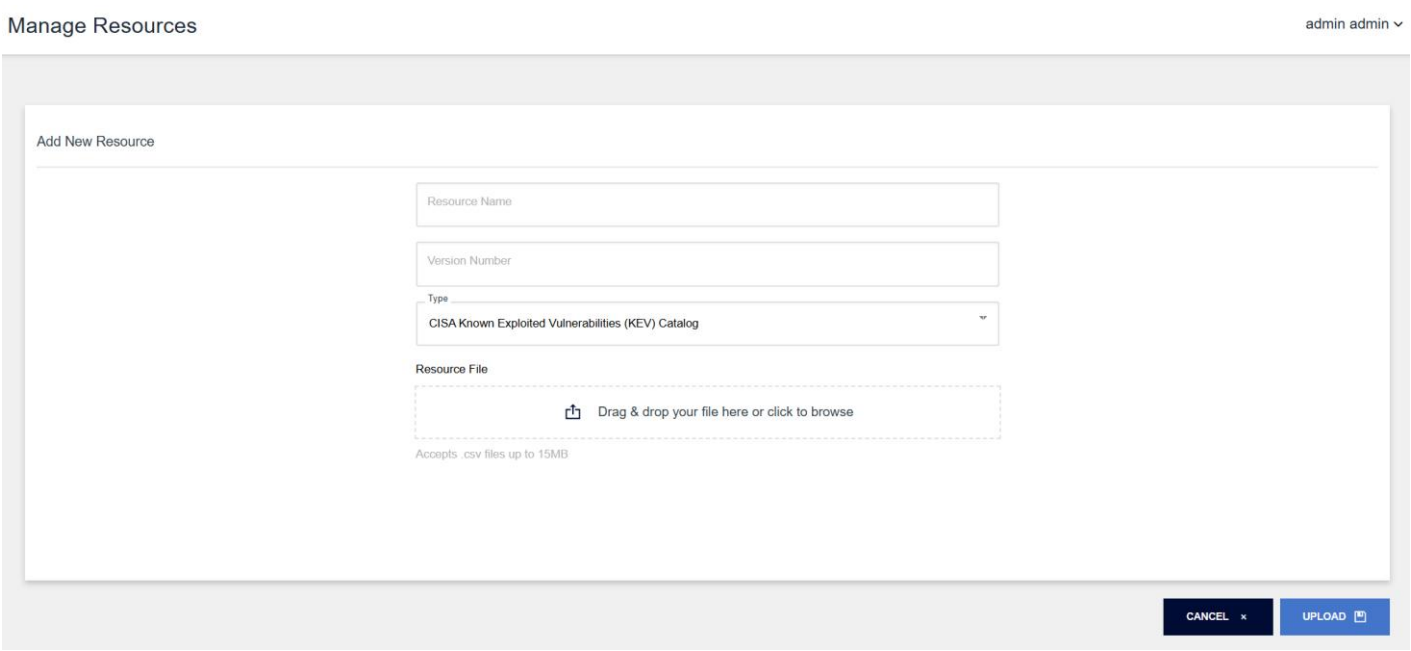




The following fields should be populated:

- **Name**: The name of the resource.
- **Version**: The version of the resource.
- **Type**: The type of resource
- **Upload File**: The resource file you wish to upload.

Note: The resource file size cannot exceed 15MB.

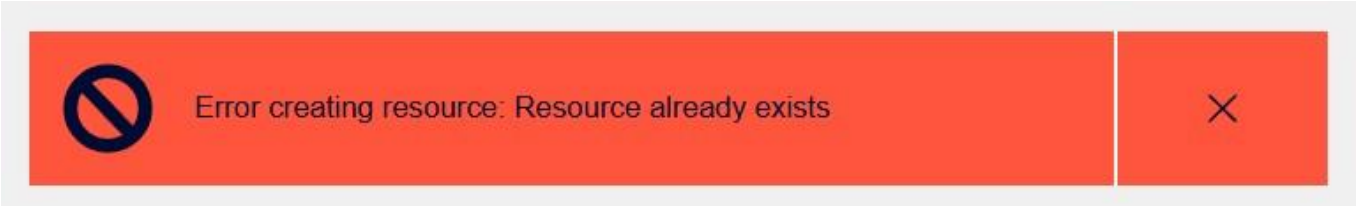


Once the fields are complete and the file has been attached, press the **Save** button to add the resource.

