nemasis®

Vulnerability Management Suite

# Pro

# Vulnerability Assessment

## User Guide

Product Version: 22.0.1000.123

Document Version: NVA-UG-2201

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. This User Guide may include typographical errors, technical or other inaccuracies.

MicroWorld does not offer any warranty to this User Guide's accuracy or use. Any use of the User Guide or the information contained therein is at the risk of the user.  This User Guide may contain links to websites of other companies or organizations that MicroWorld does not own or control. MicroWorld neither evaluates nor makes any representations regarding the accessibility of these websites. MicroWorld reserves the right to make changes without any prior notice. No part of this User Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Technologies Incorporated.

The terms MicroWorld, MicroWorld logo, Nemasis, and Nemasis logo are trademarks of MicroWorld. All other product names referenced in this User Guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the trademarks and names of others.

The product described in this User Guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

| | |
|---|---|
| **Technical Support:** | support@nemasisva.com |
| **Sales:** | sales@nemasisva.com |
| **Live Chat:** | http://www.nemasisva.com/english/livechat.asp |
| **Printed By:** | MicroWorld Technologies Incorporated |
| **Date:** | August, 2021 |

# Content

# Introduction

The Nemasis PRO is a Vulnerability Management Suite that detects vulnerabilities in your network and provides an accurate solution to fix it. It assists you in managing your organization's overall governance, risk, and compliance with regulations. Nemasis PRO automates point-in-time assessments to help quickly detect and fix vulnerabilities across a variety of operating systems, devices, databases, firmware, and applications, including software flaws, missing patches, malware, open-ports, active services, and misconfigurations.

Nemasis PRO is ideally designed for the organizations and security consultants who need unlimited assessments and configurable reports along with a fast and easy way to proactively fix vulnerabilities. It is designed to keep you and your organization safe from the cybersecurity threats and make sure you are protected 24x7. Below we have mentioned key features of Nemasis PRO:

- Scan the endpoints connected across the network for vulnerabilities.
- Report the vulnerabilities found and provide accurate solutions to fix them.
- Monitor the security status of the endpoints in the organization.
- Create and manage scan tasks for endpoints.
- Send customized alerts and reports of scan tasks according to your preferences.
- Inform about open ports, malicious applications, or services running on systems connected across a network.

As technology is evolving, so are the threats. But with Nemasis PRO at your hand, we are sure that your organization operations will run fluid smooth. The Nemasis PRO follows the best industry security compliances and regulatory frameworks that will help you strengthen your IT security, improve productivity, and accomplish business goals within time.

# Scope and Purpose

The purpose of this User Guide is to provide readers an understanding of the Nemasis PRO Vulnerability Management Console and guidance on the best way to use it. This User Guide will prove useful for whoever is involved in developing, monitoring, or learning about the Nemasis PRO.

The User Guide covers processes of creating a scan target, running the scan task, generating the report, and fixing the discovered vulnerabilities. If you are familiar with managing vulnerabilities, the User Guide will be easy to understand. If you are not familiar, please read more about it on the Internet as this User Guide does not offer in-depth information.

It is recommended that you read this User Guide side by side as you operate the Nemasis PRO console. Please note that this User Guide does not cover the installation process. If you want to read about the installation process, download the Installation Guide by clicking **here**.

# Supported Platforms/Browsers

**Supported Devices/Systems / Heterogeneous Platforms/ applications**

- Network devices
- Virtual Systems: VMware, Microsoft Hyper-V, and Oracle Virtual Box
- Operating systems: Windows, Mac, and Linux
- Databases: Oracle and SQL Server
- Web applications: Web servers, web services, OWASP Top 10 vulnerabilities
- IPv4/hybrid networks

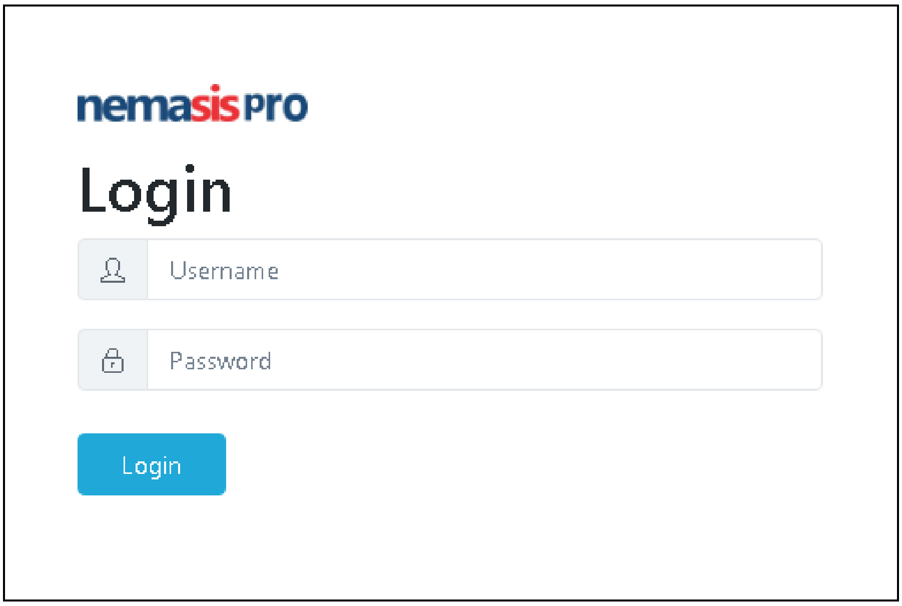
**Browsers (with HTML5 support)**

- Google Chrome (Recommended)
- Mozilla Firefox
- Mozilla Firefox ESR
- Safari

# Login

To log in to the Nemasis PRO console, follow the steps given below:

1. Launch a web browser.
2. Enter the following URL:
   https://<IP address of the Nemasis PRO installed system>:10442
   Nemasis PRO console login page appears.



nemasis PRO

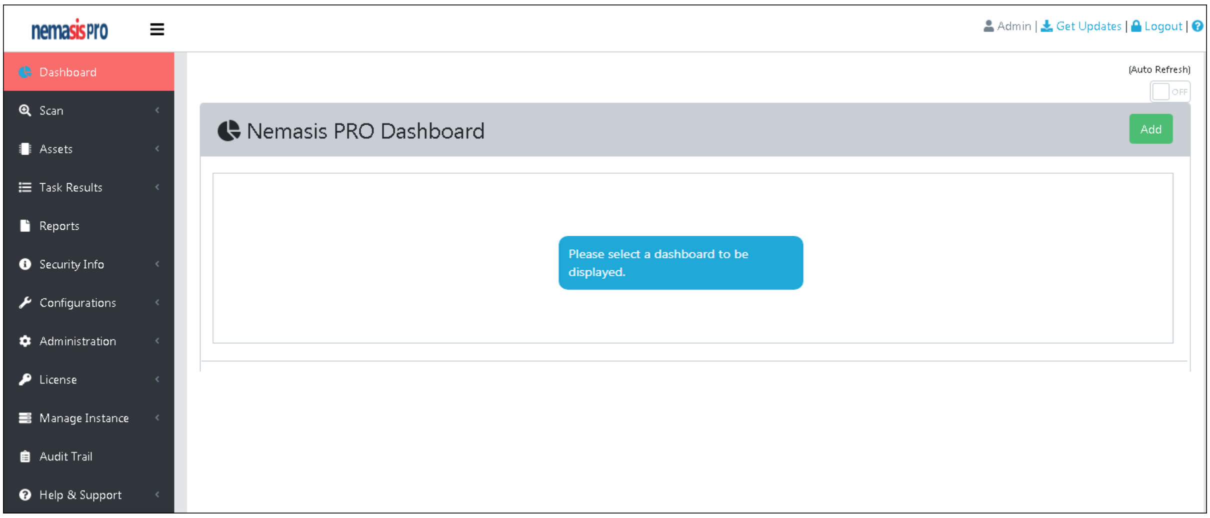
Login

Username

Password

3. Enter the default login credentials.
   **Username** – admin
   **Password** – admin
4. Click **Login**.

After logging in to the Nemasis PRO, following screen appears:



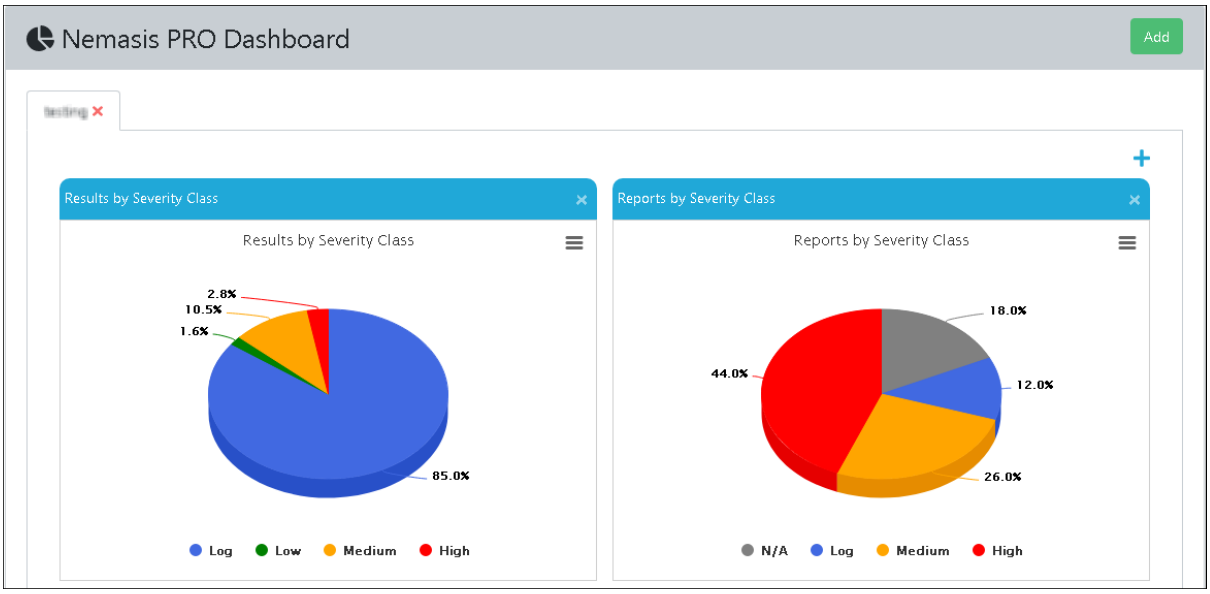
Please select a dashboard to be displayed.

The console tree on the left side displays the following modules:

- **Dashboard**
- **Scan**
- **Assets**
- **Task Results**
- **Reports**
- **Security Info**
- **Configuration**
- **Administration**
- **License**
- **Manage Instance**
- **Audit Trial**
- **Help & Support**

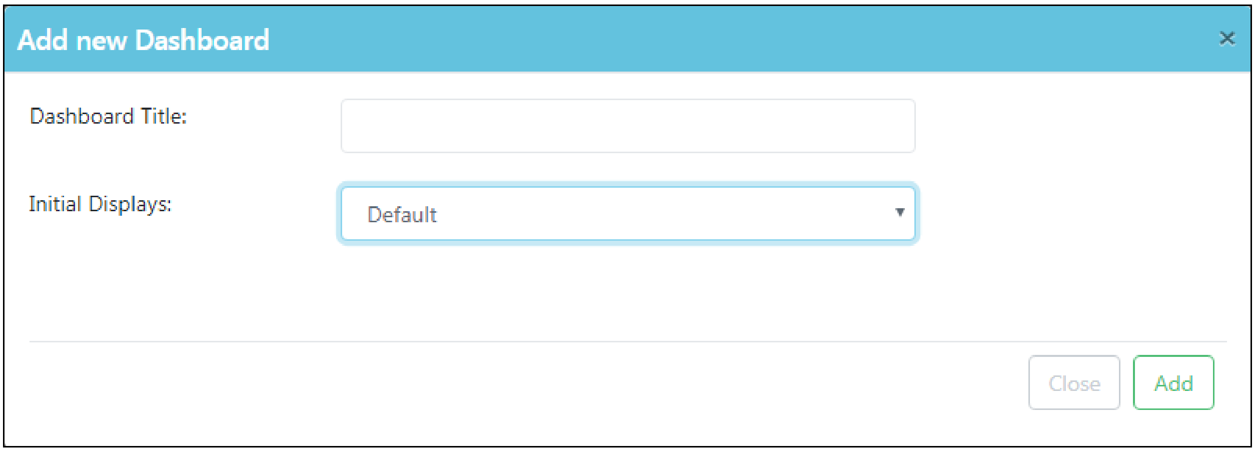
# Dashboard

The Dashboard module displays overall scan results in the interactive pie, bar, and line charts. By clicking in pie and bar charts a user can view the specific information.


Nemasis PRO Dashboard
Add
testing
+
Results by Severity Class
Results by Severity Class
2.8%
10.5%
1.6%
85.0%
● Log ● Low ● Medium ● High
Reports by Severity Class
Reports by Severity Class
18.0%
44.0%
12.0%
26.0%
● N/A ● Log ● Medium ● High

# Adding a Dashboard

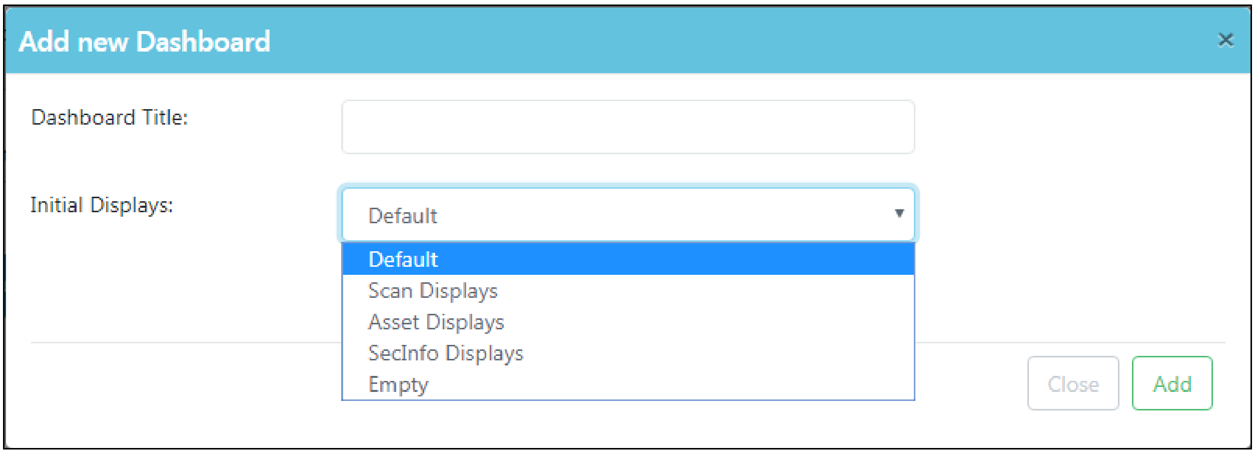
1. In the upper right corner, click **Add**.
   Add a new Dashboard pop-up window appears.



Dashboard Title:

Initial Displays: Default

2. Enter a name in the **Dashboard Title** field.
3. Click **Initial Displays** dropdown, select the preferred display, and then click **Add**.



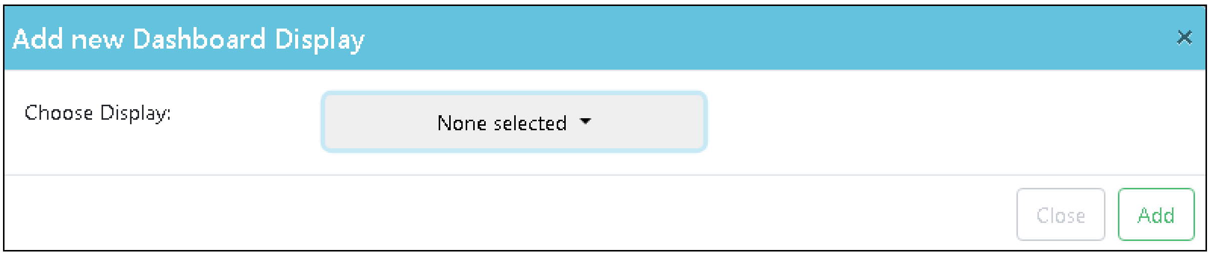
Dashboard Title:

Initial Displays: Default

The new Dashboard display will be added to the Dashboard.

# Adding a Display to Dashboard

1. In the Dashboard display, at the upper right corner, click +.
   Add new Dashboard Display prompt appears.



Add new Dashboard Display

Choose Display: None selected

2. Click **Choose Display** dropdown, select the required display, and then click **Add**.
   The new Dashboard display will be added to the Dashboard.

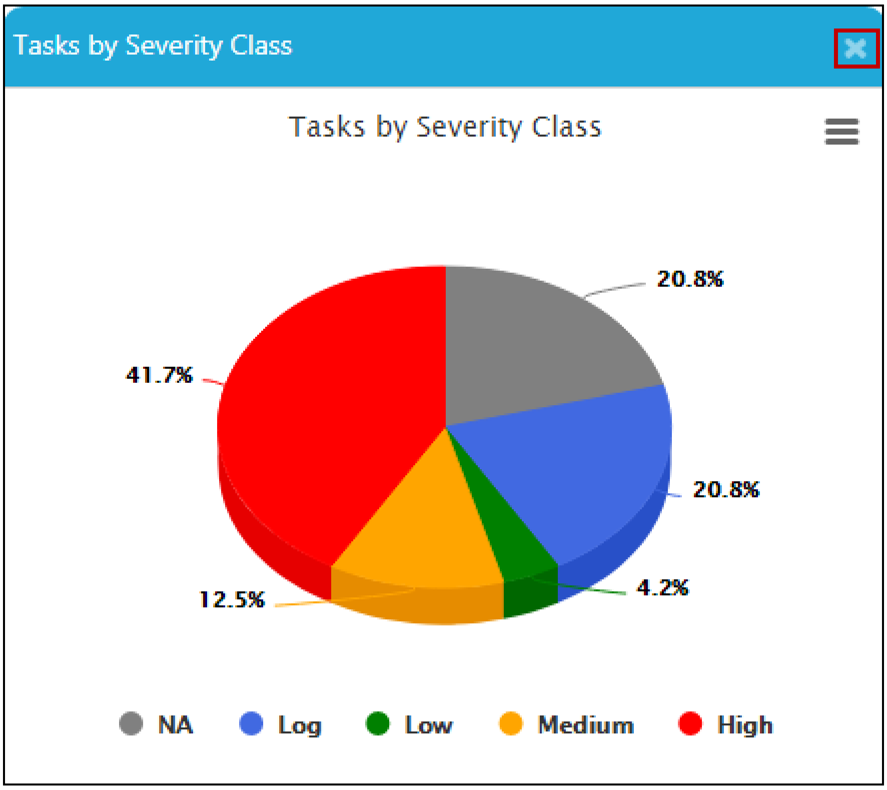
   Following displays can be added to the Dashboard:

   - Tasks by Status
   - Results by Severity Class
   - Reports by Severity Class
   - Reports with High Results
   - Tasks by Severity Class
   - Tasks by CVSS
   - Tasks by Most High Results
   - Tasks by High Results per host
   - Reports by CVSS
   - Results by CVSS
   - Results Description Word Cloud
   - Results Vulnerability Word Cloud
   - Vulnerabilities by CVSS
   - Vulnerabilities by Hosts
   - Vulnerabilities by Severity Class
   - Hosts by CVSS
   - Hosts by Modification Time
   - Hosts (High) by Modification Time
   - Hosts by Severity Class
   - Hosts by Topology
   - Most Vulnerable Hosts
   - Operating Systems by CVSS
   - Operating Systems by Severity Class
   - Most Vulnerable Operating Systems
   - Plugins by CVSS
   - Plugins by Family
   - Plugins by Severity Class
   - Plugins by Detection Threshold
   - Plugins by Detection Threshold Type
   - Plugins by Creation Time

- OVAL Definitions by Class
- OVAL Definitions by Creation Time
- OVAL Definitions by CVSS
- OVAL Definitions by Severity Class
- CVEs by Creation Time
- CVEs by CVSS
- CVEs by Severity Class
- CVEs by Creation Time
- CPEs by CVSS
- CPEs by Severity Class

## Deleting a Display from Dashboard

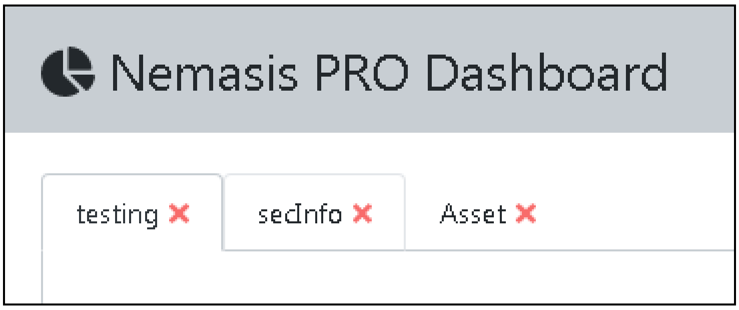
1. In a display, click ☒.



The display will be deleted from the Dashboard.

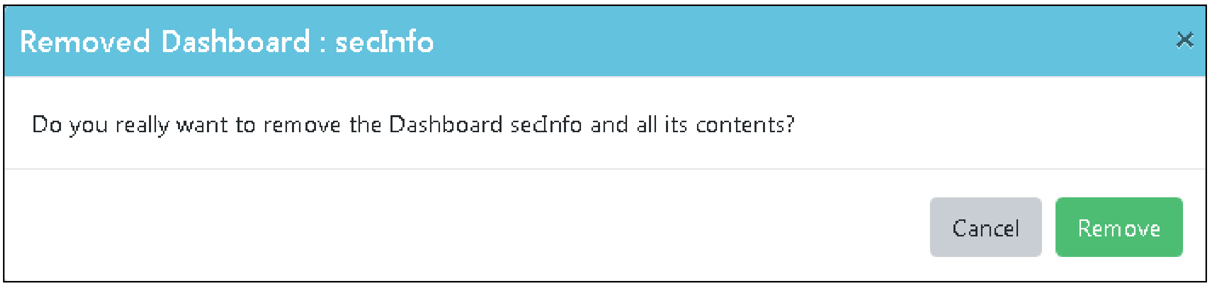
# Removing a Dashboard display

1. To remove a Dashboard display, click ✖.



Nemasis PRO Dashboard

A confirmation prompt appears.

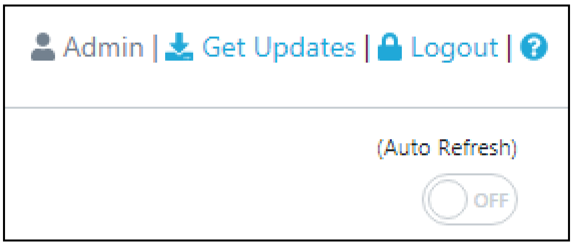


Removed Dashboard : secInfo

Do you really want to remove the Dashboard secInfo and all its contents?

2. Click **Remove**.
   The Dashboard display will be removed.

In the top right corner, there are additional options.



**Get Updates**

Clicking **Get Updates** will initiate the download of a new database for Nemasis PRO.