A new card will appear showing the current state of the update. It will begin in a **Pending** state while the upload is in progress.

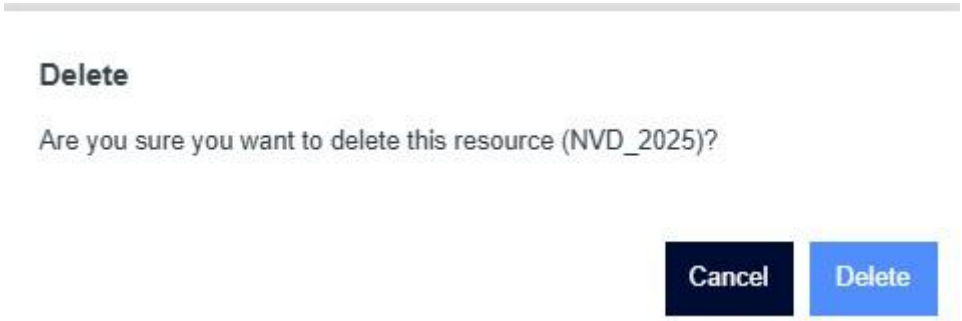
If the upload is successful, the state will change to **Success.**

If you try to upload a resource with the same name as a previously uploaded resource, you will get an error message.

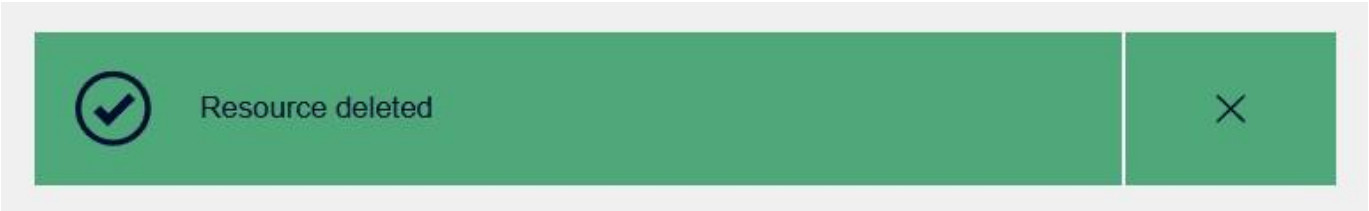


5.11.3 Deleting a Resource

To delete a resource, select the **Delete** icon on the right hand side. This will open a dialog box asking you to confirm your choice to delete. If you wish to proceed, select Delete.



A message will pop up to confirm the resource has been successfully deleted.



5.12 Settings

The settings listed within the settings page apply globally to all users of Nipper OmniSight and can be edited on the Settings page, which can be navigated to by using the link in the sidebar menu.

Here are all the settings that are editable in Nipper OmniSight.

Note: Settings is only available to users in the Administrators group.

Low Disk Space

This value, in GB, sets the threshold below which Nipper OmniSight will start displaying warnings about low disk space. Decimal values may be entered, e.g. 15.7GB.

E.g. if the disk that Nipper OmniSight is on has 14GB free space left and the setting is set to 15GB then a warning will be displayed to all users.

This threshold must be greater than 1GB and greater than or equal to the critical disk space threshold.

Critical Disk Space

This value, in GB, sets the threshold below which Nipper OmniSight will consider disk space to be critical. Decimal values may be entered, e.g. 15.7GB.

E.g. if the disk that Nipper OmniSight is on has 9GB free space left and the setting is set to 10GB then a critical disk space level has been reached.

When the disk space is critical, new assessments will not be performed and a warning will be displayed to all users.

This threshold must be greater than 1GB and less than or equal to the low disk space threshold.

Note: When the system is in a critical state, assessments are disabled.

Retained Assessment Results per Device

This limits how many assessment results are retained for each device within Nipper OmniSight. Assessment results are large so limiting the number stored in Nipper OmniSight can reduce disk usage.

If more assessment results than the limit are generated for a device then the oldest assessment results will be removed keeping only a summary of the assessment results within Nipper OmniSight. For removed assessment results, the reports table will not have the option to view the report.

When assessment results are removed from Nipper OmniSight this does not affect any assessment results that have been sent to SIEMs.

Changing this setting will not cause assessment results to be removed immediately. Assessment results for a device are only removed when a new result is generated for that device.

If the value is set to -1 then an unlimited number of assessment results are retained.