**Logout**

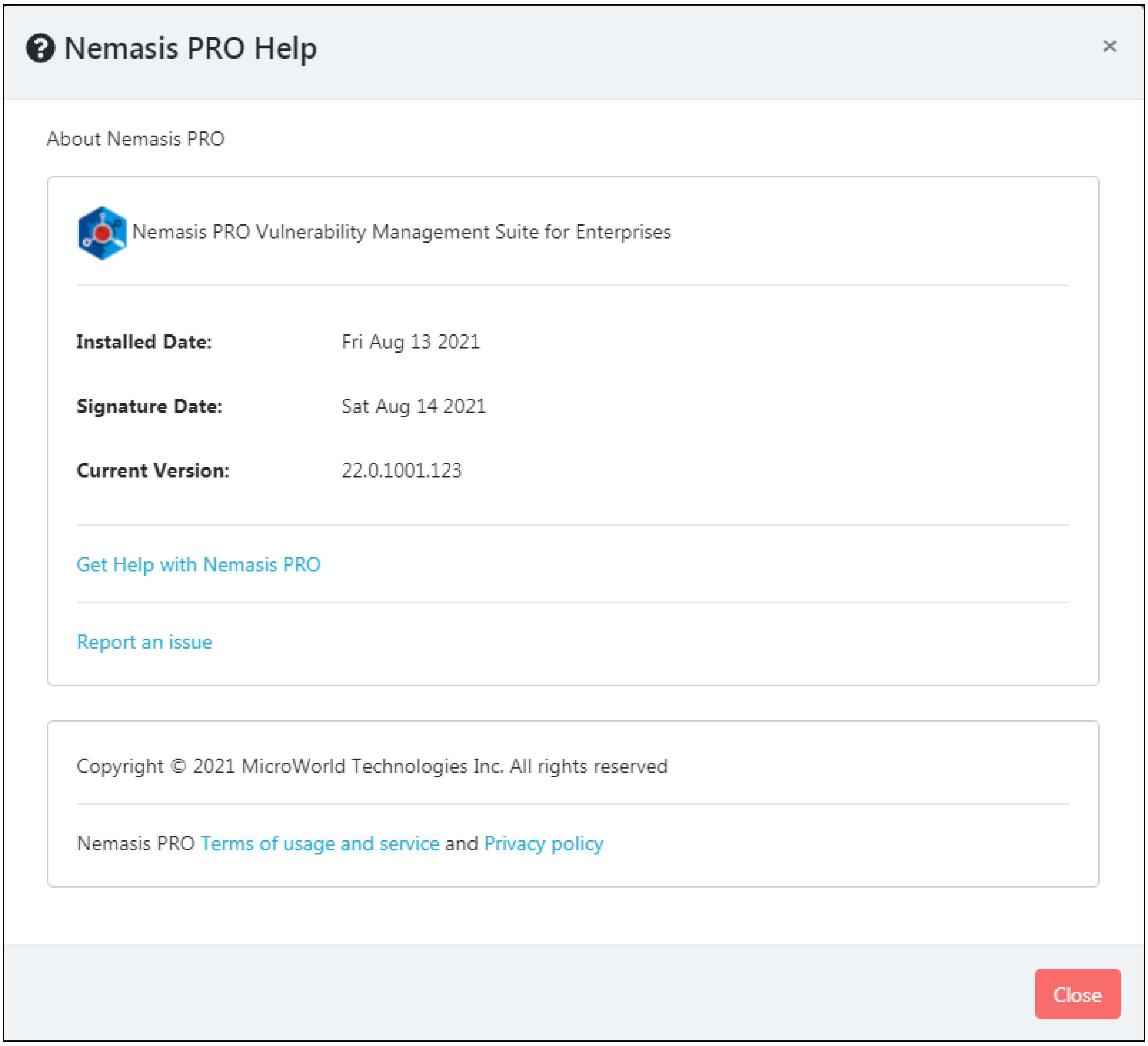
Clicking **Logout** will log you out of the Nemasis PRO console.

### Auto Refresh

Clicking the toggle will enable auto-refresh feature. The Dashboard displays will be refreshed after every scan task is completed.

### Nemasis PRO Help ?

Clicking ? displays the Nemasis PRO Help pop-up.



Nemasis PRO Help

About Nemasis PRO

Nemasis PRO Vulnerability Management Suite for Enterprises

| | |
|---|---|
| **Installed Date:** | Fri Aug 13 2021 |
| **Signature Date:** | Sat Aug 14 2021 |
| **Current Version:** | 22.0.1001.123 |

Get Help with Nemasis PRO

Report an issue

Copyright © 2021 MicroWorld Technologies Inc. All rights reserved

Nemasis PRO Terms of usage and service and Privacy policy

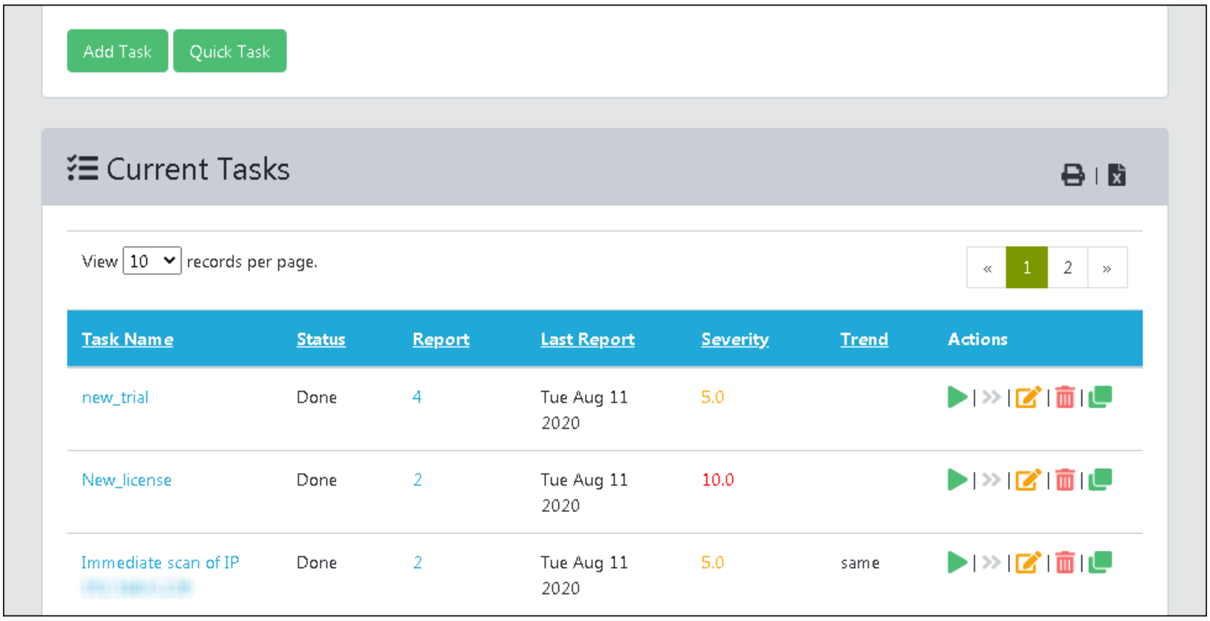
The pop-up displays Nemasis PRO Installed Date, Signature Date and the Current Version in use. By clicking **Get Help with Nemasis PRO** you get redirected to Nemasis PRO webpage containing Help Documentation and a link to Chat Support. If you are facing any issue with the Nemasis PRO, click **Report an issue**. You will be redirected to the Nemasis PRO Support webpage where you can report your issue and get it solved quickly. You can also read about the Nemasis PRO's **Terms of Usage and Service** and **Privacy Policy** by clicking the respective links.

# Scan

The Scan module lets you run a scan task for finding vulnerabilities in the endpoints. It contains three submodules namely **Task**, **Quick Task**, and **Advanced Quick Task**.

## Task

The Task submodule displays the list of current tasks. The Status column displays whether a task is In Progress, Paused, or Done. You can view the task progress and check its report while the scanning is in process.



| Task Name | Status | Report | Last Report | Severity | Trend | Actions |
|---|---|---|---|---|---|---|
| new_trial | Done | 4 | Tue Aug 11 2020 | 5.0 | | ▶ \| » \| ✎ \| 🗑 \| ⧉ |
| New_license | Done | 2 | Tue Aug 11 2020 | 10.0 | | ▶ \| » \| ✎ \| 🗑 \| ⧉ |
| Immediate scan of IP [redacted] | Done | 2 | Tue Aug 11 2020 | 5.0 | same | ▶ \| » \| ✎ \| 🗑 \| ⧉ |

The Severity column displays the severity level of the completed tasks. The severity level is color-coded for their ratings:

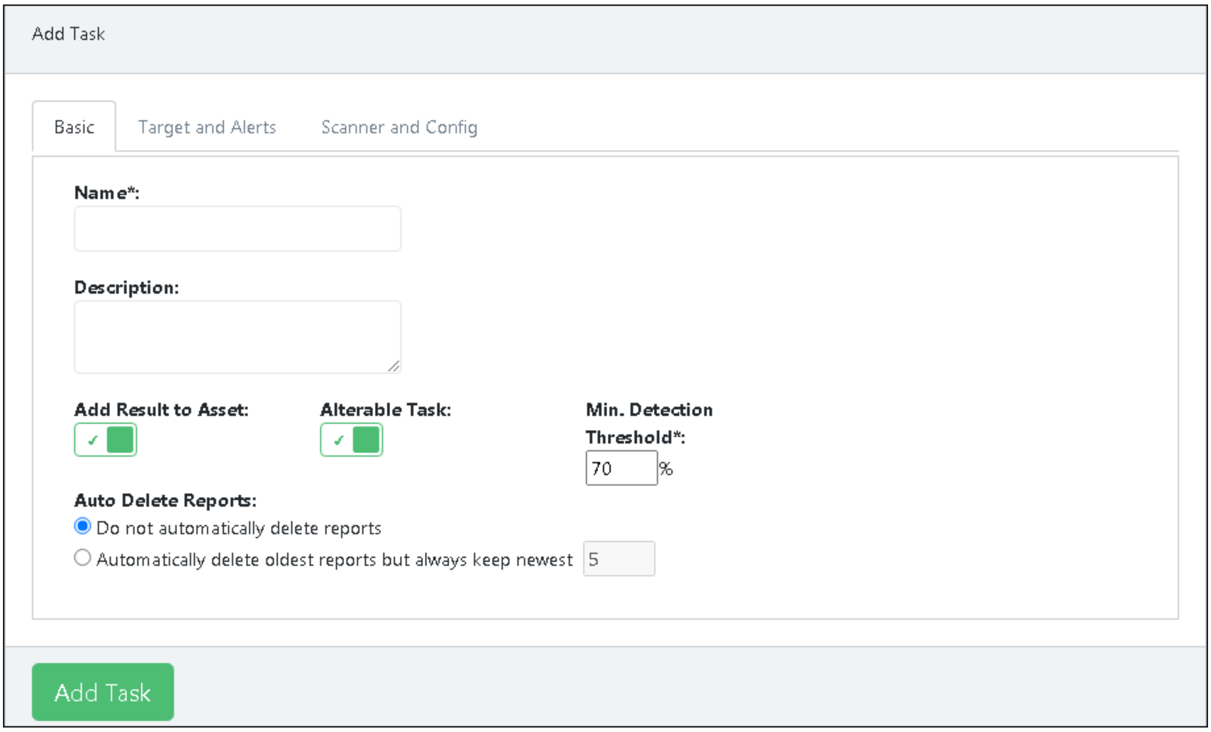
- Severity **Low** –ranges from 1 to 4
- Severity **Medium** –ranges from 4.1 to 7.0
- Severity **High** –ranges from 7.1 to 10

The Trend column displays the vulnerability comparison result of the latest scan with the last scan. For example, if fewer vulnerabilities are found after the task is re-run, the Trend column will display **down**. Whereas if more vulnerabilities are found after the task is re-run, the Trend column will display **up**. If similar vulnerabilities are found after the re-run, the Trend column will display **same**.

# Adding a Task

To add a Task, click **Add Task.**

Add Task form appears on the right pane.



Add Task

Name*:

Description:

Add Result to Asset: ✓

Alterable Task: ✓

Min. Detection Threshold*: 70 %

Auto Delete Reports:

● Do not automatically delete reports

○ Automatically delete oldest reports but always keep newest 5

In the Add New Task, there are three tabs available.

- **Basic**
- **Targets and Alerts**
- **Scanner and Config**

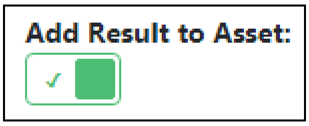
## Basic

The Basic tab has the following options:

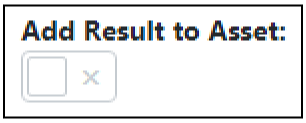
**Name:** Enter the task name in this field.

**Description:** Enter the task description in this field.

**Add Result to Asset:** This feature lets you add the task result to the Assets module. By default this option is enabled, you can disable it based on your preference.

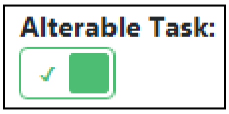


Add Result to Asset:
✓

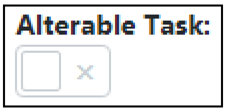


Add Result to Asset:
✕

**Alterable Task:** This feature lets you modify a task even if the report for the same task is already generated. If the tasks are altered, there will be no consistency amongst task reports.



Alterable Task:
✓



Alterable Task:
✕

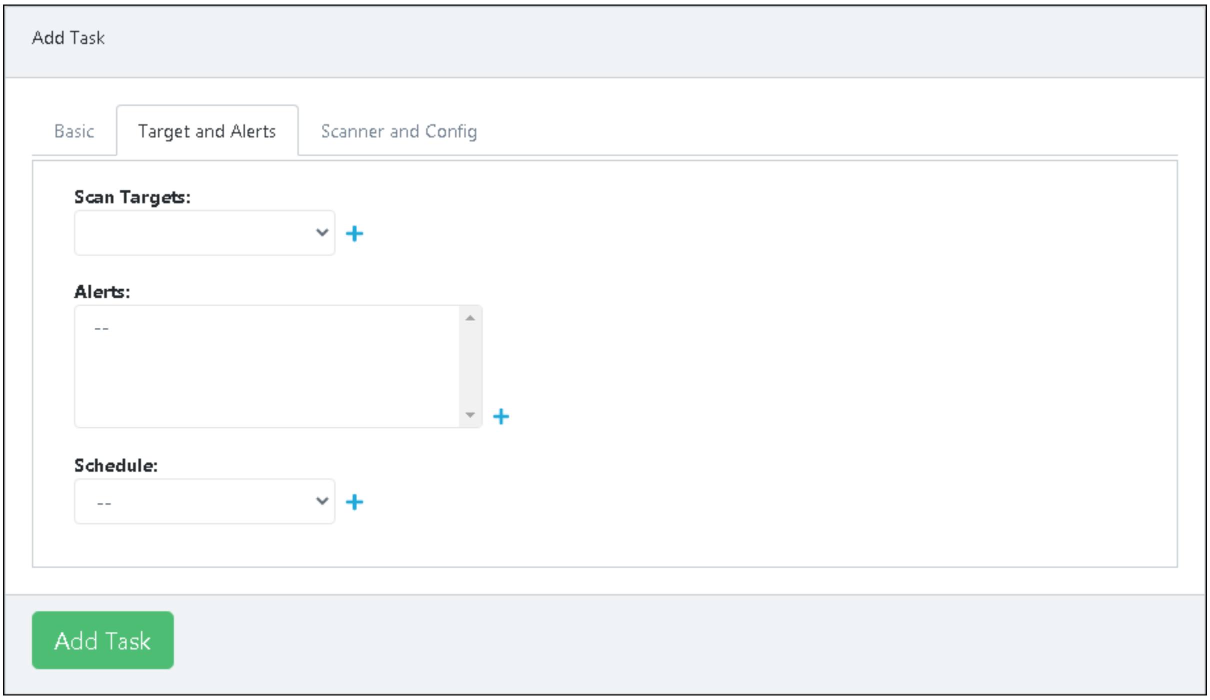
**Min Detection Threshold:** This feature lets you specify quality for the addition of the results to the asset database.

**Auto Delete reports**

- **Do not automatically delete reports** – By selecting this option, Nemasis PRO will not delete the task reports. You will have to delete each task report manually. By default, this option is selected.
- **Automatically delete oldest reports but always keep newest** – By selecting this option you enable Nemasis PRO to auto-delete old reports. You can specify the maximum number of task reports to be stored. If the count exceeds, the task reports will be automatically deleted in the reverse-chronological order.

# Targets and Alerts

The Targets and Alerts tab is explained below.



Add Task

Scan Targets:

Alerts:

--

Schedule:

--

### Scan Targets

Click the dropdown and select the appropriate Target. To add a new Target from the tab, click +. Learn more about Targets by clicking **here**.

### Alerts

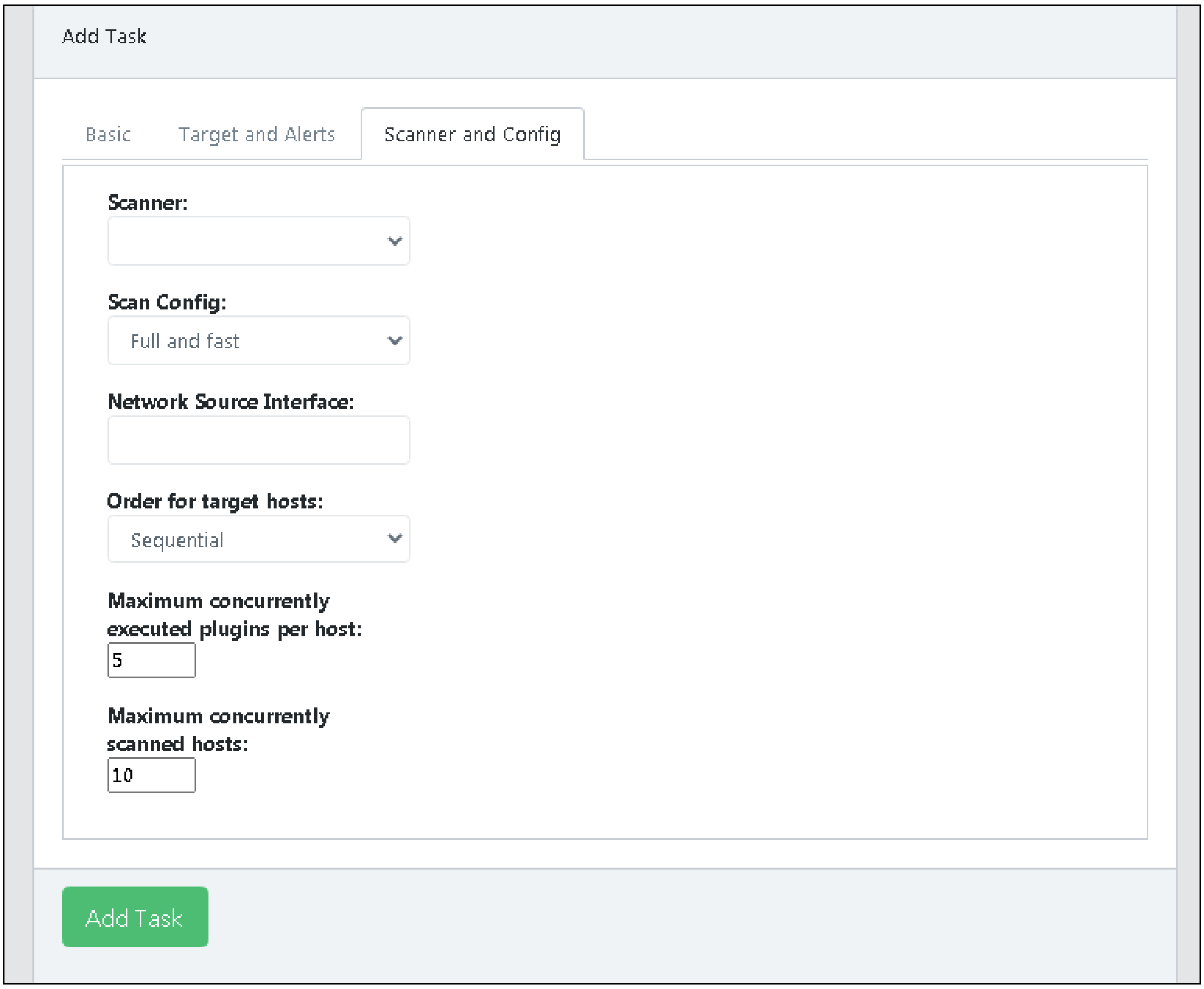
Select the appropriate Alert from the list. To add a new alert from the tab, click +. Learn more about Alerts by clicking **here**.

### Schedule

Click the dropdown and select the appropriate Schedule. To add a new schedule from the tab, click +. Learn more about Schedule by clicking **here**.

# Scanner and Config

The Scanner and Config tab is explained below.



Add Task

Scanner:

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

Maximum concurrently executed plugins per host: 5

Maximum concurrently scanned hosts: 10

## Scanner

Click the dropdown and select the appropriate Scanner.
Learn more about Scanner by clicking here.

## Scan Config

Click the dropdown and select the appropriate Scan Config.
Learn more about Scan Config by clicking here.

## Network Source Interface

Enter the network source interface of the Nemasis PRO for the scan.

**Order for target hosts**

You can select the search type for a specified network area. Click the dropdown to select from the following options:

- Sequential
- Random
- Reverse

For example, if you are scanning a network 192.168.0.0/24 consisting of many systems at the beginning or end of the IP address range. By selecting Random mode, the progress view will be more meaningful.

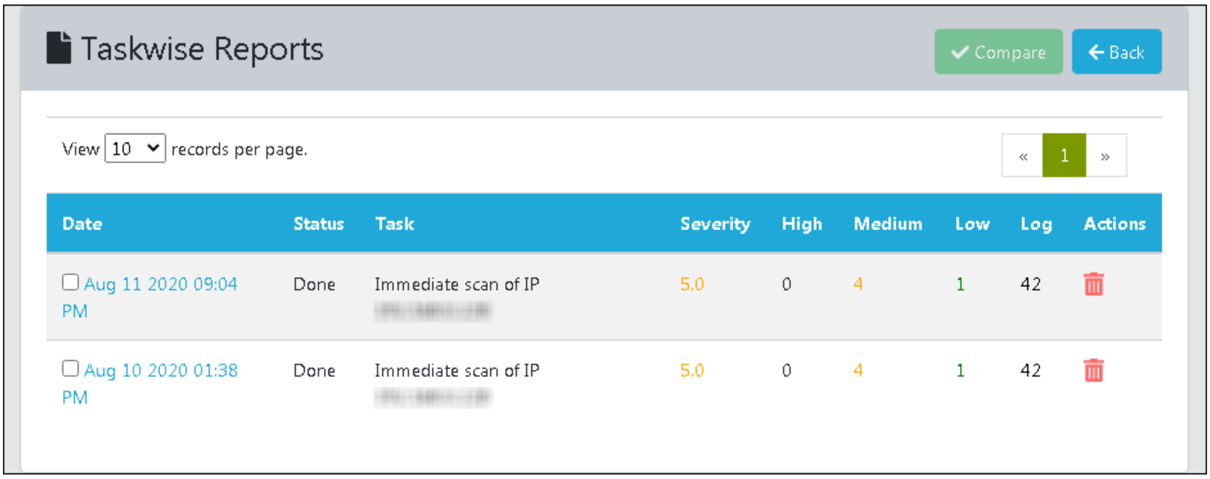
**Maximum concurrently executed plugins per host / Maximum concurrently scanned hosts**

You can specify the maximum number of Scan Plugins that will scan a Target concurrently. The default number of Scan Plugins is chosen with the utmost care. If a system is scanned with more Scan Plugins concurrently or a scan is run for multiple systems at the same time, the target systems, the network, or the Nemasis PRO appliance may face a negative impact. You can edit the maximum Scan Plugins and Scanned Hosts value.

## Comparing Reports

To compare reports of a task after it is re-run, follow the steps given below:

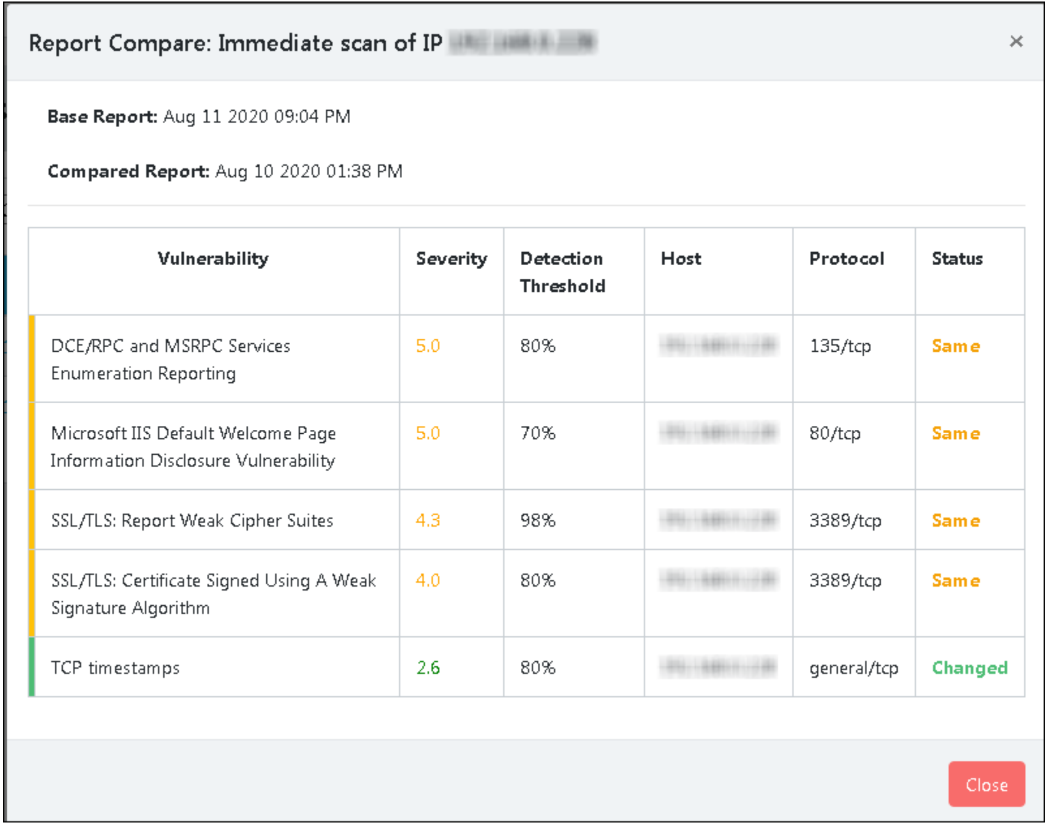
1. Click the numerical value in **Reports** column.
   Taskwise Reports page appears.



Taskwise Reports

| Date | Status | Task | Severity | High | Medium | Low | Log | Actions |
|---|---|---|---|---|---|---|---|---|
| □ Aug 11 2020 09:04 PM | Done | Immediate scan of IP [redacted] | 5.0 | 0 | 4 | 1 | 42 | 🗑 |
| □ Aug 10 2020 01:38 PM | Done | Immediate scan of IP [redacted] | 5.0 | 0 | 4 | 1 | 42 | 🗑 |

2. In this comparison, the first report selected will be the **Base Report**, while the next selected report will be the **Compared Report**. Ensure the correct selection sequence and then in the upper right corner, click **Compare**.
   Report Compare pop-up appears.



Report Compare: Immediate scan of IP [redacted]

**Base Report:** Aug 11 2020 09:04 PM

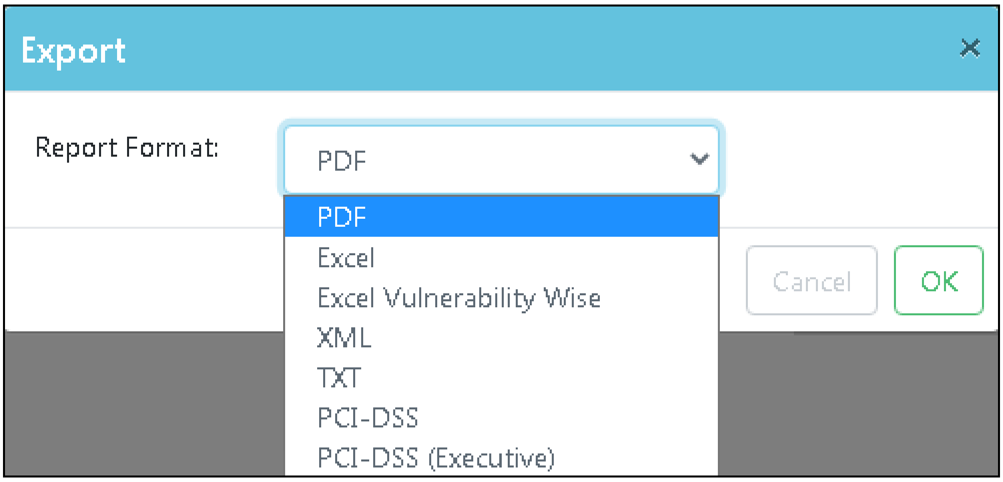
**Compared Report:** Aug 10 2020 01:38 PM

| Vulnerability | Severity | Detection Threshold | Host | Protocol | Status |
|---|---|---|---|---|---|
| DCE/RPC and MSRPC Services Enumeration Reporting | 5.0 | 80% | [redacted] | 135/tcp | Same |
| Microsoft IIS Default Welcome Page Information Disclosure Vulnerability | 5.0 | 70% | [redacted] | 80/tcp | Same |
| SSL/TLS: Report Weak Cipher Suites | 4.3 | 98% | [redacted] | 3389/tcp | Same |
| SSL/TLS: Certificate Signed Using A Weak Signature Algorithm | 4.0 | 80% | [redacted] | 3389/tcp | Same |
| TCP timestamps | 2.6 | 80% | [redacted] | general/tcp | Changed |

Users should note that at a time only two reports can be compared.

## Exporting a Report

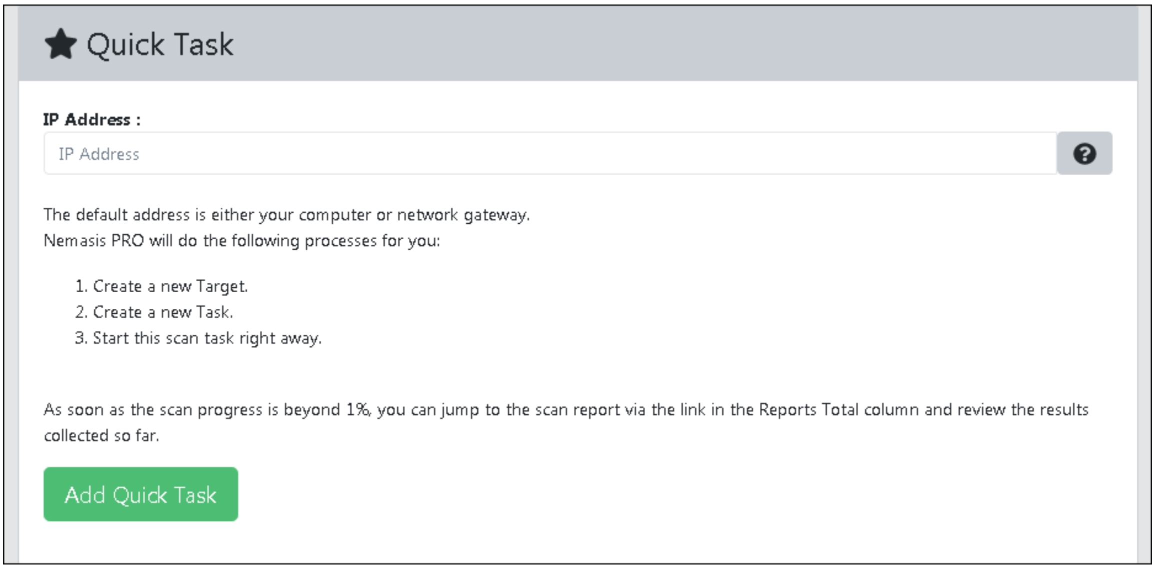
To export a report to your system, click **Export**. Export pop-up window appears.



The report can be downloaded in four formats that are PDF, Excel, Excel Vulnerability Wise, XML, TXT, PCI-DSS, and PCI-DSS (Executive). Select the preferred format and then click **OK**. The report will be downloaded to your system. The report contains details like Summary, Vulnerability Detected, Solution, Vulnerability Insight, Detection Method, and CVE references.

# Quick Task

The Quick Task lets you run a scan task instantly.



Quick Task

**IP Address :**

IP Address

The default address is either your computer or network gateway.
Nemasis PRO will do the following processes for you:

1. Create a new Target.
2. Create a new Task.
3. Start this scan task right away.

As soon as the scan progress is beyond 1%, you can jump to the scan report via the link in the Reports Total column and review the results collected so far.

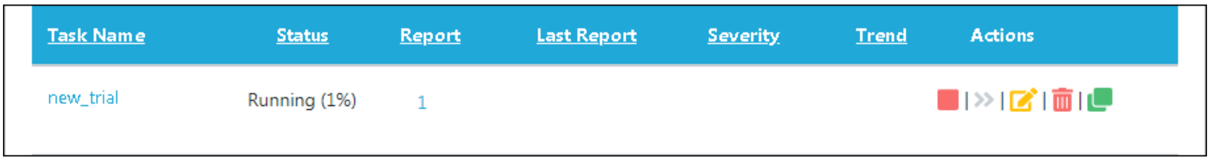
Add Quick Task

Enter the IP address of the target system and then click **Add Quick Task**.

Nemasis PRO will do the following processes for you:

1. Create a new Target.
2. Create a new Task.
3. Start this scan task right away.

As soon as the scan progress is beyond 1%, you can view the report by clicking the numerical in the **Report** column and view the results collected so far.



| Task Name | Status | Report | Last Report | Severity | Trend | Actions |
|---|---|---|---|---|---|---|
| new_trial | Running (1%) | 1 | | | | ■ » ✎ 🗑 ⧉ |

You can manage the task by clicking icons in the **Actions** column.

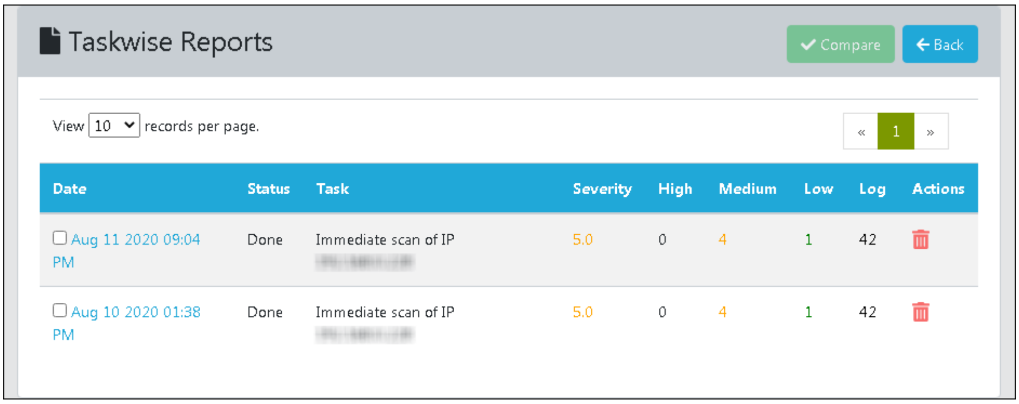
- ▶ Start Task
- ■ Stop Task
- » Resume Task
- ✎ Edit Task
- 🗑 Delete Task
- ⧉ Clone Task
- 🕓 Task is scheduled

**NOTE**

The icon » will change to » only if a running task is stopped.

If you resume a stopped task, the Nemasis PRO will exclude the scanned IP addresses.

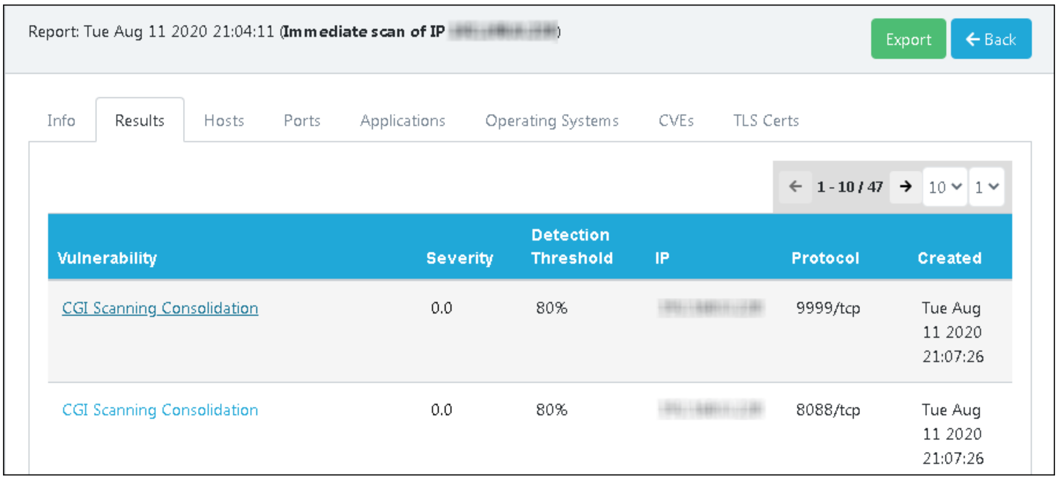
You can view the report during the scan and after the scan task is completed by clicking the numerical in the **Report** column. The Severity column displays the criticality of any vulnerability detected. Clicking the numerical in **High**, **Medium**, **Low** and **Log** column display only Results tab from the report.



View 10 records per page.

| Date | Status | Task | Severity | High | Medium | Low | Log | Actions |
|---|---|---|---|---|---|---|---|---|
| □ Aug 11 2020 09:04 PM | Done | Immediate scan of IP [redacted] | 5.0 | 0 | 4 | 1 | 42 | 🗑 |
| □ Aug 10 2020 01:38 PM | Done | Immediate scan of IP [redacted] | 5.0 | 0 | 4 | 1 | 42 | 🗑 |

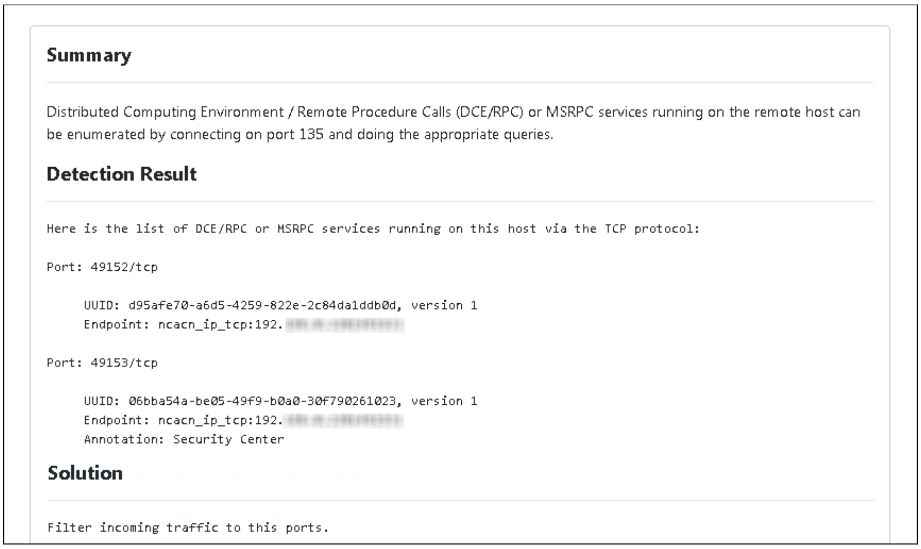
To view the detailed report, click the date in **Date** column.



Report: Tue Aug 11 2020 21:04:11 (**Immediate scan of IP** [redacted])

| Vulnerability | Severity | Detection Threshold | IP | Protocol | Created |
|---|---|---|---|---|---|
| CGI Scanning Consolidation | 0.0 | 80% | [redacted] | 9999/tcp | Tue Aug 11 2020 21:07:26 |
| CGI Scanning Consolidation | 0.0 | 80% | [redacted] | 8088/tcp | Tue Aug 11 2020 21:07:26 |

Clicking the vulnerability displays its **Summary**, **Detection Result**, and **Solution**.



**Summary**

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Detection Result**

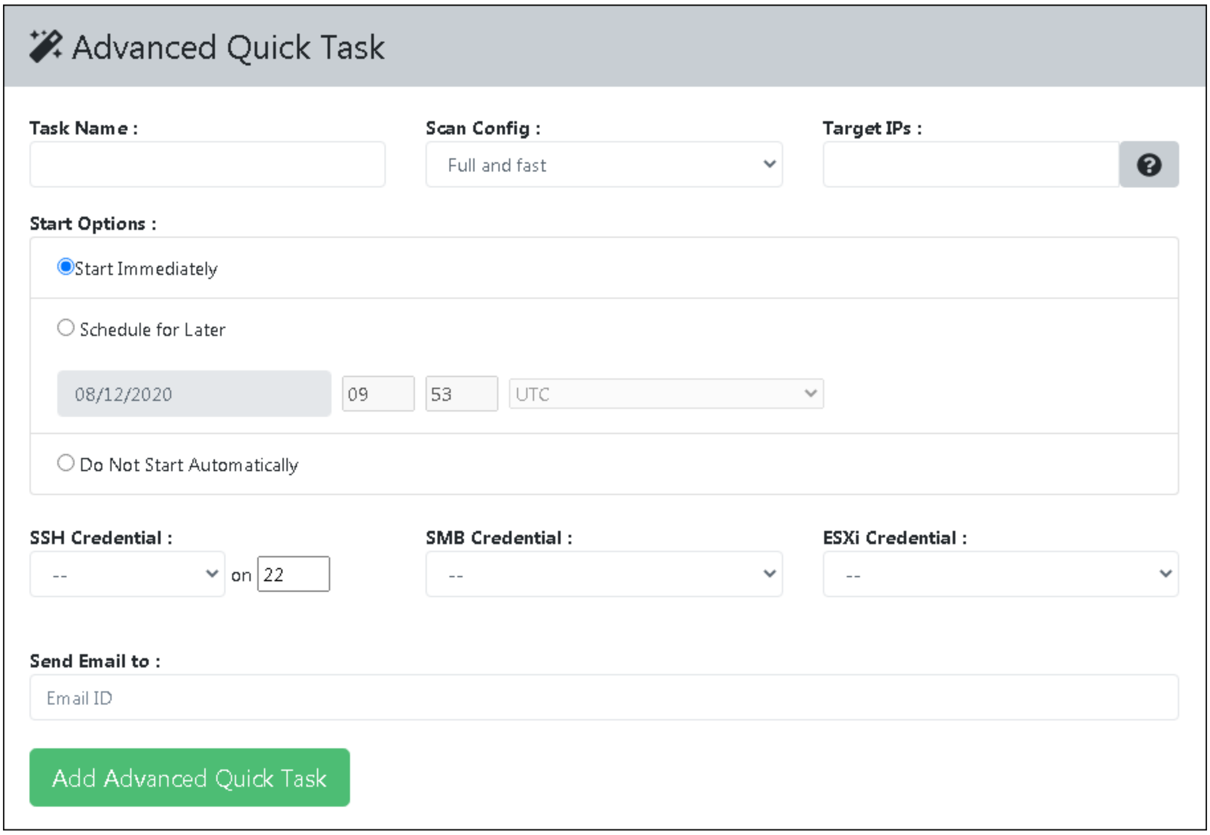
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49152/tcp

     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.[redacted]

Port: 49153/tcp

     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.[redacted]
     Annotation: Security Center
```

**Solution**