Increasing this setting from a smaller value to a larger value will not restore any assessment results that have been removed due to the previous smaller retention limit.

Reducing this setting from a larger value to a smaller value will require you, when you save, to acknowledge that deletion of assessment results may occur.

How long files to keep files before they are automatically deleted

This setting is how long before uploaded configuration files are automatically deleted. The default value is 24 hours, this can be increased to as high as 168 hours (1 week) or as low as 1 minute.

Saving Settings

When you have made changes, the Save button will be enabled. Clicking this button will cause your changes to be applied.

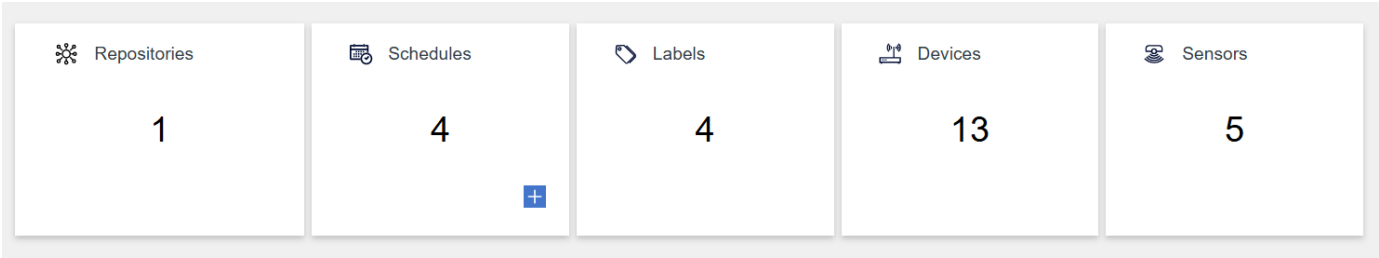
Resetting Changes

If you have made changes to the settings but have not yet saved them you can click the Reset button in the bottom right to return the page to its original state.

5.13 Dashboard

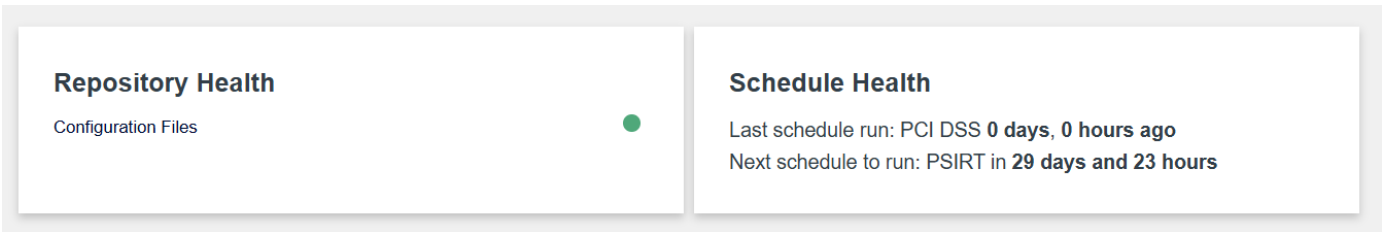
The Nipper OmniSight home screen provides a dashboard overview of key components and assessment information. By default, all widgets shown on the page will automatically update every 10 seconds.

The top widgets show the total number of Schedules, Repositories, Labels, Devices and Sensors set up within Nipper OmniSight. From here, you can navigate to the Add Repositories or Create Schedules pages by clicking on the plus icon within the widget.