```
Filter incoming traffic to this ports.
```

# Advanced Quick Task

The Advanced Quick Task lets you run a task according to your needs by cutting down on excess manual configuration.



Advanced Quick Task

Task Name :

Scan Config : Full and fast

Target IPs :

Start Options :

● Start Immediately

○ Schedule for Later

08/12/2020 09 53 UTC

○ Do Not Start Automatically

SSH Credential : -- on 22

SMB Credential : --

ESXi Credential : --

Send Email to : Email ID

**Task Name:** Enter a name for the Task.

**Scan Config:** Click the dropdown and select the scan configuration of your preference.

**Target Host:** Enter the IP address or import a list of IP addresses in this field. You can enter the IP address in the field with the following formats:

- Single IP address, for example, 192.168.25.151
- IPv4 address range, for example, 192.168.25.151-251
- IPv4 network in CIDR notation, for example, 192.168.25.0/24
- Multiple IP addresses separated by commas

**Start options:** There are three options available to start the task.

- **Start Immediately** – Select this option to start the task immediately.
- **Schedule for Later** – Select this option to schedule the task on your preferred date, time, and region.
- **Do Not Start Automatically** – Select this option to start the task manually.

**SSH Credential:** If the target system runs on Linux or UNIX, click this dropdown and select the appropriate credential.

**SMB Credential:** If the target system runs on Microsoft Windows, click this dropdown and select the appropriate credential.

**ESXi Credential:** If the target system is a VMWare ESXi system, click this dropdown and select the appropriate credential.

**Send Email to:** Enter a report recipient’s email ID in this field. The report details will be in the email’s body text.

After filling all the fields, click **Add Advanced Quick Task**. The task will be added to the Current Tasks list.

In the upper right corner there are two buttons available:

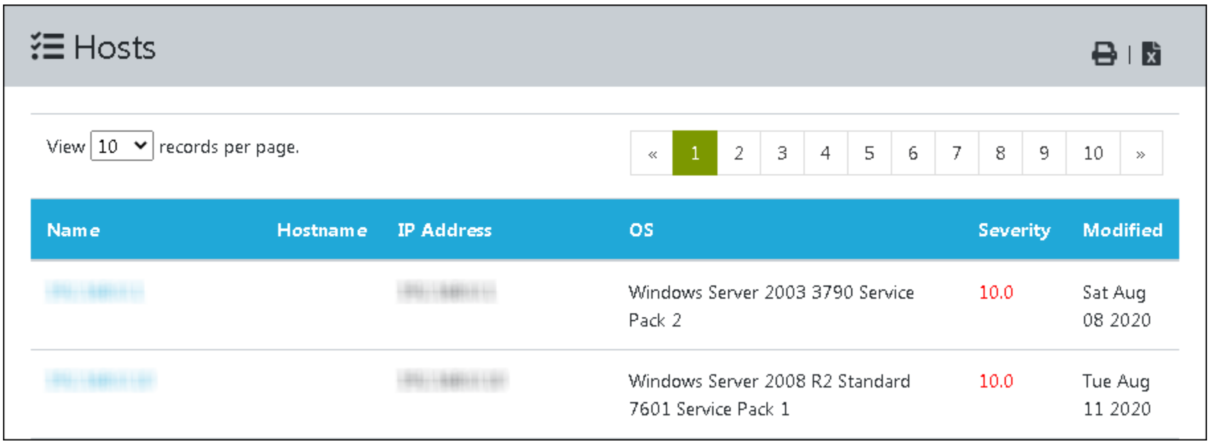
- 🖨 Click this icon to print the report.
- X Click this icon to export the report in XLS format.

# Assets

The Assets module displays the hostnames and OS of the scanned endpoints. Users should note that the endpoints will be displayed in Assets only after they are scanned by Nemasis PRO.

## Host

The Host submodule displays the Hostname, IP address, OS installed and severity level of the scanned endpoint along with the host discovery date.



Hosts

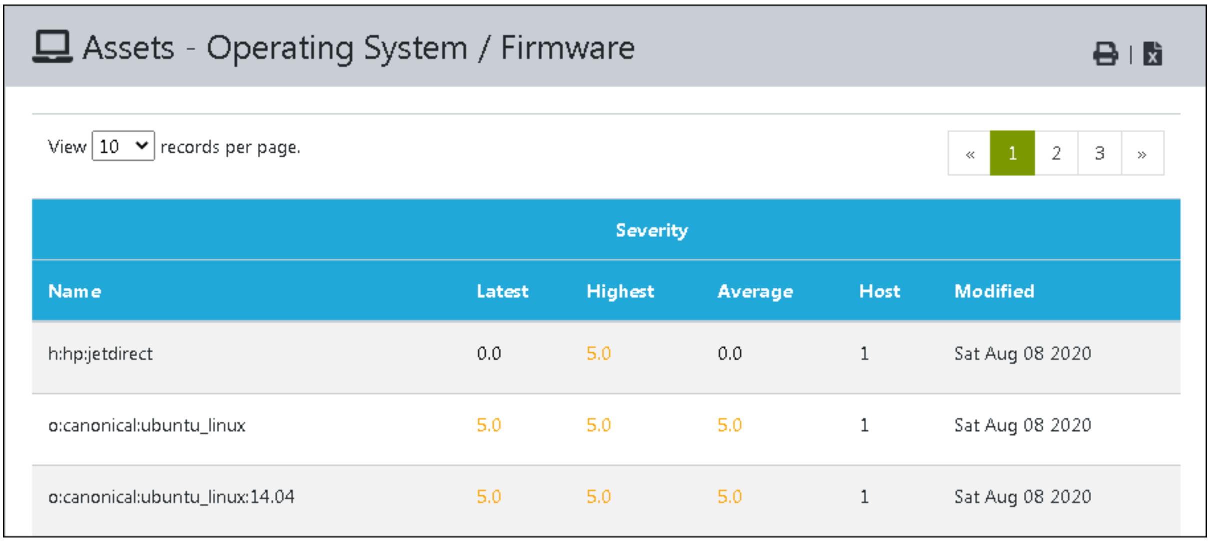
View 10 records per page.

« 1 2 3 4 5 6 7 8 9 10 »

| Name | Hostname | IP Address | OS | Severity | Modified |
|---|---|---|---|---|---|
| [redacted] | | [redacted] | Windows Server 2003 3790 Service Pack 2 | 10.0 | Sat Aug 08 2020 |
| [redacted] | | [redacted] | Windows Server 2008 R2 Standard 7601 Service Pack 1 | 10.0 | Tue Aug 11 2020 |

## Operating Systems

The Operating Systems submodule displays the OS names, Severity level by its latest, highest, and average classification and detection amongst the number of hosts along with detection date.



Assets - Operating System / Firmware

View 10 records per page.

« 1 2 3 »

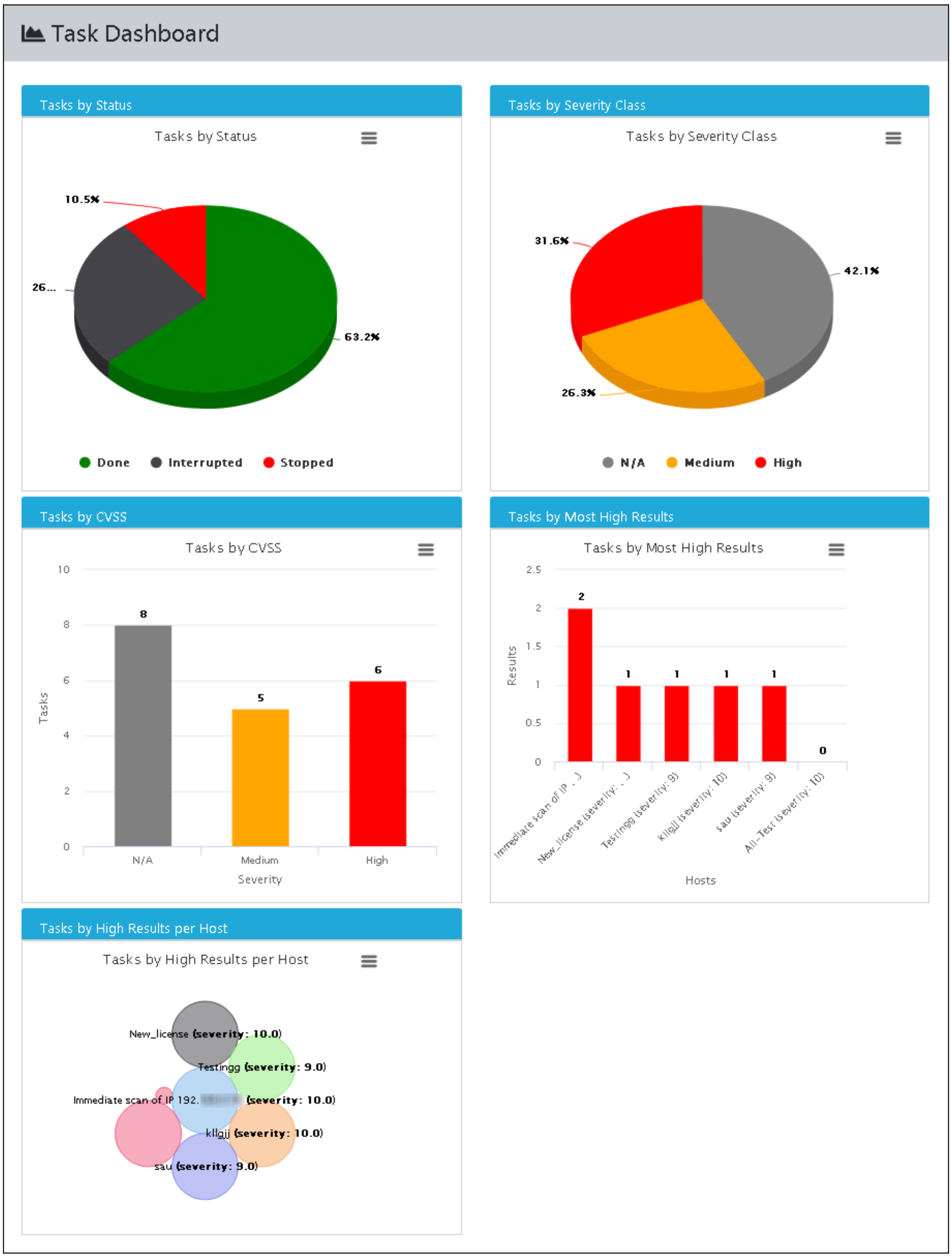
| | Severity | | | | |
|---|---|---|---|---|---|
| Name | Latest | Highest | Average | Host | Modified |
| h:hp:jetdirect | 0.0 | 5.0 | 0.0 | 1 | Sat Aug 08 2020 |
| o:canonical:ubuntu_linux | 5.0 | 5.0 | 5.0 | 1 | Sat Aug 08 2020 |
| o:canonical:ubuntu_linux:14.04 | 5.0 | 5.0 | 5.0 | 1 | Sat Aug 08 2020 |

# Task Results

The Task Results module contains results of all tasks run in the database. It consists of three submodules which are **Task Dashboard**, **Results**, and **Vulnerabilities**.

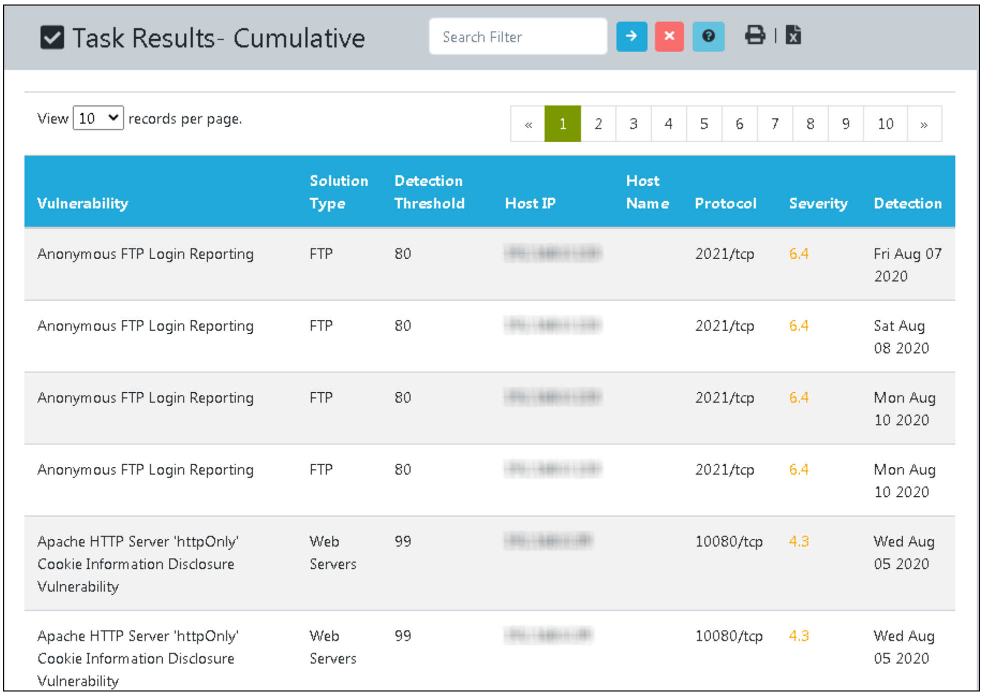
## Task Dashboard

The Task Dashboard submodule displays results of the tasks by status, severity class, CVSS, most high results, and high results per host in various interactive chart formats.



# Results

The Results submodule displays the type of Vulnerability found, Solution for vulnerability, Detection Threshold, Host IP address, Host Name, type of Protocol used, Severity level, and Detection date.



| Vulnerability | Solution Type | Detection Threshold | Host IP | Host Name | Protocol | Severity | Detection |
|---|---|---|---|---|---|---|---|
| Anonymous FTP Login Reporting | FTP | 80 | [redacted] | | 2021/tcp | 6.4 | Fri Aug 07 2020 |
| Anonymous FTP Login Reporting | FTP | 80 | [redacted] | | 2021/tcp | 6.4 | Sat Aug 08 2020 |
| Anonymous FTP Login Reporting | FTP | 80 | [redacted] | | 2021/tcp | 6.4 | Mon Aug 10 2020 |
| Anonymous FTP Login Reporting | FTP | 80 | [redacted] | | 2021/tcp | 6.4 | Mon Aug 10 2020 |
| Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | Web Servers | 99 | [redacted] | | 10080/tcp | 4.3 | Wed Aug 05 2020 |
| Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | Web Servers | 99 | [redacted] | | 10080/tcp | 4.3 | Wed Aug 05 2020 |

## Search Filter

You can filter the displayed information by using the following filter tags:

- ~ contains for example, name~admin
- = equals for example, family=Product detection
- < less than for example, severity < 7.0
- > greater than for example, severity > 4.0

To filter by date, enter the date format as YYYY-MM-DD.

To search for the exact result, enter your search in Double Quotation Marks. For example, family="Web Servers", severity="5.0"

To filter the result by two categories, enter the filter tags in the following manner: family="Web Servers" and severity="5.0"

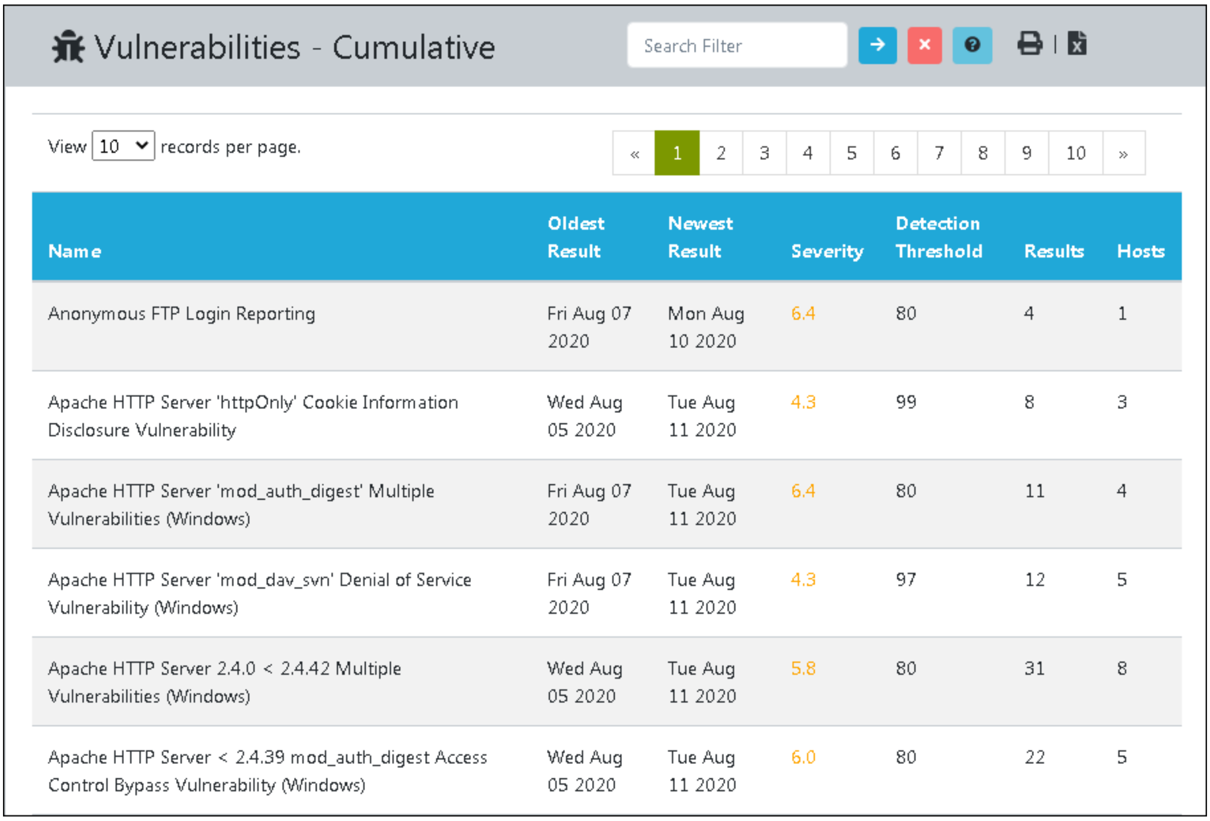
| | |
|---|---|
| **NOTE** | The filter tags are case sensitive and must be entered in lowercase. |

You can filter the displayed information to find a specific result by using the following filter tags:

- name (Vulnerability)
- host (Host IP)
- severity

# Vulnerabilities

The Vulnerabilities submodule displays the Vulnerability’s name, Oldest Result, Newest Result, Severity level, Detection Threshold, Results, and the number of Hosts on which it occurred.



Vulnerabilities - Cumulative

| Name | Oldest Result | Newest Result | Severity | Detection Threshold | Results | Hosts |
|---|---|---|---|---|---|---|
| Anonymous FTP Login Reporting | Fri Aug 07 2020 | Mon Aug 10 2020 | 6.4 | 80 | 4 | 1 |
| Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability | Wed Aug 05 2020 | Tue Aug 11 2020 | 4.3 | 99 | 8 | 3 |
| Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Windows) | Fri Aug 07 2020 | Tue Aug 11 2020 | 6.4 | 80 | 11 | 4 |
| Apache HTTP Server 'mod_dav_svn' Denial of Service Vulnerability (Windows) | Fri Aug 07 2020 | Tue Aug 11 2020 | 4.3 | 97 | 12 | 5 |
| Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Windows) | Wed Aug 05 2020 | Tue Aug 11 2020 | 5.8 | 80 | 31 | 8 |
| Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Windows) | Wed Aug 05 2020 | Tue Aug 11 2020 | 6.0 | 80 | 22 | 5 |

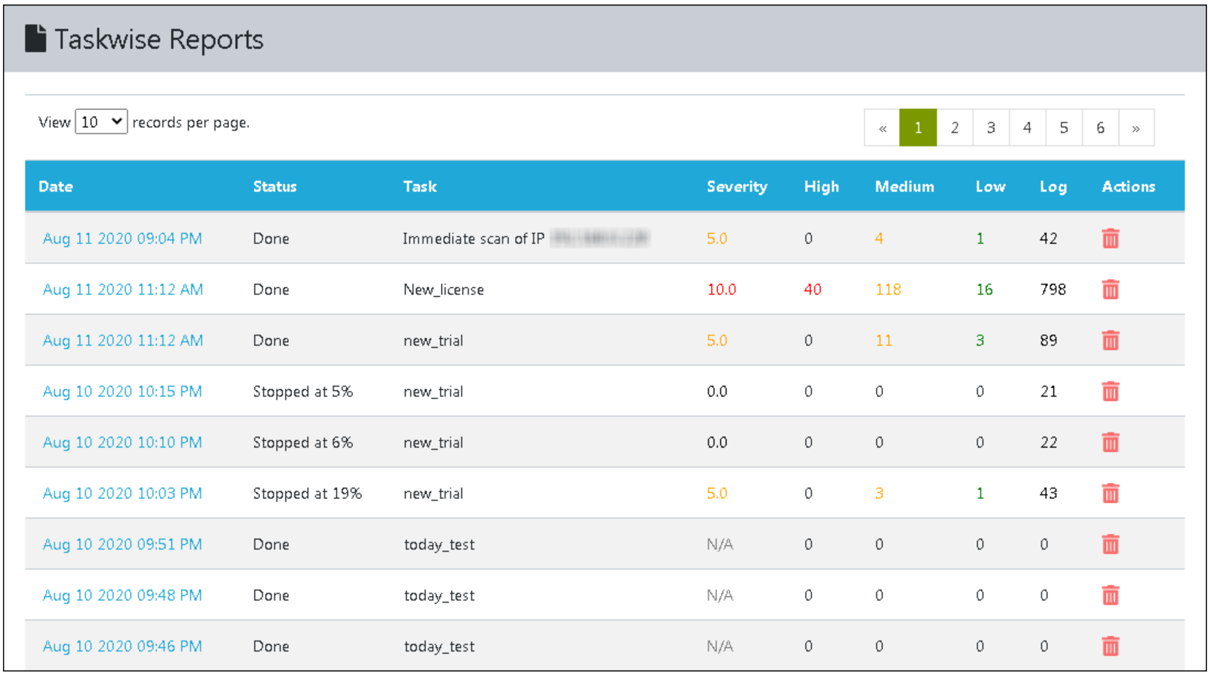
The **Results** and **Vulnerabilities** submodules display a cumulative result.

You can filter the displayed information to find a specific result by using following filter tags:

- name
- severity

# Reports

The Reports module displays task wise reports sorted by date. Clicking the date shows a report containing details like Info, Results, Host, Ports, Applications, OS, Network CVEs, Local CVEs, and TLS certifications. In the **Results** tab, additional information about the vulnerability is displayed containing its summary, detection result, and solution. The report can be exported in PDF, Excel, Excel Vulnerability Wise, XML, TXT, PCI-DSS, and PCI-DSS (Executive) formats.



Taskwise Reports

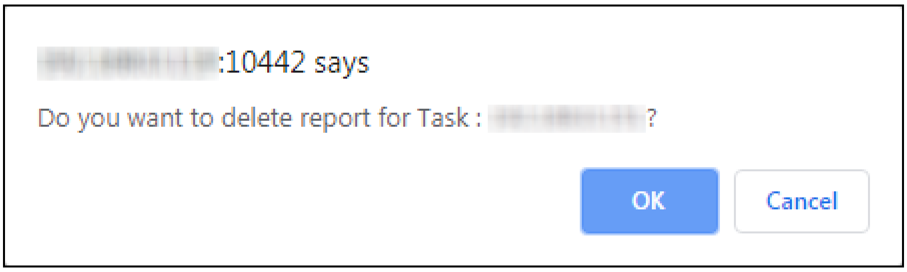
View 10 records per page.

| Date | Status | Task | Severity | High | Medium | Low | Log | Actions |
|---|---|---|---|---|---|---|---|---|
| Aug 11 2020 09:04 PM | Done | Immediate scan of IP [redacted] | 5.0 | 0 | 4 | 1 | 42 | 🗑 |
| Aug 11 2020 11:12 AM | Done | New_license | 10.0 | 40 | 118 | 16 | 798 | 🗑 |
| Aug 11 2020 11:12 AM | Done | new_trial | 5.0 | 0 | 11 | 3 | 89 | 🗑 |
| Aug 10 2020 10:15 PM | Stopped at 5% | new_trial | 0.0 | 0 | 0 | 0 | 21 | 🗑 |
| Aug 10 2020 10:10 PM | Stopped at 6% | new_trial | 0.0 | 0 | 0 | 0 | 22 | 🗑 |
| Aug 10 2020 10:03 PM | Stopped at 19% | new_trial | 5.0 | 0 | 3 | 1 | 43 | 🗑 |
| Aug 10 2020 09:51 PM | Done | today_test | N/A | 0 | 0 | 0 | 0 | 🗑 |
| Aug 10 2020 09:48 PM | Done | today_test | N/A | 0 | 0 | 0 | 0 | 🗑 |
| Aug 10 2020 09:46 PM | Done | today_test | N/A | 0 | 0 | 0 | 0 | 🗑 |

## Deleting a Report

To delete a Report, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete report for Task : [redacted]?

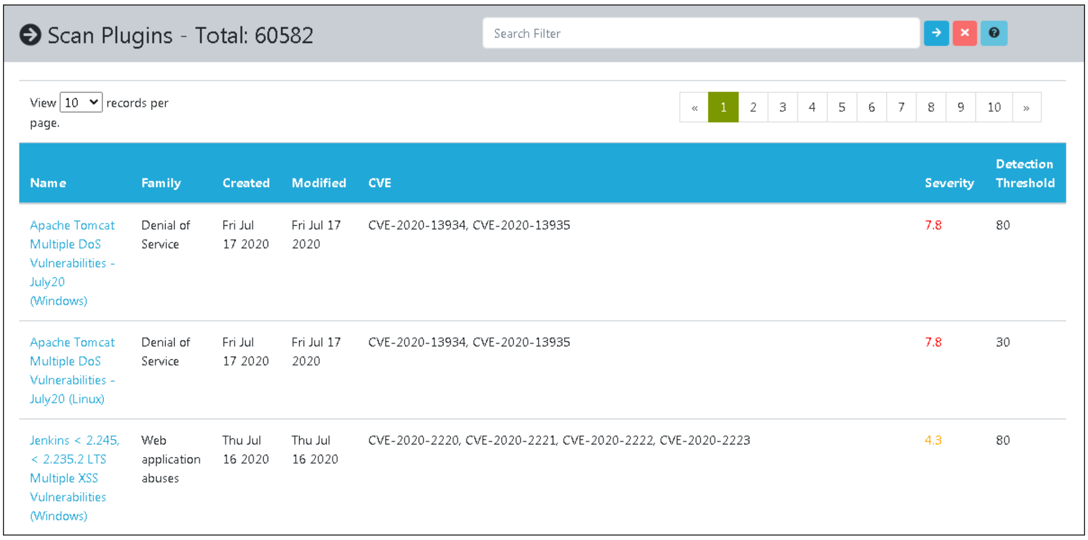
2. Click **OK**. The report will be deleted.

# Security Info

The Security Info module displays information related to asset security. It contains four submodules which are **Scan Plugins, CVE, CPE**, and **OVAL Definitions**.

## Scan Plugins

Scan Plugins are tests used by Nemasis PRO to scan a system for potential vulnerabilities. You can update Scan Plugins, run them against an endpoint, and identify the network vulnerabilities. After the scan is completed, the Nemasis PRO will provide accurate solutions to patch vulnerabilities.



Scan Plugins - Total: 60582

| Name | Family | Created | Modified | CVE | Severity | Detection Threshold |
|---|---|---|---|---|---|---|
| Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows) | Denial of Service | Fri Jul 17 2020 | Fri Jul 17 2020 | CVE-2020-13934, CVE-2020-13935 | 7.8 | 80 |
| Apache Tomcat Multiple DoS Vulnerabilities - July20 (Linux) | Denial of Service | Fri Jul 17 2020 | Fri Jul 17 2020 | CVE-2020-13934, CVE-2020-13935 | 7.8 | 30 |
| Jenkins < 2.245, < 2.235.2 LTS Multiple XSS Vulnerabilities (Windows) | Web application abuses | Thu Jul 16 2020 | Thu Jul 16 2020 | CVE-2020-2220, CVE-2020-2221, CVE-2020-2222, CVE-2020-2223 | 4.3 | 80 |

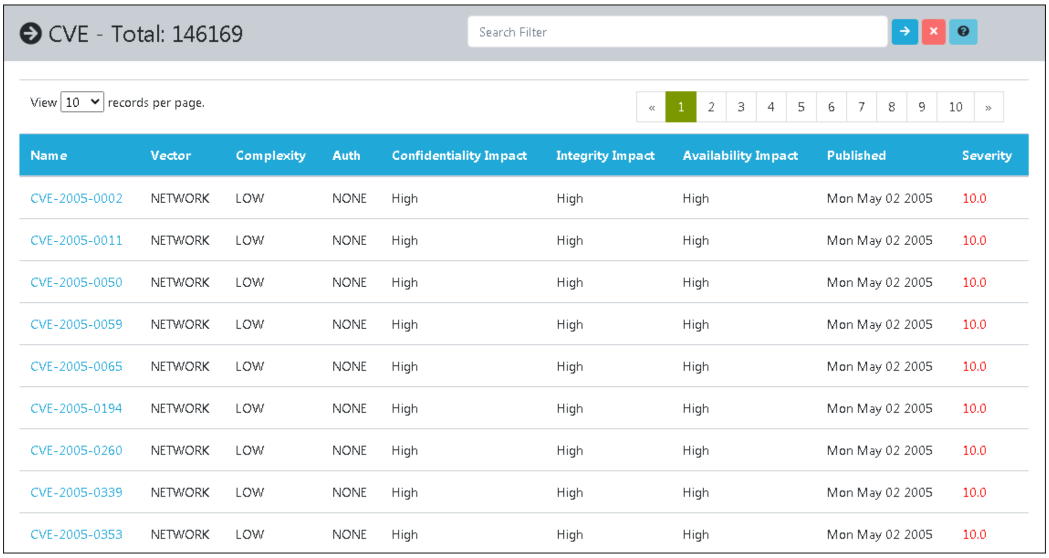
You can filter the displayed information to find a specific result by using the following filter tags:

- name
- family
- severity

Clicking a Scan Plugin Name displays its Summary, Affected Software/OS, Scoring according to CVSS Base, Insight, Detection Method, how the system can be Impacted, accurate Solution to fix it, Family the vulnerability belongs to, and other References.

# CVE

CVE stands for Common Vulnerabilities and Exposures. The CVE database contains details of known security threats. As per the CVE website, **Vulnerability** is a flaw in software code that provides an attacker with direct access to a network or system. The **Exposure** is a flaw in software code that provides an attacker with indirect access to a network or system. Nemasis PRO has a database of vast vulnerabilities and provides a solution for the same.



| Name | Vector | Complexity | Auth | Confidentiality Impact | Integrity Impact | Availability Impact | Published | Severity |
|---|---|---|---|---|---|---|---|---|
| CVE-2005-0002 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0011 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0050 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0059 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0065 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0194 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0260 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0339 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |
| CVE-2005-0353 | NETWORK | LOW | NONE | High | High | High | Mon May 02 2005 | 10.0 |

In the past, a lot of organizations reported the discovered vulnerabilities at the same time by assigning them different names. The various scanners too reported the same vulnerability with various names. This led to comparing all vulnerabilities and finding out later that it was the same vulnerability reported multiple times.

In 1999, The MITRE Corporation addressed this issue by founding the CVE project. Each vulnerability is allocated a special identifier that consists of a year and number. The NVD (National Vulnerability Database) looks up MITRE's CVE database and provides the solution for vulnerability, its severity level, products affected, and its impact. Nemasis PRO refers to the NVD's CVE database and combines the information with Scan Plugins to display the accurate scan results.

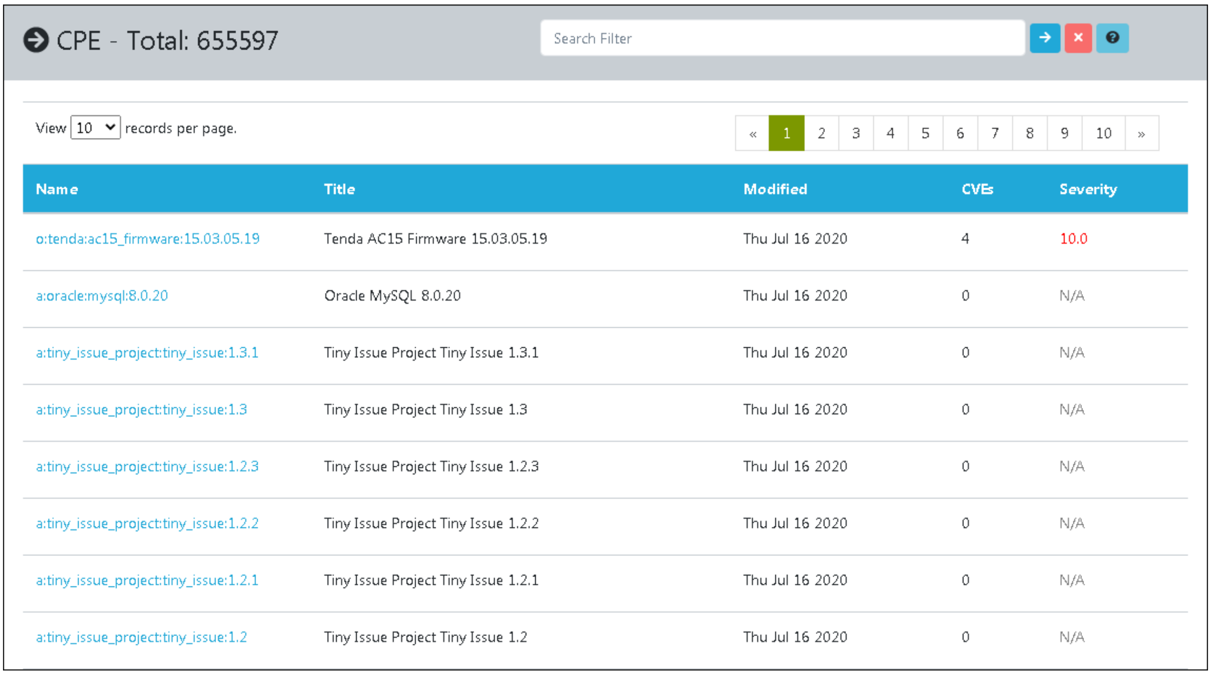
You can filter the displayed information to find a specific result by using the following filter tags:

- name
- severity
- vector
- complexity
- confidentiality impact
- integrity impact

Clicking a CVE displays its Description, CVSS details, and the products vulnerable to specific CVE.

# CPE

CPE stands for Common Platform Enumerations. After CVEs, MITRE introduced this structured method of identifying and describing classes of OS, hardware devices, and software installed on an enterprise's computing assets. The CPE is a structured naming schema based on the generic syntax of the URI (Uniform Resource Identifier). As the CPE standard is closely associated with CVE standards, the unique combination helps identify vulnerabilities quickly across a product or platform.



CPE - Total: 655597

| Name | Title | Modified | CVEs | Severity |
|---|---|---|---|---|
| o:tenda:ac15_firmware:15.03.05.19 | Tenda AC15 Firmware 15.03.05.19 | Thu Jul 16 2020 | 4 | 10.0 |
| a:oracle:mysql:8.0.20 | Oracle MySQL 8.0.20 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.3.1 | Tiny Issue Project Tiny Issue 1.3.1 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.3 | Tiny Issue Project Tiny Issue 1.3 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.2.3 | Tiny Issue Project Tiny Issue 1.2.3 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.2.2 | Tiny Issue Project Tiny Issue 1.2.2 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.2.1 | Tiny Issue Project Tiny Issue 1.2.1 | Thu Jul 16 2020 | 0 | N/A |
| a:tiny_issue_project:tiny_issue:1.2 | Tiny Issue Project Tiny Issue 1.2 | Thu Jul 16 2020 | 0 | N/A |

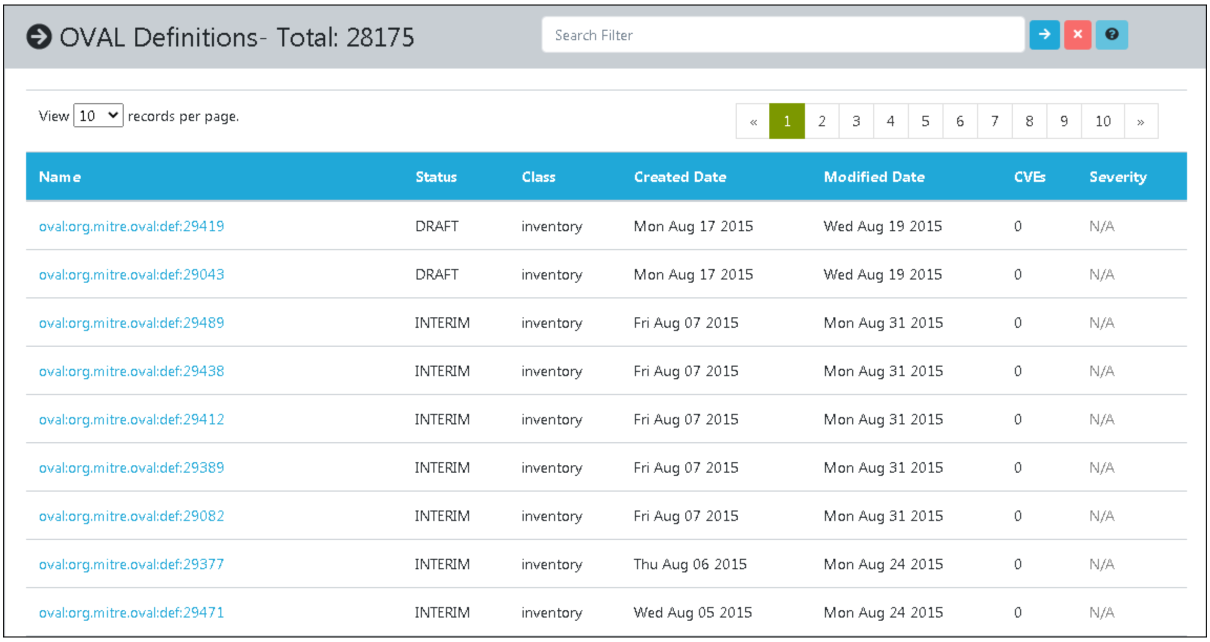
The CPE project was also initiated by MITRE but currently, it is maintained by NIST (National Institute for Standards and Technology) as a part of NVD. You can filter the displayed information to find a specific result by using the following filter tags:

- name
- cves
- severity
- title

Clicking a CPE displays its NVD ID, Last Updated date, and Status.

# OVAL Definitions

The OVAL Definitions are machine-readable standardized tests written in Open Vulnerability and Assessment Language. The OVAL Definitions scan systems for vulnerabilities, programs, patches, and configuration issues. The OVAL project was also initiated by MITRE. These XML based definitions allow for easy processing by automated systems.



OVAL Definitions- Total: 28175

| Name | Status | Class | Created Date | Modified Date | CVEs | Severity |
|---|---|---|---|---|---|---|
| oval:org.mitre.oval:def:29419 | DRAFT | inventory | Mon Aug 17 2015 | Wed Aug 19 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29043 | DRAFT | inventory | Mon Aug 17 2015 | Wed Aug 19 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29489 | INTERIM | inventory | Fri Aug 07 2015 | Mon Aug 31 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29438 | INTERIM | inventory | Fri Aug 07 2015 | Mon Aug 31 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29412 | INTERIM | inventory | Fri Aug 07 2015 | Mon Aug 31 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29389 | INTERIM | inventory | Fri Aug 07 2015 | Mon Aug 31 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29082 | INTERIM | inventory | Fri Aug 07 2015 | Mon Aug 31 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29377 | INTERIM | inventory | Thu Aug 06 2015 | Mon Aug 24 2015 | 0 | N/A |
| oval:org.mitre.oval:def:29471 | INTERIM | inventory | Wed Aug 05 2015 | Mon Aug 24 2015 | 0 | N/A |

The OVAL definition **oval:org.mitre.oval:29082** of the inventory class describes the Microsoft Visual Studio while the OVAL definition **oval:org.mitre.oval:def:28834** of the vulnerability class describes the vulnerability of Internet Explorer.

You can filter the displayed information to find a specific result by using the following filter tags:

- name
- class
- cves
- severity

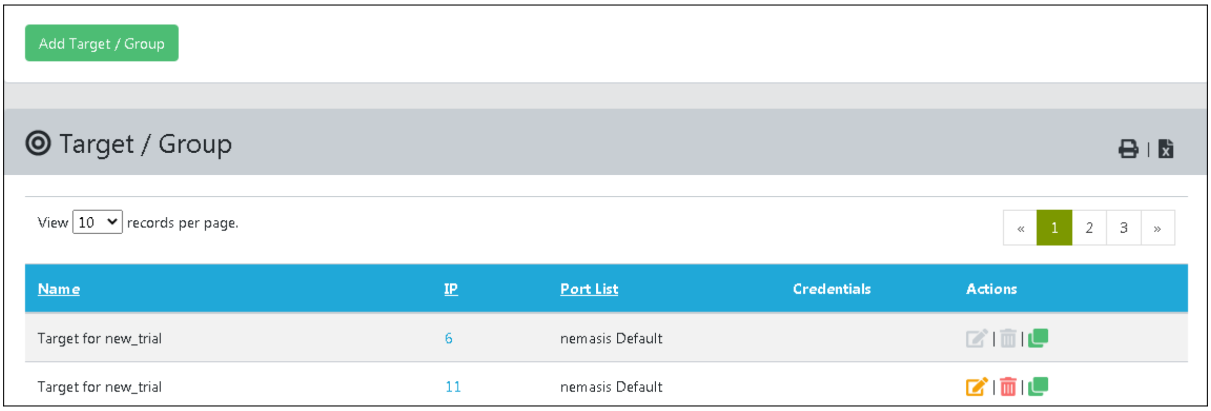
Clicking an OVAL Definition displays its Title, Definition Class, Referenced CVEs, Security, and File path.

# Configurations

The Configurations module contains **Target, Port List, Credentials, Alerts, Scan Config, Schedule, Scanners**, **False Positive**, and **SMTP** submodules.

## Target / Group

A Target can be a single computer or a group of computers to be scanned for vulnerabilities. The Target submodule lets you add targets, its login credentials for scanning an endpoint, and displays a list of added targets.

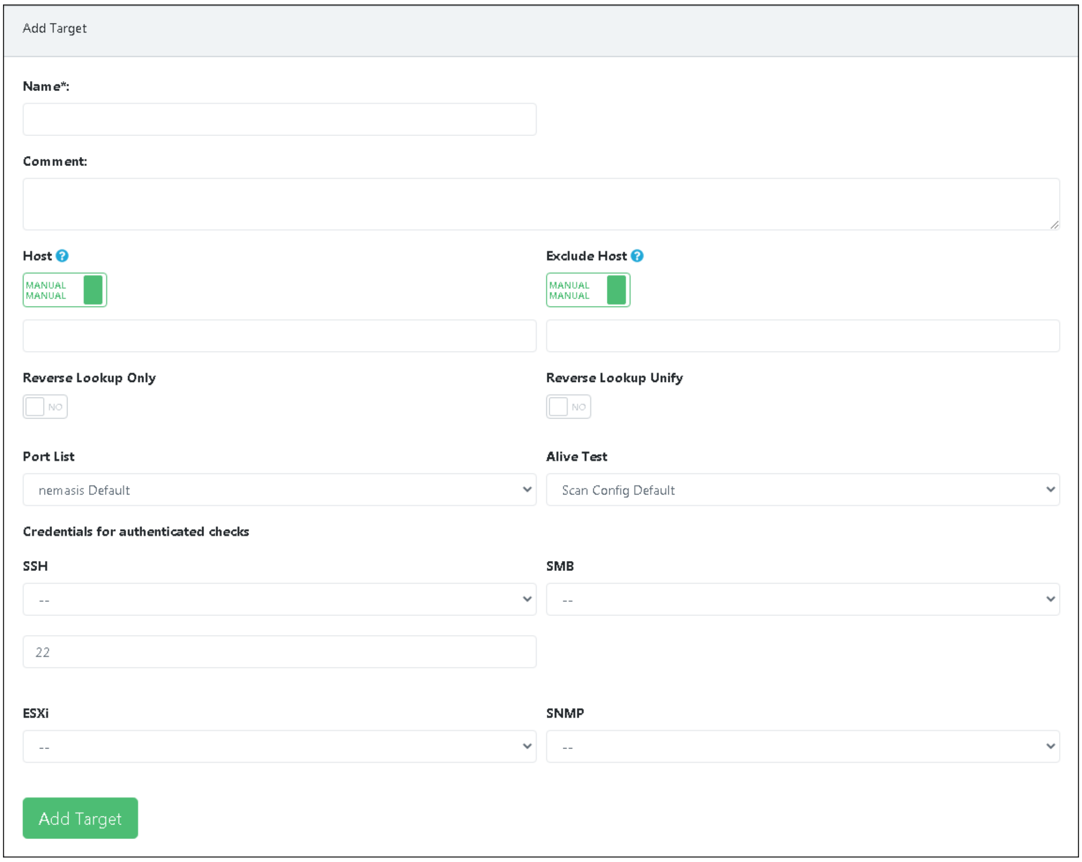


View 10 records per page.

| Name | IP | Port List | Credentials | Actions |
|---|---|---|---|---|
| Target for new_trial | 6 | nemasis Default | | |
| Target for new_trial | 11 | nemasis Default | | |

# Adding a Target

To add a Target, click **Add Target / Group**.
Add Target form appears on the right pane.



Add Target

Name*:

Comment:

Host
MANUAL

Exclude Host
MANUAL

Reverse Lookup Only
NO

Reverse Lookup Unify
NO

Port List
nemasis Default

Alive Test
Scan Config Default

Credentials for authenticated checks

SSH
--
22

SMB
--

ESXi
--

SNMP
--

**Name:** Enter a name for the Target.

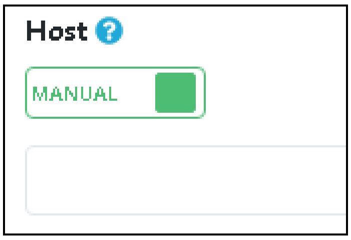
**Comment:** Enter a descriptive comment for the Target.

**Host:** Enter the IP address or import a list of IP addresses in this field. You can enter the IP address in the field with the following formats:

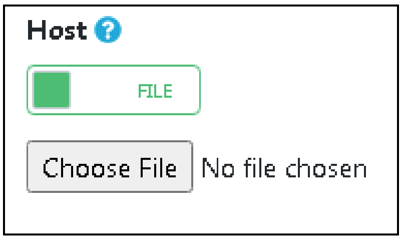
- Single IP address, for example, 192.168.25.151
- IPv4 address range, for example, 192.168.25.151-251
- IPv4 network in CIDR notation, for example, 192.168.25.0/24
- Multiple IP addresses separated by commas

When importing IP addresses from a file, the same format can be used. In the file, the IP addresses can be entered in multiple lines. If you are scanning a list full of systems, this strategy will be more beneficial.