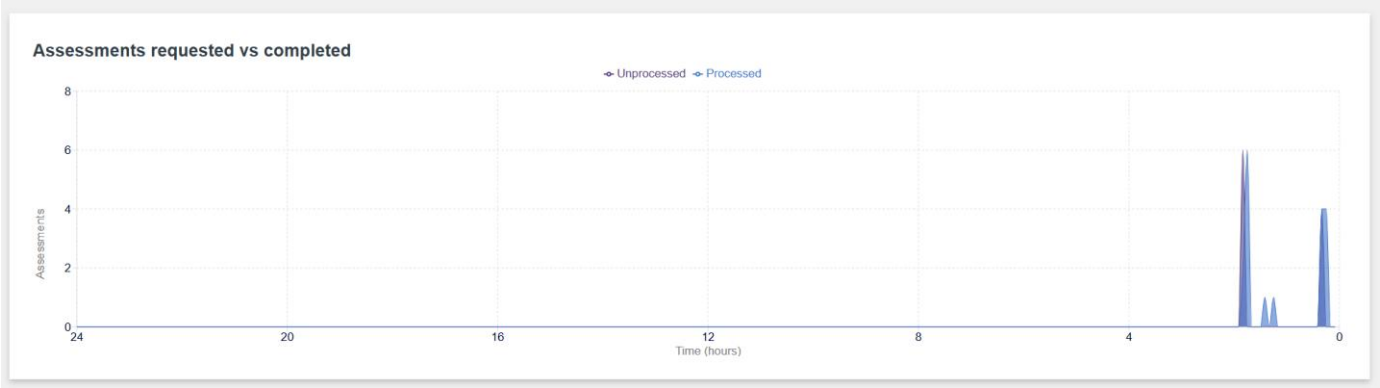


The Repository Health Widget displays all the synced repositories along with their current health status. A green indicator signifies a healthy connection, while a red indicator denotes an unhealthy connection. Users can hover over the status indicator to view more details.

The Schedule Health Widget displays the last run schedule, including its name and execution time, as well as the next scheduled run, if applicable.



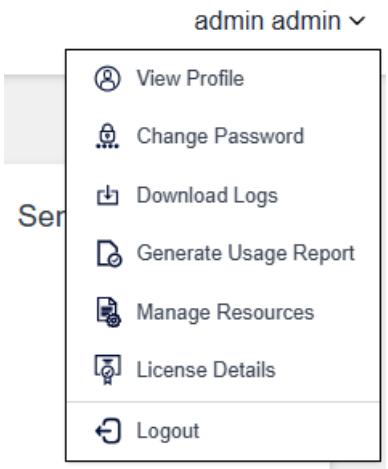
The graph displays the number of assessments requested and the number of assessments completed within a 24 hour time period. The 24 hour graph is split into 5 minute sections.



The report success vs fail bar graph displays the number of successful and failed assessments completed within 24 hours, 1 month, and 1 quarter. The green bar represents the total number of successful assessments, while the red bar represents the total number of failed assessments. Users can click on each bar to open the reports list page, pre-filtered based on the selected time interval and status.

5.13.1 Profile Dropdown

From any page with Nipper OmniSight, if you select the dropdown against the username in the top right of the screen, you will see a number of Profile options.



- **View Profile**: Clicking on View Profile from the Profile dropdown menu, takes you to your User Profile when you can view your name, email address and the group you belong to.
- **Change Password**: You can select Change Password from the Profile dropdown menu, this will navigate you to the Change Password screen.
- **Download Logs**: If you experience issues, such as being unable to create a schedule, and are getting an error back, our Customer Support team may request you download and share the log

file to assist with debugging the issue. To do so, select Download Logs from the Profile dropdown menu and save the downloaded file.

- **Generate Usage Report**: Selecting Generate usage report from the Profile dropdown menu will allow you to download and save a JSON report that will show the following information for the last 12 months:
    - Total number of distinct devices assessed
    - Broken down per month:
        - Number of distinct devices assessed
        - Total Assessments Performed
        - Schedule count
        - Report count per assessment type
        - Report count per device type
- **Manage Resources**: Clicking on Manage Resource from the Profile dropdown menu, takes you to the Add new resource page, you can upload a resource file into Nipper OmniSight using this feature. Please refer to Manage Resources for more details.
- **License Details:** The License Details page lets you see which features are included in your license, along with its current status, activation and expiry dates, and a visual overview of how much of the license is being used.