If you have a CSV or TXT file containing a list of IP addresses, click the **Host** toggle. The toggle will change from **MANUAL** to **FILE**.


Host

MANUAL


Host

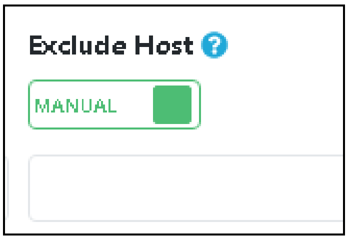
FILE

Choose File No file chosen

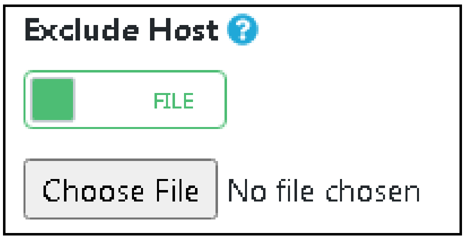
Click **Choose File** and select the file from the destination path.

**Exclude Host:** Enter the IP addresses you want to exclude from the above list.

If you have a CSV or TXT file containing IP addresses to be excluded from the scan, click the **Exclude Host** toggle. The toggle will change from **MANUAL** to **FILE**.


Exclude Host

MANUAL

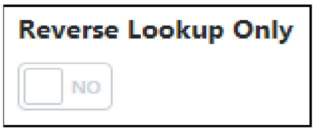

Exclude Host

FILE

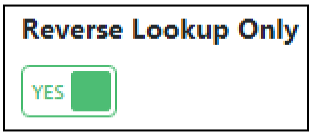
Choose File No file chosen

Click **Choose File** and select the file from the destination path.

**Reverse Lookup Only:** Nemasis PRO will scan specific IP addresses that can be resolved into a DNS name. By default the toggle is set to **NO**, click the toggle to change it to **YES**.

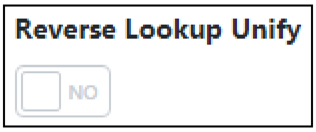

Reverse Lookup Only

NO

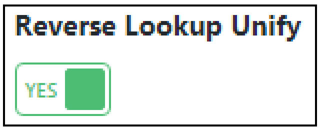

Reverse Lookup Only

YES

**Reverse Lookup Unify:** If multiple IP addresses resolve to one DNS name, the Nemasis PRO will scan the DNS name only once. By default the toggle is set to **NO**, click the toggle to change it to **YES**.


Reverse Lookup Unify

NO


Reverse Lookup Unify

YES

**Port List:** Click the dropdown and select the appropriate Port List. Learn more about Port List by clicking [here].

**Alive Test:** This option lets you specify the method to check whether a target(s) is reachable. Following options are available in the dropdown:

- ICMP Ping
- TCP-ACK Service Ping
- TCP-SYN Service Ping
- ARP Ping
- ICMP & TCP-ACK Service Ping
- ICMP & ARP Ping
- TCP-ACK Service & ARP Ping
- ICMP, TCP-ACK Service & ARP Ping
- Consider Alive
- Scan Config Default

### Credentials for authenticated checks

**SSH Credential:** Select this credential to log into the target system for a scan if the system is a UNIX or Linux system.

**SMB Credential:** Select this credential to log into the target system for a scan if the system is a Microsoft Windows system.

**ESXi Credential:** Select this credential to log into the target system for a scan if the system is a VMWare ESXi system.

**SNMP Credential:** Select this credential to log into the target system for a scan if the system is an SNMP aware system.

You can add new credentials by going to **Configurations > Credentials > Add Credential**.

After filling all the fields, click **Add Target**. The new Target will be added to the Targets list.

## Actions

Clicking icons in the Actions column lets you take actions regarding a Target.

- 🗑 Delete Target
- 📝 Edit Target
- ❐ Clone Target

The Target assigned to a Task cannot be edited or deleted unless you assign it a different Target.

- ✎ Edit Target (in use)
- 🗑 Delete Target (in use)

In order to edit or delete such a Target,

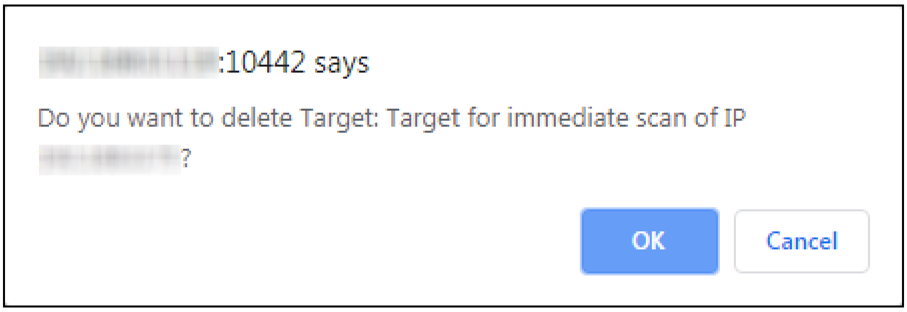
1. Go to **Scan > Task**.
   Current Tasks list appears.
2. Find the Task to which the specific Target is assigned and then in the **Actions** column, click ✎ (Edit Task).
   Edit Task pop-up window appears.
3. Click the **Target and Alerts** tab.
4. Click the **Scan Targets** dropdown, select a different Target, and then click **Update Task.**

As the Task is assigned a different Target, you can now delete or edit the specific Target.

## Deleting a Target

To delete a Target, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete Target: Target for immediate scan of IP [redacted]?

2. Click **OK**.
   Target will be deleted.

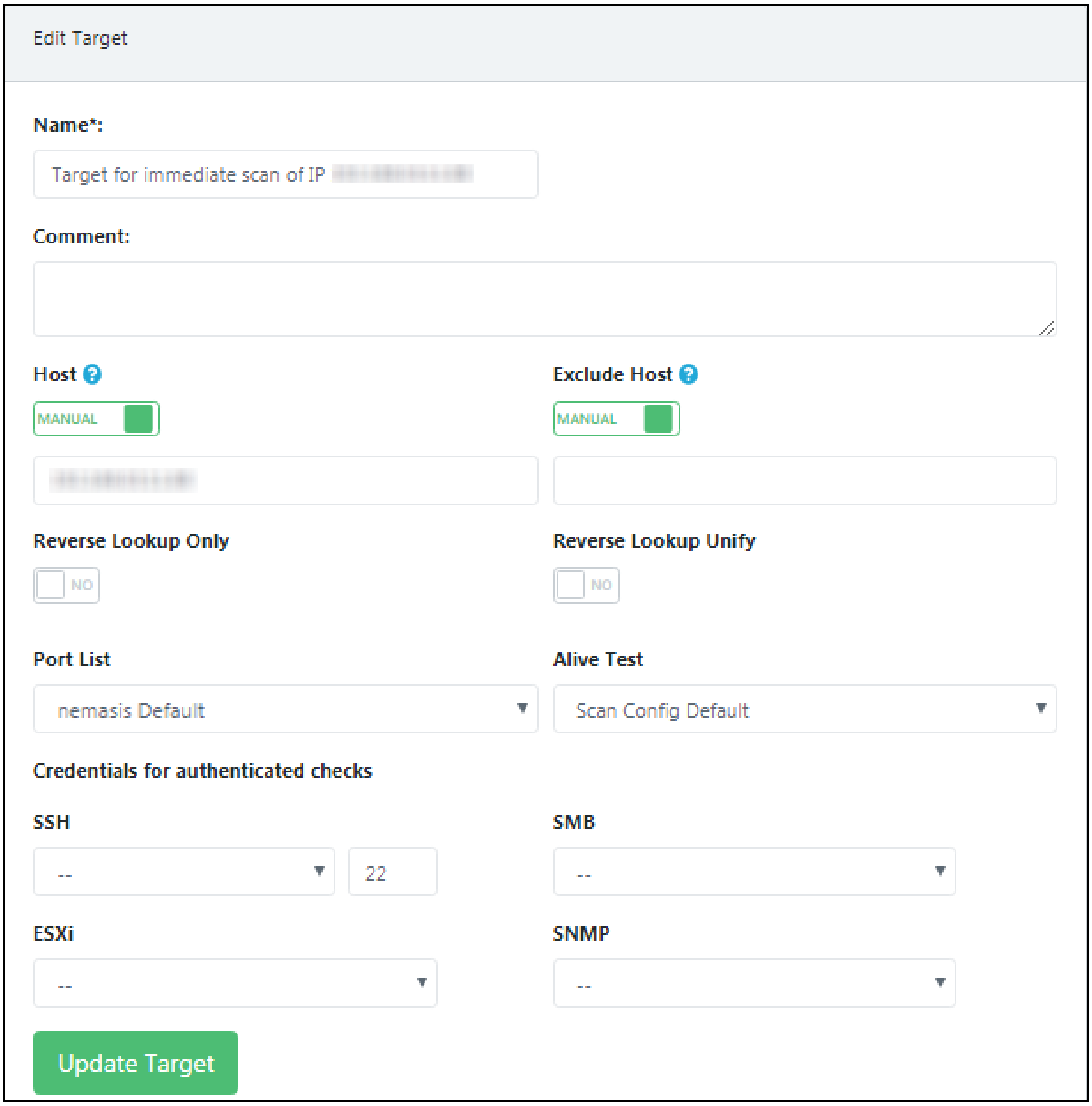
## Cloning a Target

To clone a Target, click ❐ in the **Actions** column. The Target will be cloned instantly.

# Editing a Target

To edit a Target, follow the steps given below:

1. In the **Actions** column, click ✎.
   Edit Target pop-up window appears.



Edit Target

Name*: Target for immediate scan of IP [redacted]

Comment:

Host

MANUAL

[redacted]

Exclude Host

MANUAL

Reverse Lookup Only: NO

Reverse Lookup Unify: NO

Port List: nemasis Default

Alive Test: Scan Config Default

Credentials for authenticated checks

SSH: -- 22

SMB: --

ESXi: --

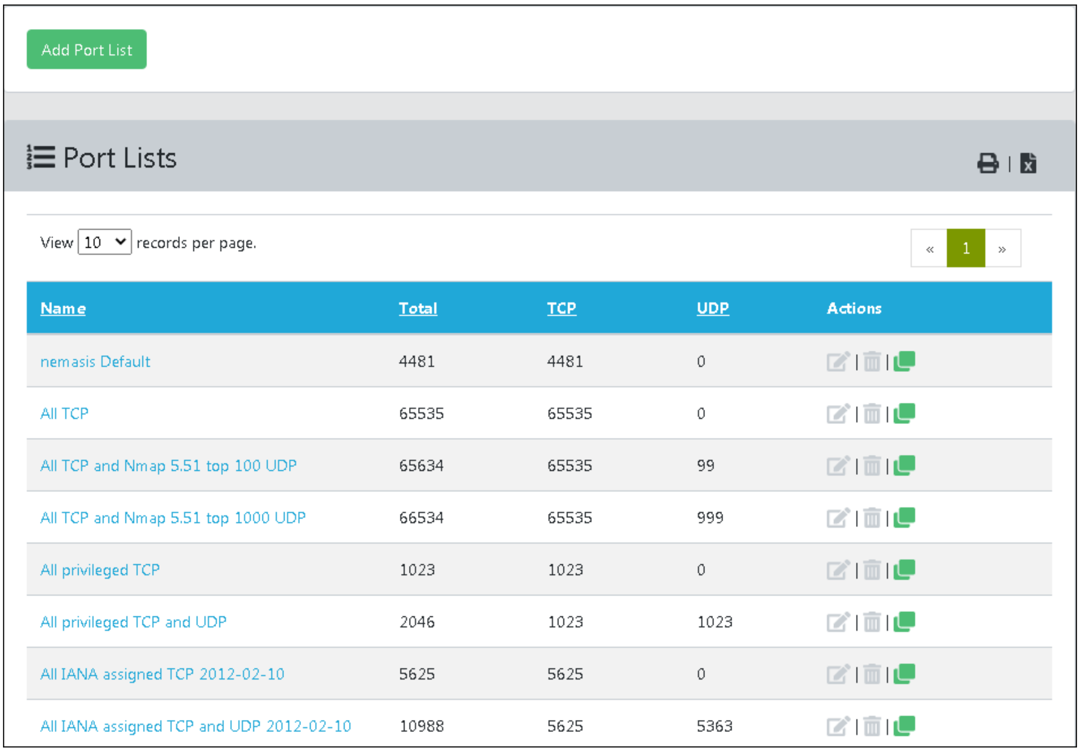
SNMP: --

Update Target

2. Make the necessary changes and then click **Update Target**.
   The Target will be updated.

# Port List

The Port List submodule displays default port lists that consist of TCP and UDP ports. It also lets you add a port or port range manually or from a CSV or TXT file.



| Name | Total | TCP | UDP | Actions |
|---|---|---|---|---|
| nemasis Default | 4481 | 4481 | 0 | ✎ \| 🗑 \| ⧉ |
| All TCP | 65535 | 65535 | 0 | ✎ \| 🗑 \| ⧉ |
| All TCP and Nmap 5.51 top 100 UDP | 65634 | 65535 | 99 | ✎ \| 🗑 \| ⧉ |
| All TCP and Nmap 5.51 top 1000 UDP | 66534 | 65535 | 999 | ✎ \| 🗑 \| ⧉ |
| All privileged TCP | 1023 | 1023 | 0 | ✎ \| 🗑 \| ⧉ |
| All privileged TCP and UDP | 2046 | 1023 | 1023 | ✎ \| 🗑 \| ⧉ |
| All IANA assigned TCP 2012-02-10 | 5625 | 5625 | 0 | ✎ \| 🗑 \| ⧉ |
| All IANA assigned TCP and UDP 2012-02-10 | 10988 | 5625 | 5363 | ✎ \| 🗑 \| ⧉ |

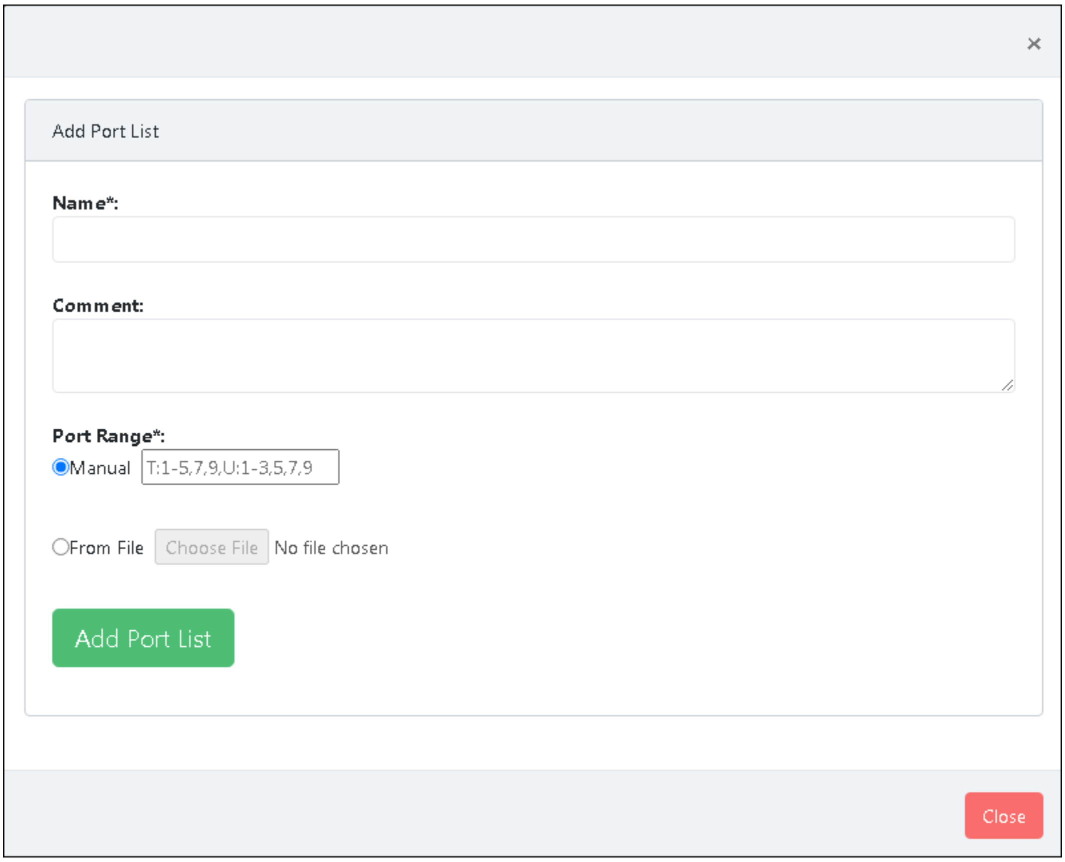
The UDP and TCP protocols support 65535 ports. In multiple cases, scanning all ports consumes time as most of the ports are normally not used. An IT company developing an application approaches IANA (Internet Assigned Numbers Authority) to reserve a port. For many scans, it is sufficient enough to scan the IANA registered ports. But, keep in mind that the registered ports are different from the privileged ports. The privileged ports are smaller than 1024 with the exception of the ports 3306/TCP (MySQL) and 1433/TCP (MS-SQL) are registered and included in the lists. The Nemasis PRO is equipped with default Port lists that contain specific TCP and UDP ports for scanning.

Normally, TCP ports get scanned fast. Operating systems that lack firewall features always respond to a TCP request and inform if the port is closed (TCP-RST) or open (TCP-ACK). The UDP ports behave in a different manner. The operating system replies consistently only if the port is closed (ICMP-Port-Unreachable). If the scanner does not get any response, it will not scan the open port. Due to this, the scanner has to wait till it gets a response. The above-mentioned case happens only with the firewall unprotected systems. If the firewall is active, it becomes difficult to discover open or closed ports.

If the application runs on a different port and needs continuous monitoring and testing by Nemasis PRO, verify the default port list and adapt it by going to **Configuration > Port List**. You can even create your very own port list that includes your specified port, by clicking **Add Port List**. Please note that you can't modify the default port lists.

# Adding a Port List

To add a Port List, click **Add Port List**.
Add Port List pop-up window appears.



×

Add Port List

Name*:

Comment:

Port Range*:
● Manual T:1-5,7,9,U:1-3,5,7,9

○ From File Choose File No file chosen

Add Port List

Close

**Name:** Enter a name for the Port List.

**Comment:** Enter a descriptive comment for the Port List.

**Port Range:** You can enter the port range either manually or by importing a CSV or TXT file. Here the alphabets **T** and **U** stand for TCP and UDP ports respectively.
Enter the port range in the following formats:

- Single port, for example, T:7, U:6
- Port Range, for example, T:1-10, U:15-250
- Multiple ports, for example T:1,3,5,7, U:150,273,375

| | |
|---|---|
| **NOTE** | The letters **T** and **U** must be entered in uppercase.<br>Ensure you enter **T:** for TCP and **U:** for UDP ports before specifying port numbers.<br>When entering ports/port range, at a time only one format should be followed. |

After filling all the fields, click **Add Port List**. The new Port List will be added to the Port Lists.

## Actions

Clicking icons in the Actions column lets you take actions regarding a Port List.

- 🗑 Delete Port List
- 📝 Edit Port List
- ❐ Clone Port List

The Port List assigned to a Target cannot be edited or deleted unless you assign it a different Port List.

- 📝 Edit Port List (in use)
- 🗑 Delete Port List (in use)

In order to edit or delete such a Port List,

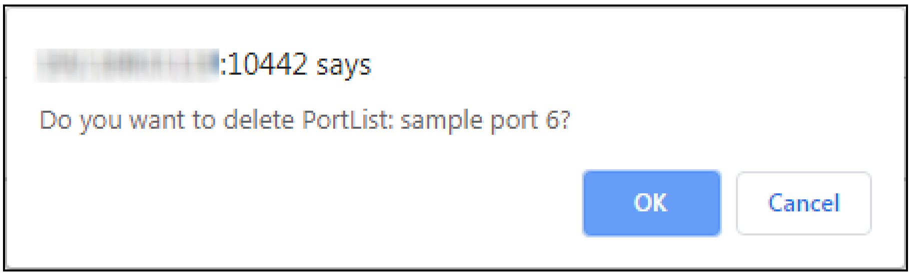
1. Go to **Configurations > Target/Group**.
   Targets list appears.
2. Find the Target to which the specific Port List is assigned and then in the **Actions** column, click 📝 (Edit Target).
   Edit Target pop-up window appears.
3. Click the **Port List** dropdown, select a different Port List and then click **Update Target.**

As the Target is assigned a different Port List, you can now edit or delete the specific Port List.

# Deleting a Port List

To delete a Port List, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete PortList: sample port 6?

2. Click **OK**.
   The Port List will be deleted.

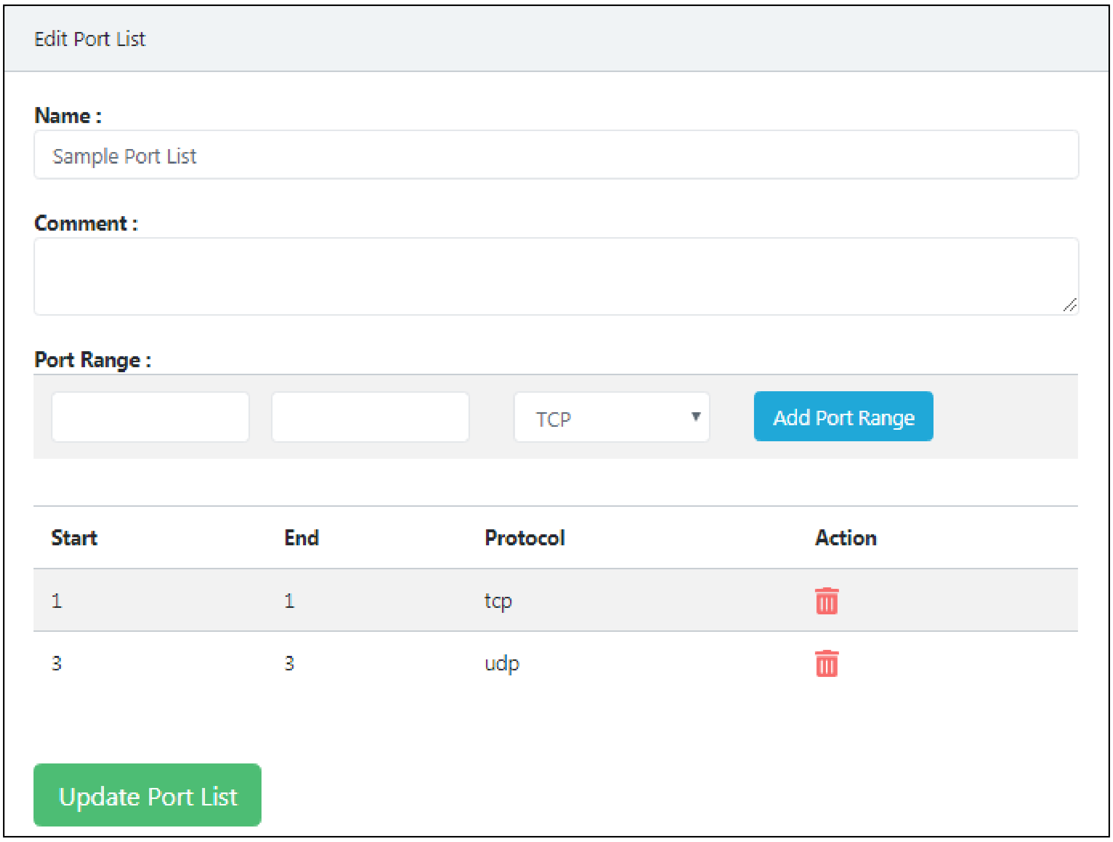
# Cloning a Port List

To clone a Port List, click ❐ in the **Actions** column. The Port List will be cloned instantly.

# Editing a Port List

To edit a Port List, follow the steps given below:

1. In the **Actions** column, click 📝.
   Edit Port List pop-up window appears.



Edit Port List

Name : Sample Port List

Comment :

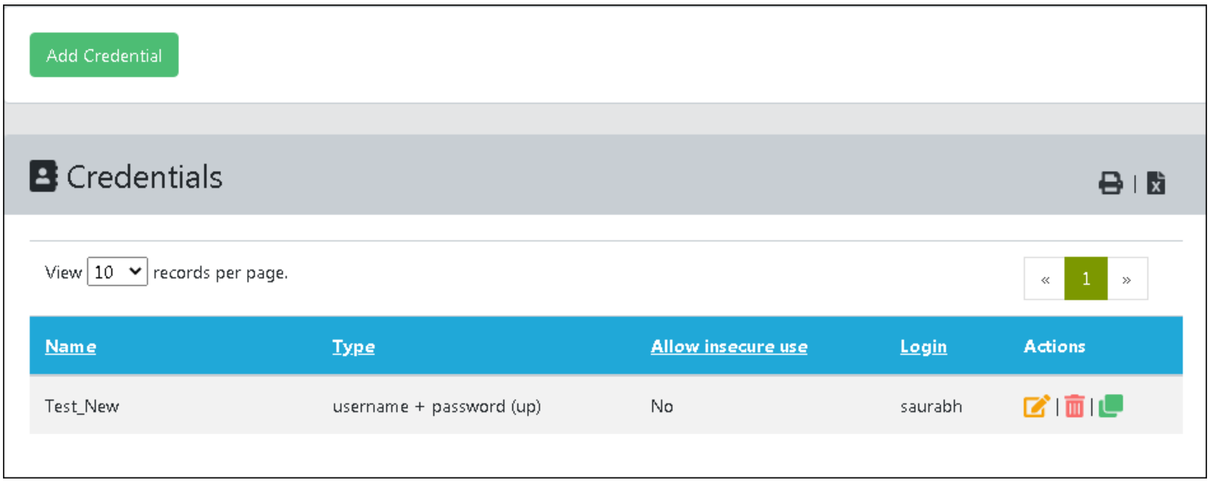
Port Range :

| Start | End | Protocol | Action |
|---|---|---|---|
| 1 | 1 | tcp | 🗑 |
| 3 | 3 | udp | 🗑 |

2. Modify the port range by clicking TCP/UDP dropdown and then click **Add Port Range**.
3. After making the necessary changes, click **Update Port List**.
   The Port List will be updated.

# Credentials

The Credentials submodule lets you add a user's login credentials by selecting a preferred authentication type for a target.



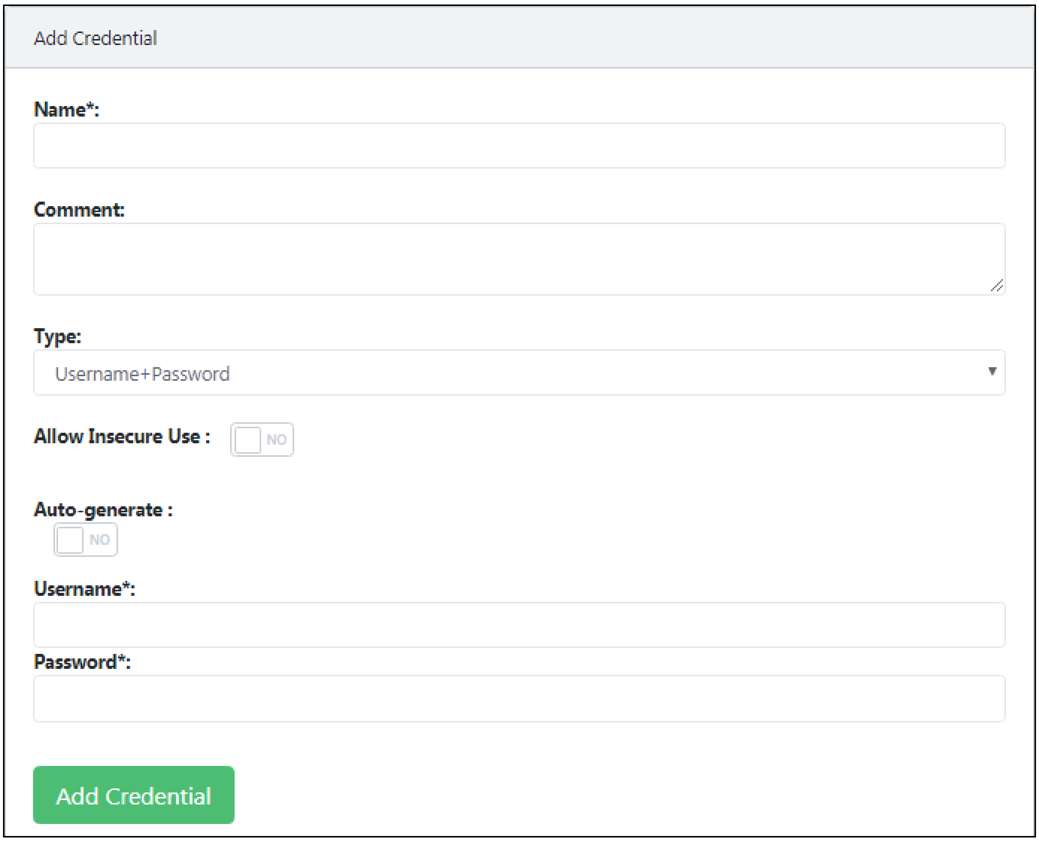
| Name | Type | Allow insecure use | Login | Actions |
|---|---|---|---|---|
| Test_New | username + password (up) | No | saurabh | |

With the login credentials, the scan plugins can log in to the target system and carry out local security checks. An authenticated scan provides you with all remotely detectable and exploitable vulnerabilities, whereas an unauthenticated scan will display only the remotely detectable vulnerabilities. You can scan the target with and without credentials, compare the results, and prioritize your attention on vulnerabilities with high severities.

During an unauthenticated scan, the Nemasis PRO will use similar protocols and techniques as a hacker to gain access of a target system and carry out tests on a target to extract the information available on software. For example, the scanner may send a malformed request to trigger a response containing more information on the software.

# Adding a Credential

To add a Credential, click **Add Credential**.
Add Credential pop-up window appears.



Add Credential

Name*:

Comment:

Type: Username+Password

Allow Insecure Use : NO

Auto-generate : NO

Username*:

Password*:

**Name:** Enter a name for the Credential.

**Comment:** Enter a descriptive comment for the Credential.

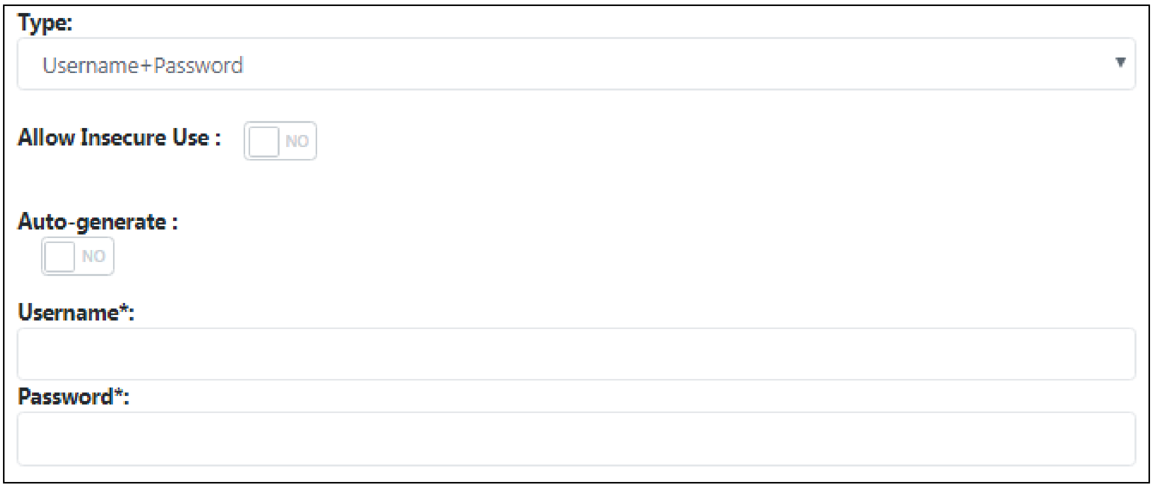
**Type:** Click the dropdown and select a preferred authentication from the following:

- Username + Password
- Username + SSH Key
- SNMP

**Allow Insecure Use:** The Nemasis PRO uses the credentials using only encrypted protocols. By default, this option is set to **NO**. If you want Nemasis PRO to use credentials without encrypted protocols, click the toggle to change it to **YES**.

**Auto-generate:** The Nemasis PRO will autogenerate a password for the Credential. By default, this option is set to **NO**. Click the toggle to change it to **YES**.

## For Username+Password type authentication



Type:

Username+Password

Allow Insecure Use : NO

Auto-generate : NO

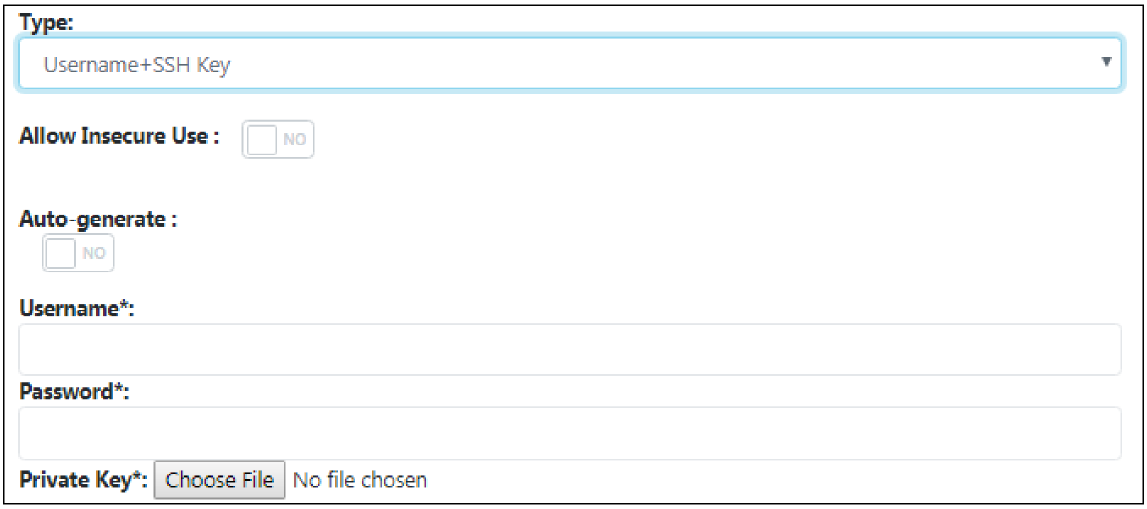
Username*:

Password*:

**Username:** Enter the username of the target system.

**Password:** Enter the password of the target system.

## For Username+SSH Key type authentication



Type:

Username+SSH Key

Allow Insecure Use : NO

Auto-generate : NO

Username*:

Password*:

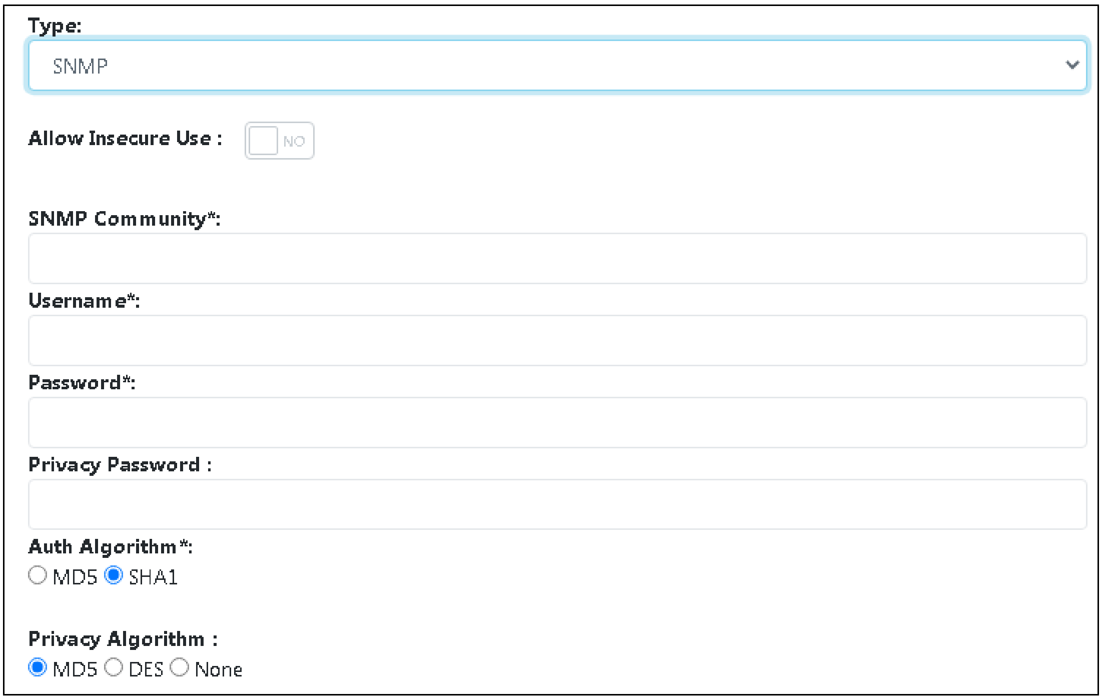
Private Key*: Choose File No file chosen

**Username:** Enter the username of the target system.

**Password:** Enter the password of the target system.

**Private Key:** The login process can be completed via SSH. Click **Choose File** and then select the private key from the destination path.

## For SNMP type authentication



Type:

SNMP

Allow Insecure Use : NO

SNMP Community*:

Username*:

Password*:

Privacy Password :

Auth Algorithm*:

○ MD5 ● SHA1

Privacy Algorithm :

● MD5 ○ DES ○ None

**SNMP Community:** Enter the protocols used for the SNMP community.

**Username:** Enter the Username for the SNMP.

**Password:** Enter the Password for the SNMP.

**Privacy password:** Enter the password to encrypt the communication in the SNMP system.

**Auth Algorithm:** Select an authentication algorithm:

- MD5
- SHA1

**Privacy Algorithm:** Select an encryption algorithm:

- AES128
- DES
- None

After filling all the fields, click **Add Credential**. The new Credential will be added to the Credentials list.

## Actions

Clicking icons in the Actions column lets you take actions regarding a Credential.

- 🗑 Delete Credential
- 📝 Edit Credential
- ⧉ Clone Credential

The Credential assigned to a Target cannot be deleted unless you assign it a different Credential.

- 🗑 Delete Credential (in use)

In order to delete such a Credential,

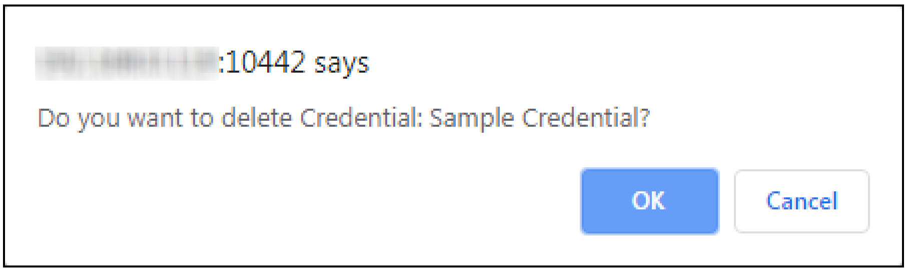
1. Go to **Configurations > Target/Group**.
   Targets list appears.
2. Find the Target to which the specific Credential is assigned and then in the Actions column, click 📝 (Edit Target).
   Edit Target pop-up window appears.
3. Click the appropriate **Credential** dropdown, select a different Credential, and then click **Update Target.**

As the Target is assigned a different Credential, you can now delete the specific Credential.

# Deleting a Credential

To delete a Credential, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete Credential: Sample Credential?

2. Click **OK**.
   The Credential will be deleted.

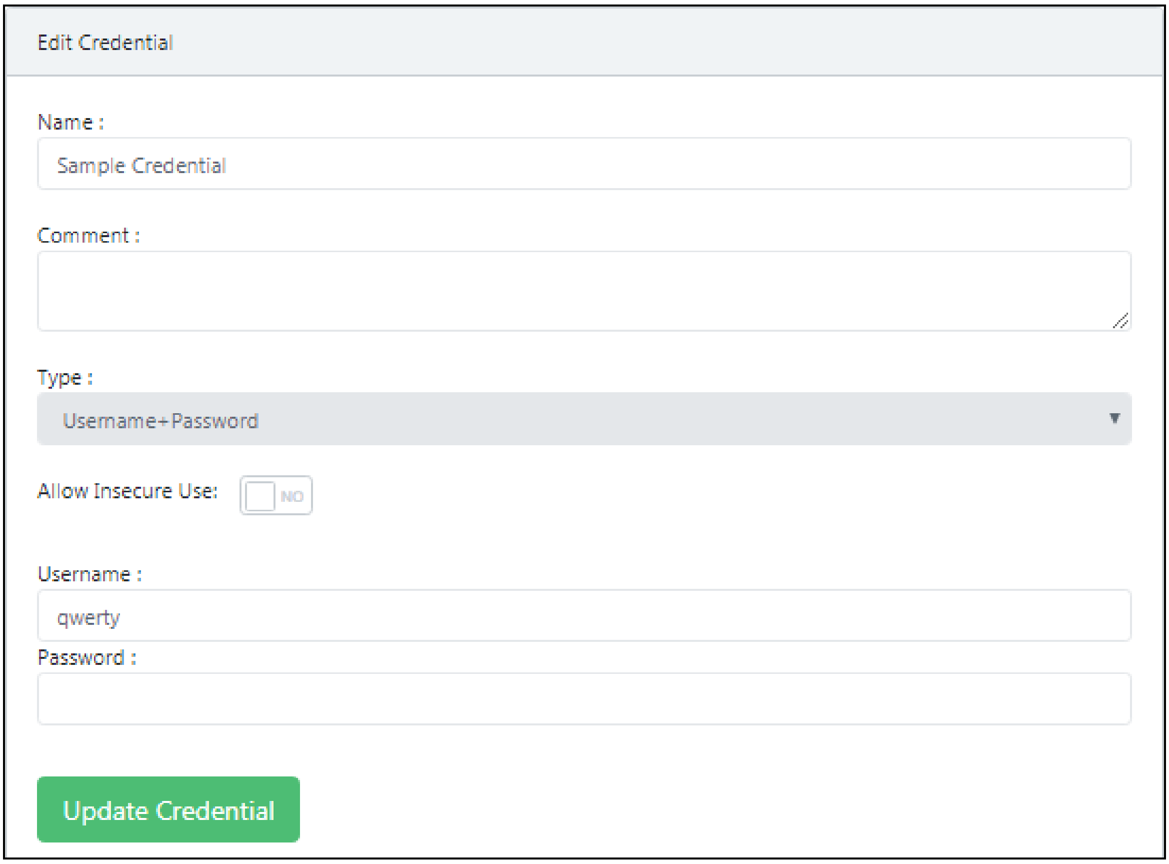
# Cloning a Credential

To clone a Credential, click ⧉ in the **Actions** column. The Credential will be cloned instantly.

# Editing a Credential

To edit a Credential, follow the steps given below:

1. In the **Actions** column, click 📝.
   Edit Credential pop-up window appears.



Edit Credential

Name : Sample Credential

Comment :

Type : Username+Password

Allow Insecure Use: NO

Username : qwerty

Password :

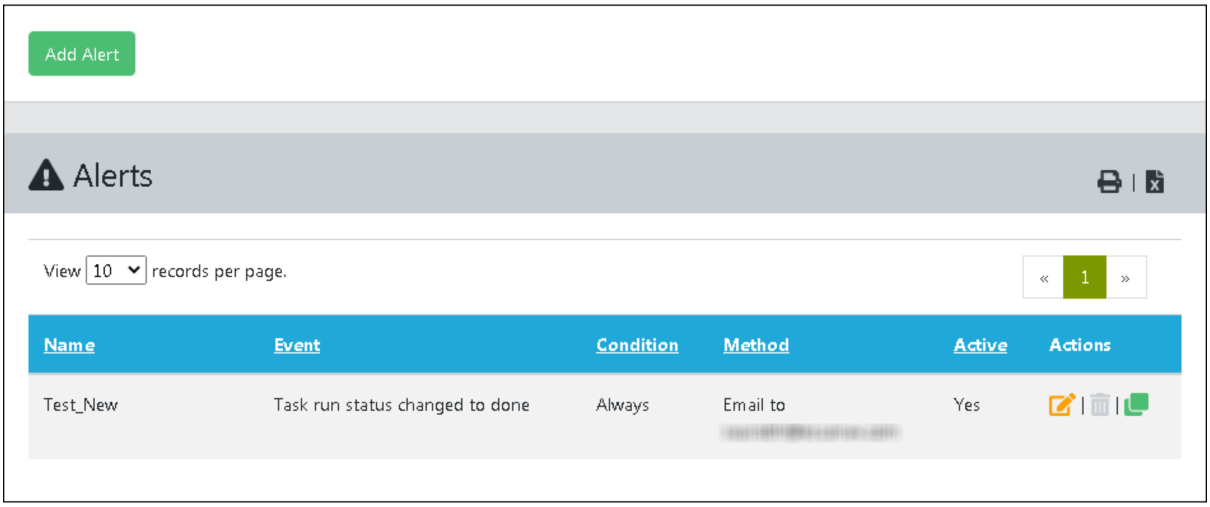
2. Make the necessary changes and then click **Update Credential**.
   The Credential will be updated.

# Alerts

After you run a task, you look forward to the scan results. You will definitely want to know whether a severe vulnerability is brought to your notice or the task in progress gets interrupted due to any reason. In such a scenario, you can configure the Nemasis PRO to send you an Alert informing you about the scan progress.

Though creating an Alert is not necessary in order to scan a Target, it will provide you updates based on the task events you have set it for. This feature comes handy when you are not constantly monitoring the scan progress or don't have access to the Nemasis PRO console.

The Alerts submodule lets you create custom alerts for a task that inform you about change in task status via email and send you the task report in XML format.

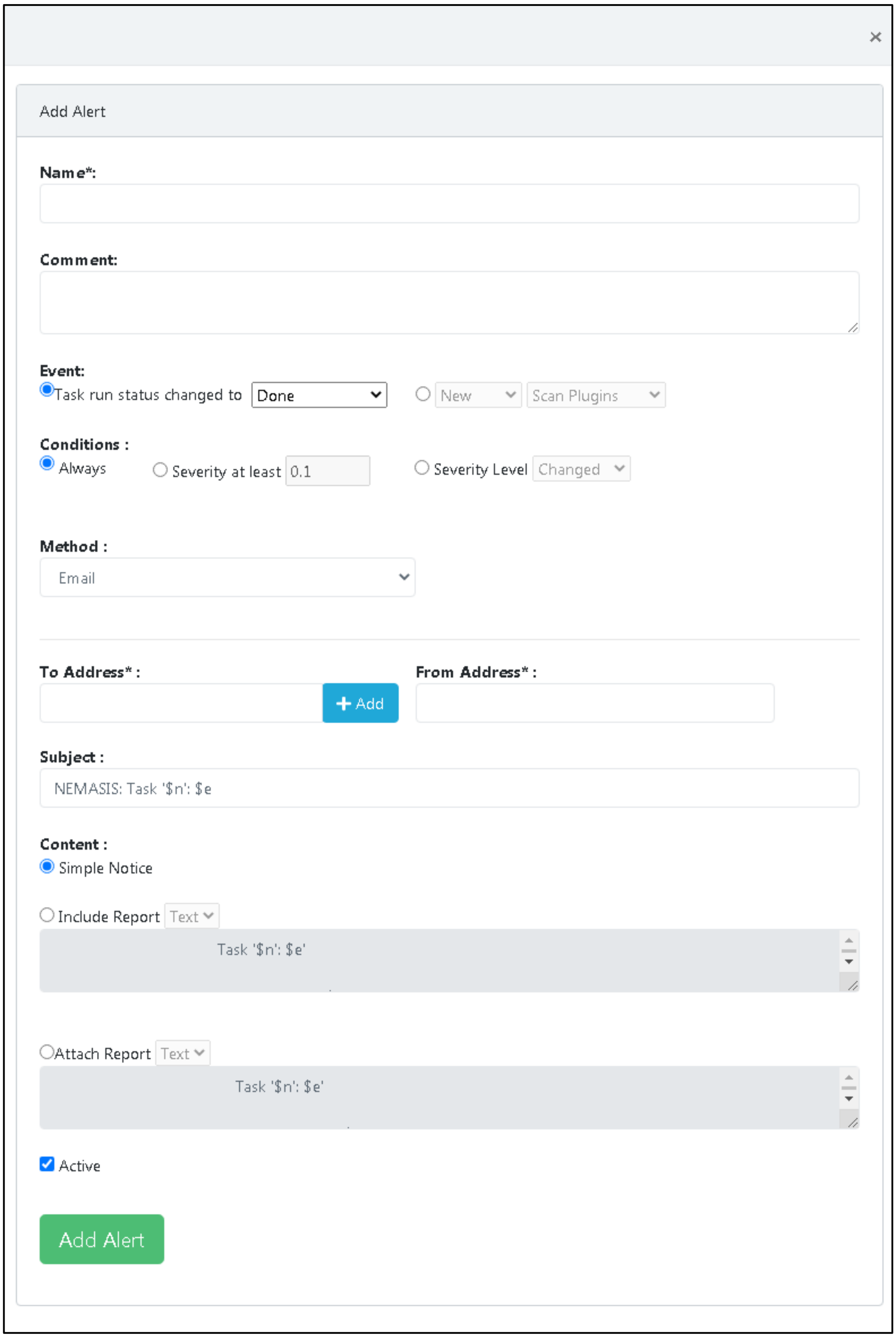


View 10 records per page.

| Name | Event | Condition | Method | Active | Actions |
|---|---|---|---|---|---|
| Test_New | Task run status changed to done | Always | Email to [redacted] | Yes | |

# Adding an Alert

To add an Alert, click **Add Alert**.
Add Alert pop-up window appears.



×

Add Alert

Name*:

Comment:

Event:
● Task run status changed to Done ○ New Scan Plugins

Conditions :
● Always ○ Severity at least 0.1 ○ Severity Level Changed

Method :
Email

To Address* : + Add

From Address* :

Subject :
NEMASIS: Task '$n': $e

Content :
● Simple Notice

○ Include Report Text
Task '$n': $e'

○ Attach Report Text
Task '$n': $e'

☑ Active

Add Alert

**Name:** Enter a name for the Alert.

**Comment:** Enter a descriptive comment for the Alert.

**Event:** You can specify when you want to receive an Alert. There are two options:

- **Task run status changed to:** Click the dropdown and select the event in which you want to receive an Alert. Following options are available:
  - Done
  - New
  - Requested
  - Running
  - Stop requested
  - Stopped
- **New/Updated:** Select whether you want to receive an Alert when the new Scan Plugins, CVEs, CPEs, and OVAL Definitions are added to the Nemasis PRO database or get updated.

**Conditions:** You can define additional conditions to be met for an event alert. You will receive an alert message on the following conditions:

- Always
- If the severity matches at least defined value
- If the severity level changes, increases or decreases

**Method:** Click the dropdown and select your preferred alert method. You can select only one method per Alert. If you want different alerts for the same event, create multiple alerts and link them to the same task.

The following methods can be used to receive an event alert.

- **Email**
- **SCP**
- **SMB**
- **Start Another Task**

## Email

**To Address:** Enter the email address to which the email alerts should be sent. You can add a maximum of 10 email addresses. After entering the email address, click **+Add**.

**From Address:** Enter the email address for the Nemasis PRO generated email.

**Subject:** Enter the subject for the email. You are free to use variables like $n (Task Name) and $e (Event Description).

**Content:** Define the email content in this field.

**Simple Notice:** You will receive a simple description of the event.

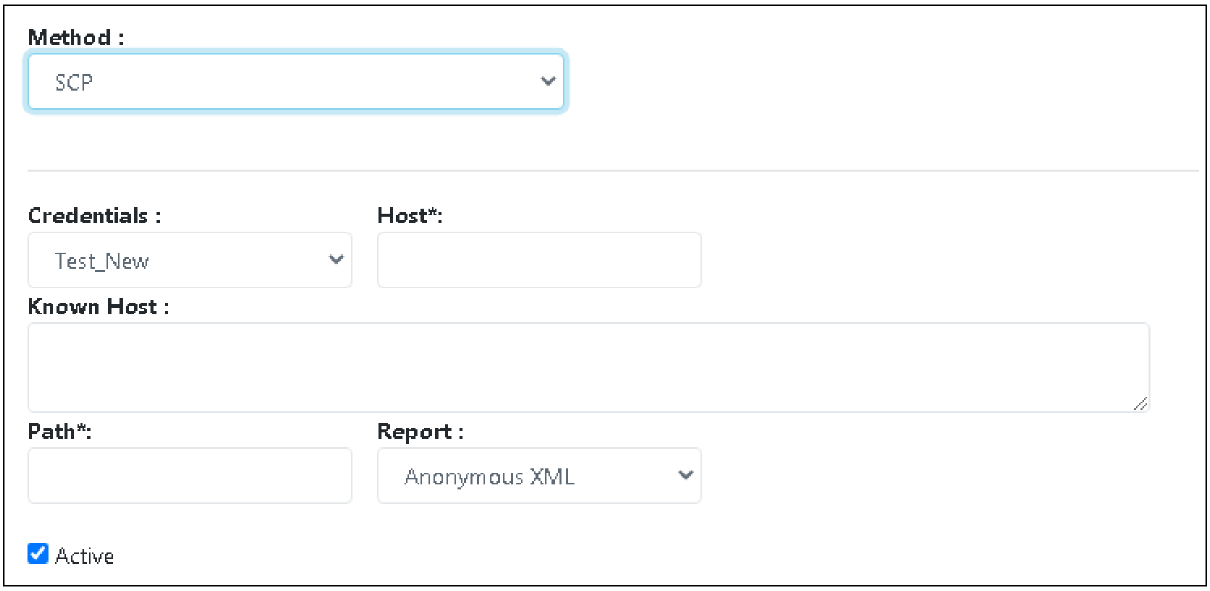