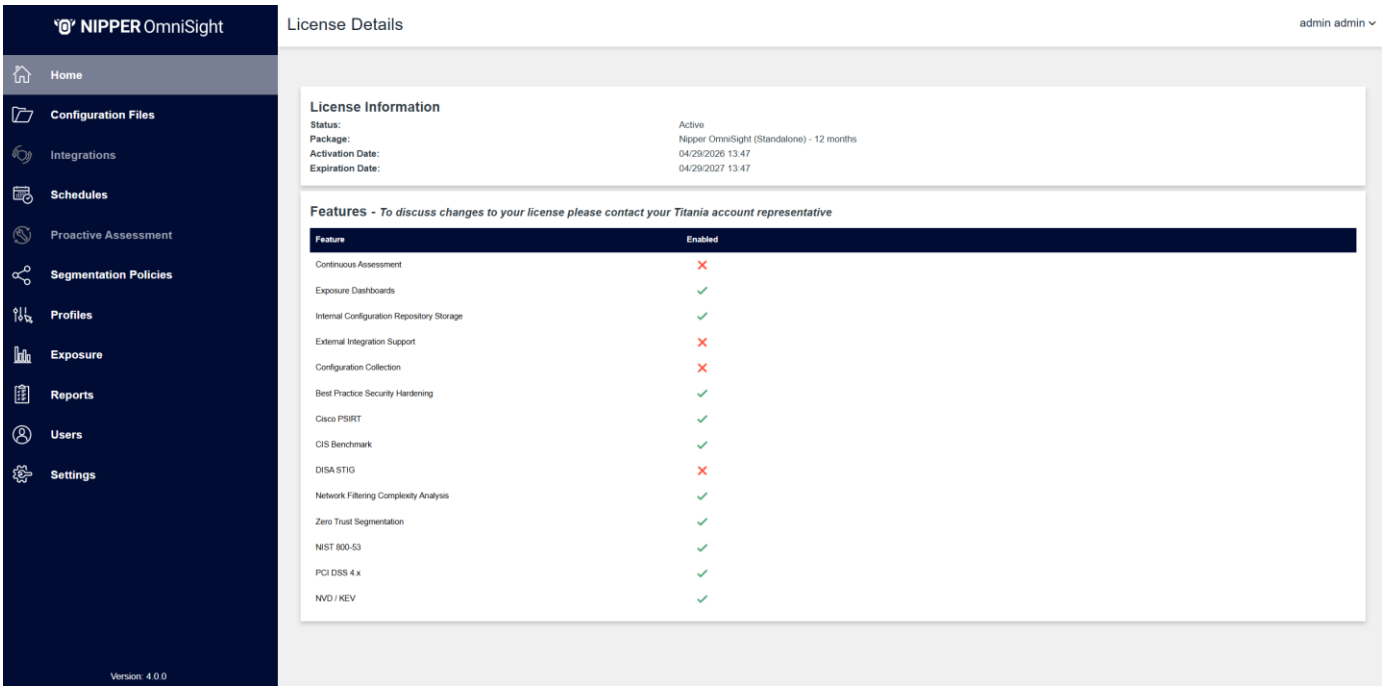
Note: Usage report and Manage Resources are only available to users in the Administrators group.

Download Logs is only available to users in the Administrators group and User group.

5.14 License Details

To view your license details, click your username in the top right corner and select License Details.

The License Details page will allow you to view what Features you have enabled within your license, as well as its status, activation date, and expiration date.


NIPPER OmniSight
License Details
admin admin
Home
Configuration Files
Integrations
Schedules
Proactive Assessment
Segmentation Policies
Profiles
Exposure
Reports
Users
Settings
Version: 4.0.0
License Information
Status: Active
Package: Nipper OmniSight (Standalone) - 12 months
Activation Date: 04/29/2026 13:47
Expiration Date: 04/29/2027 13:47
Features - To discuss changes to your license please contact your Titania account representative
Feature
Enabled
Continuous Assessment
Exposure Dashboards
Internal Configuration Repository Storage
External Integration Support
Configuration Collection
Best Practice Security Hardening
Cisco PSIRT
CIS Benchmark
DISA STIG
Network Filtering Complexity Analysis
Zero Trust Segmentation
NIST 800-53
PCI DSS 4.x
NVD / KEV

Appendix

A. Updating Nipper Omnisight

It is highly recommended to backup the virtual machine using a snapshot before proceeding with any updates to Nipper OmniSight.

The process of updating Nipper OmniSight is very similar to the initial installation.

- A backup of existing data should be generated before updating to the latest version of Nipper OmniSight.
- See Backing Up section for more information.
- Navigate to /opt/app/nipper-omnisight directory.
- Stop Nipper OmniSight using tes.sh stop .
- Upload the provided installer to the app users home directory.

UPLOAD YOUR INSTALLER

Place the installer and nipper installation file nipper.deb that we provided in a directory, navigate to that directory using the command prompt and upload both installer and nipper to VM home directory using the following command

```
scp nipper-resilience-x.x.x-POV.tar ubuntu@<ip address>:~/
scp nipper.deb ubuntu@<ip address>:~/
```

Once the files are successfully uploaded, it's now required to SSH into the VM for further steps. Run the following command

```
ssh ubuntu@<ip address>
```

Now to verify the installation files have been successfully uploaded, run the following command

```
ls -lrt | grep -i "nipper"
```

The output should be similar to the following:

```
ubuntu@ubuntu:~$ ls -lrt | grep -i "nipper"
-rw-rw-r-- 1 ubuntu ubuntu 4857357324 Aug 15 09:17 nipper-resilience-3.11.0-POV.tar
-rw-rw-r-- 1 ubuntu ubuntu  123744820 Aug 15 09:26 nipper.deb
ubuntu@ubuntu:~$
```

For security purposes we would need to place these installers in the app user's home directory and set the right permissions, so that only the app user is allowed to install and run Nipper OmniSight. Run the following commands to change the ownership and group to the app user:

```
sudo chown app:app nipper-resilience-x.x.x-POV.tar
sudo chown app:app nipper.deb
```

Now to verify the owner/group has changed from ubuntu to app, run the following command:

```
ls -lrt | grep -i "nipper"
```

The output should be similar to the following:

```
ubuntu@ubuntu:~$ ls -lrt | grep -i "nipper"
-rw-rw-r-- 1 app    app    4857357324 Aug 15 09:17 nipper-resilience-3.11.0-POV.tar
-rw-rw-r-- 1 app    app     123744820 Aug 15 09:26 nipper.deb
ubuntu@ubuntu:~$
```

After setting up the desired permissions move the files to the app user's home directory

```
sudo mv nipper-resilience-x.x.x-POV.tar /opt/app
sudo mv nipper.deb /opt/app
```

/opt/app by running the following command

To perform the next set of steps you would need to switch to the app user. To do this run

```
sudo su - app
```

Before installing Nipper OmniSight, we need to extract the installer, to do this run:

tar -xvf nipper-omnisight-x.x.x-POV.tar

As the nipper-omnisight directory should already exist, this will overwrite any files already present.

INSTALLING

Once the extraction is complete, it's now time to copy the nipper installation file nipper.deb to the right place, to do this run the following command. cp /opt/app/nipper.deb /opt/app/nipper-omnisight/docker/provisioning/nipper

Optional: If you would like to install your own SSL certificates for accessing the application please follow the instructions on SSL Setup

- Navigate to /opt/app/nipper-omnisight directory and run sudo ./install.sh .
- This will follow the same process in checking that all required packages are installed, before prompting you to set various configuration options.
- If a backup file is detected at /opt/app/backup/backup.tar.gz during the installation process, you will be prompted with an option to either:
    - Proceed with the backup to restore previous data, or
    - Skip the backup and continue with a fresh installation.
- Make your selection based on whether you want to retain the previous data or start fresh.

- After install.sh is successfully run, Nipper OmniSight will start - this process can take a few minutes.

B. Backing Up and Restoring Nipper OmniSight

Backing up your Nipper OmniSight instance will allow you to revert to a previous state upon restore.

The backup file size should be relatively small, but there will be automated checks to ensure you have sufficient disk space before beginning the process.

The following data will be included in the backup:

- Database data
- Configuration files
- SSL Certificates (Optional)
- Logs (Optional)

BACKING UP

- Ensure Nipper OmniSight is running, and no assessments are currently in progress
- Navigate to the scripts directory
- cd /opt/app/nipper-omnisight/scripts
- Run the backup script
  ./backup.sh
- Follow the on-screen prompts to select which data to back up
- If the backup process is successful, the backup will be saved in /opt/app/backup/backup.tar.gz

RESTORING

If you are restoring as part of a Nipper OmniSight update please refer to Installing section for more information.

- Ensure Nipper OmniSight is not running
- Ensure the backup file is located at /opt/app/backup/backup.tar.gz
- Navigate to the Nipper OmniSight installation directory
- cd /opt/app/nipper-omnisight
- Run the install script
  - sudo ./install.sh

- Follow the on-screen prompts, selecting that you would like to restore from the backup file
- If the restore process is successful, Nipper OmniSight will begin with the backed-up data

ADDITIONAL NOTES

All existing data will be overwritten when a restore is performed.

Reports are not backed up, only the report history. Users should download any reports they wish to keep before performing the backup.

Telephone: (+44) 1905 888 785

Technical Support: support@titania.com

Published March 2025.