**Include Report:** If you have selected this option (Default: Done), the report will be included in the email body text. You can also select a report format that uses the content type text, as an email doesn’t directly support binary content. You can also modify the email content with the help of the following variables:

- $c Condition description
- $e Event description
- $f Filter term
- $F Name of filter
- $H Host summary
- $i Report text
- $n Task name
- $r Report format name
- $t A note if the report was truncated
- $z Time zone

**Attach Report:** If you have selected this option, the report will be sent to you as a TXT file attachment containing all the details.

## SCP

SCP stands for Secure Copy Protocol. You can copy the report to a host via SCP.



Method : SCP

Credentials : Test_New

Host*:

Known Host :

Path*:

Report : Anonymous XML

☑ Active

Enter the following variables within the filename:

- $$: $
- $n: Task Name

**Credentials:** Click the dropdown and select the credential.

**Host:** Enter the IP address of the target system.

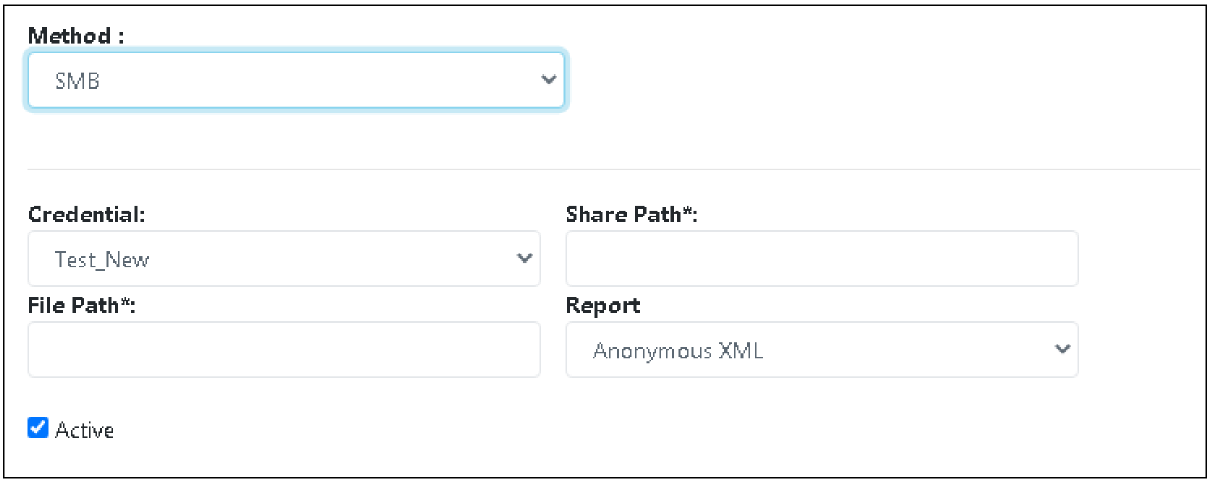
**Known Host:** Enter the public key of the remote host in this field.

**Path:** Enter the destination path where you want to the report to be stored.
For example, /Users/QA/Desktop

**Report:** Click the dropdown and select the appropriate format for Report.

## SMB

SMB stands for Server Message Block. The report can be copied to a Host via SMB.



| | |
|---|---|
| Method : | SMB |
| Credential: | Test_New |
| Share Path*: | |
| File Path*: | |
| Report | Anonymous XML |
| ☑ Active | |

Use the following variables within the filename:

- $$: $
- $n: Task Name

The Man-In-The-Middle attacks on the SMBs cannot be prevented fully as the SMB protocol doesn’t offer Fingerprinting to build mutual trust.

**Credential:** Click the dropdown and select the appropriate credential.

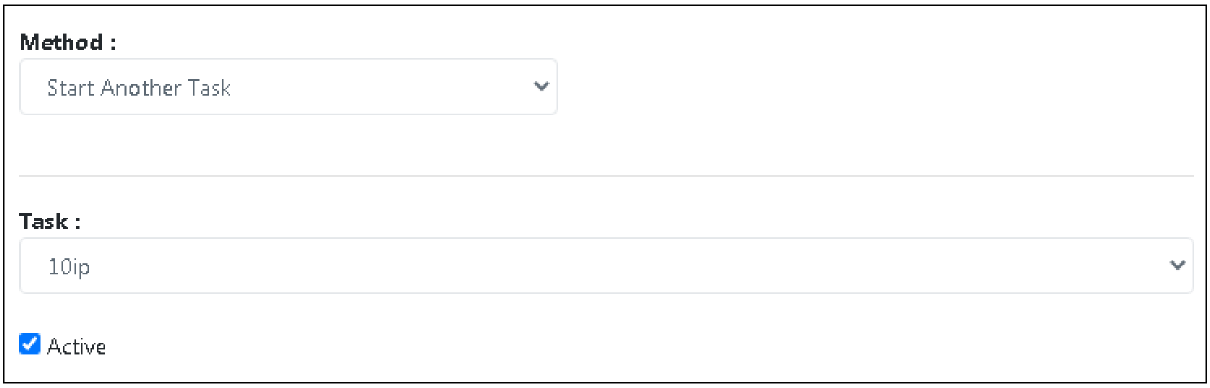
**Share Path:** Enter the path for the file to be shared. For example, \\192.168.4.157\temp

**File Path:** Enter the name for the file to be shared. For example, Task Report.txt

**Report:** Click the dropdown and select the appropriate format for the Report.

## Start Another Task

Selecting this method lets you run another task.



Method :

Start Another Task

Task :

10ip

☑ Active

**Task:** Click the dropdown and select the task you want Nemasis PRO to run after finishing the current task.

After filling all the fields, click **Add Alert**. The new Alert will be added to the Alerts list.

# Actions

Clicking icons in the **Actions** column lets you take actions regarding an Alert.

- 🗑 Delete Alert
- 📝 Edit Alert
- ❐ Clone Alert

The Alert assigned to a Task cannot be deleted unless you assign it a different Alert.

- 🗑 Delete Alert (in use)

In order to delete such an Alert,

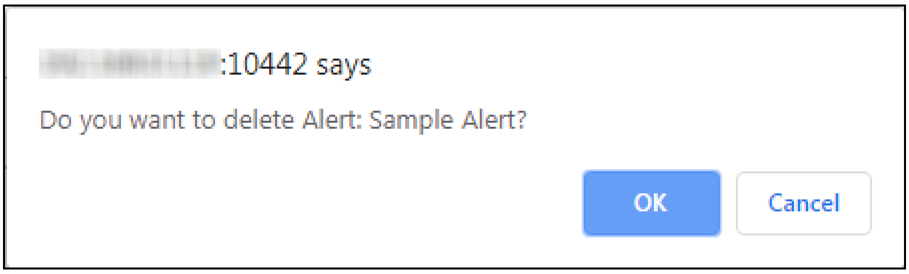
1. Go to **Scan > Task**.
   Current Tasks list appears.
2. Find the Task to which the specific Alert is assigned and then in the **Actions** column, click 📝 (Edit Task).
3. Click **Targets and Alerts** tab.
4. In the **Alerts** list, select a different Alert and then click **Update Task**.

As the Task is assigned a different Alert, you can now delete the specific Alert.

# Deleting an Alert

To delete an Alert, follow the steps given below:

1. In the Actions column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete Alert: Sample Alert?

2. Click **OK**.
   The Alert will be deleted.

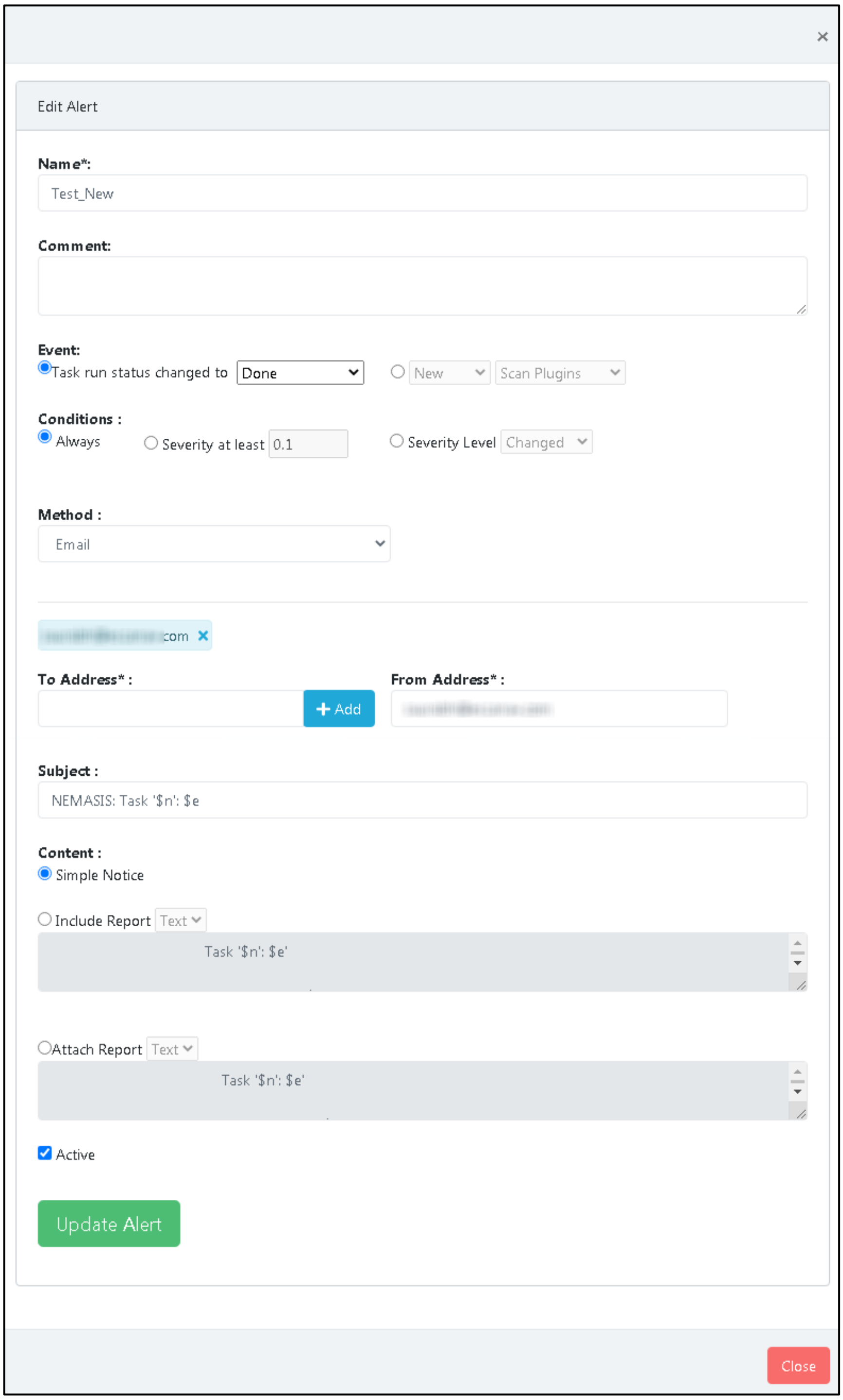
# Cloning an Alert

To clone an Alert, click ⧉ in the **Actions** column. The Alert will be cloned instantly.

# Editing an Alert

To edit an Alert, follow the steps given below:

1. In the **Actions** column, click 📝.
   Edit Alert pop-up window appears.



×

Edit Alert

**Name*:** Test_New

**Comment:**

**Event:**
● Task run status changed to Done ○ New Scan Plugins

**Conditions :**
● Always ○ Severity at least 0.1 ○ Severity Level Changed

**Method :** Email

[redacted].com ×

**To Address* :** + Add

**From Address* :** [redacted]

**Subject :** NEMASIS: Task '$n': $e

**Content :**
● Simple Notice

○ Include Report Text
Task '$n': $e'

○ Attach Report Text
Task '$n': $e'

☑ Active

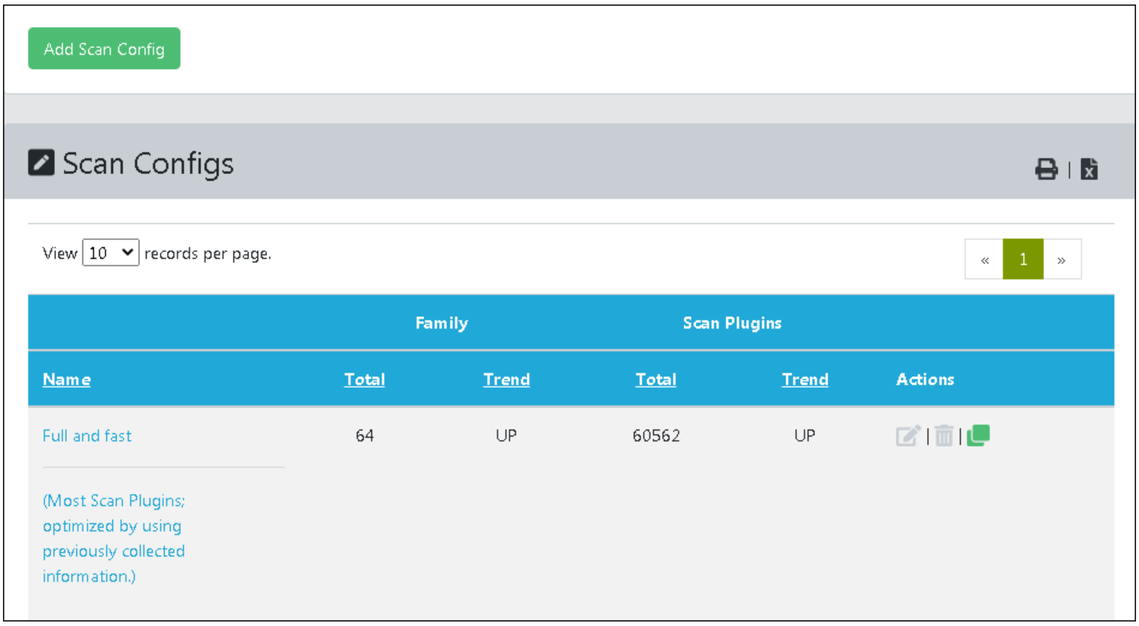
Update Alert

Close

2. Make the necessary changes and then click **Update Alert**. The Alert will be updated.

# Scan Config

The Scan Config submodule lets you customize your scans with pre-defined scan configurations and scan an endpoint.



Scan Configs

View 10 records per page.

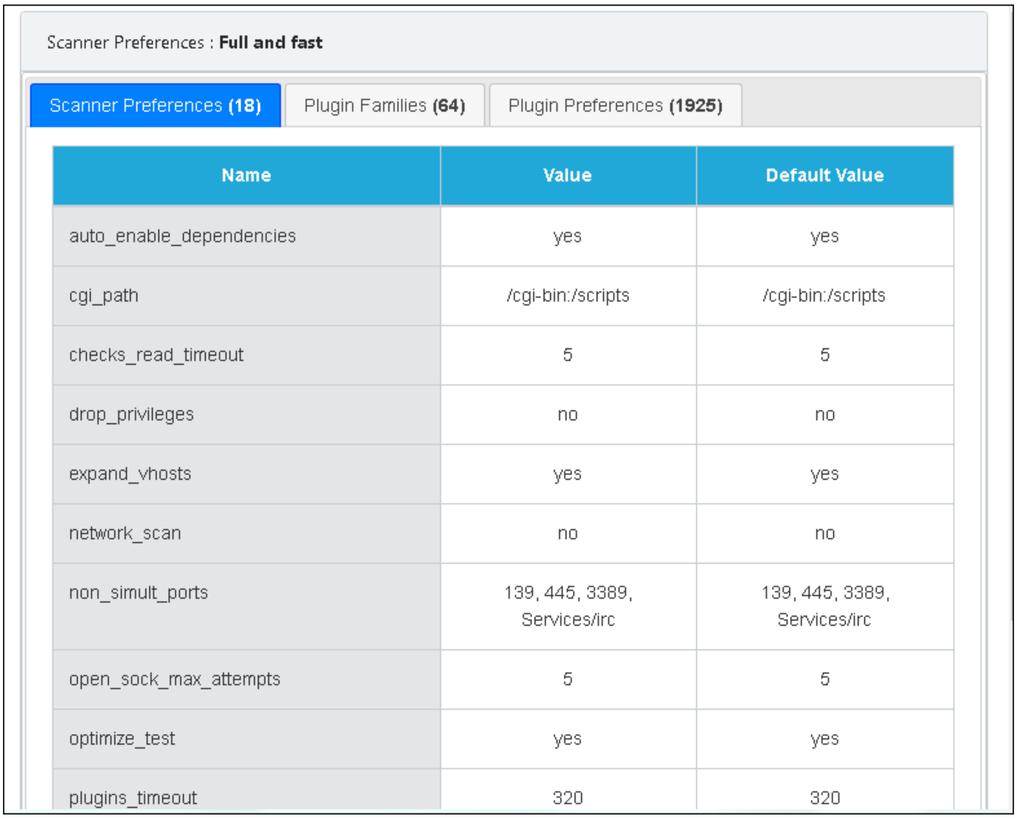
| | Family | | Scan Plugins | | |
|---|---|---|---|---|---|
| Name | Total | Trend | Total | Trend | Actions |
| Full and fast<br>(Most Scan Plugins; optimized by using previously collected information.) | 64 | UP | 60562 | UP | |

The Nemasis PRO is equipped with following scan configurations that help you scan a Target according to your requirements.

- **Full and Fast:** By default, this configuration is selected and most preferred for all environments. This configuration is based on the information gathered from the earlier port scan. It uses Scan Plugins that do not harm the target system. Also, to keep the false-negative rate low, this configuration contains optimized plugins. Compared to other configurations, it provides more value with less effort.
- **Full and Fast Ultimate:** This configuration expands the first configuration with Scan Plugins that may cause a shutdown or disrupt service.
- **Full and Very Deep:** Compared to **Full and Fast** configuration, this configuration is slow and differs in port scan results and application or service detection not having an impact on Scan Plugins selection. In this configuration, specific Scan Plugins are used that test for vulnerabilities within a service/application not detected previously or the ones that will have to wait for a timeout.
- **Empty:** If you do not want any scan configuration for the task, select this configuration.
- **Discovery:** This configuration uses Scan Plugins that provide the Target's most accurate information. This configuration does not detect any vulnerability.
- **Full and Very Deep Ultimate:** This configuration adds advanced Scan Plugins to **Full and Very Deep** configuration that may cause a system or service disruptions.
- **Host Discovery:** In this configuration, specific Scan Plugins are used that discover a target system. The report contains only the list of discovered systems.

- **System Discovery:** This configuration uses Scan Plugins that discover target systems along with hardware in use and installed operating systems.

By clicking a Scan Config, you can view its current and default value.



Scanner Preferences : **Full and fast**

| Name | Value | Default Value |
|---|---|---|
| auto_enable_dependencies | yes | yes |
| cgi_path | /cgi-bin:/scripts | /cgi-bin:/scripts |
| checks_read_timeout | 5 | 5 |
| drop_privileges | no | no |
| expand_vhosts | yes | yes |
| network_scan | no | no |
| non_simult_ports | 139, 445, 3389, Services/irc | 139, 445, 3389, Services/irc |
| open_sock_max_attempts | 5 | 5 |
| optimize_test | yes | yes |
| plugins_timeout | 320 | 320 |

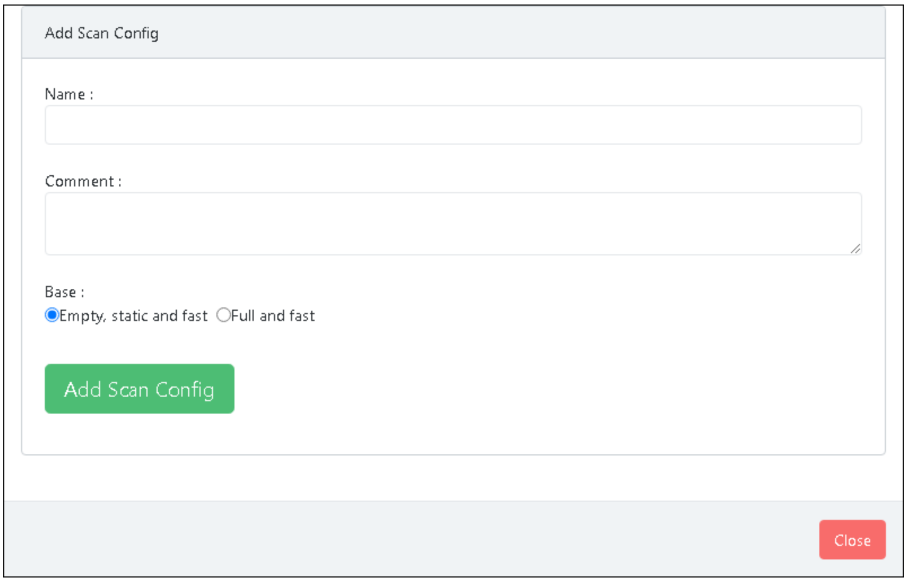
- **auto_enable_dependencies**: The scan plugins that are required by other scan plugins will be activated automatically.
- **cgi_path**: The scan plugins will use this path to access CGI scripts.
- **checks_read_timeout**: This is the timeout for the network sockets during a scan.
- **drop_privileges**: If this option is enabled, the Nemasis PRO will lose its root privileges before a scan. While this does increase the security but the results display fewer findings with few Scan Plugins.
- **network_scan**: This option scans the network in one go instead of starting Nmap for every individual host. For specific environments, this option can save a lot of time.
- **non_simult_ports**: These ports are not being tested simultaneously by scan plugins.
- **optimize_test**: The scan plugins will only be run against a host; only if specific pre-requisites are met (i.e. detected an application or open port).
- **plugins_timeout**: It is the maximum run time of scan plugins.
- **report_host_details**: The report contains detailed information of the host.
- **safe_checks**: While scanning for vulnerabilities, some scan plugins may cause damage to the host system. This setting disables those specific scan plugins.

- **scanner_plugins_timeout**: This is the maximum lifetime (in seconds) for all Scan Plugins from the Port scanners family. If a Scan Plugin runs longer, the plugin gets terminated.

- **time_between_request**: This option lets you set a wait time (in milliseconds) between two actions like opening a TCP socket, sending a request through the open TCP socket, and closing the TCP socket.
- **timeout_retry**: The maximum number of retries allowed when a socket connection attempt times out.
- **unscanned_closed**: This parameter defines if TCP ports that were not scanned should be treated as closed ports.
- **unscanned_closed_udp**: This parameter defines if UDP ports that were not scanned should be treated as closed ports.

## Adding a Scan Config

To add a Scan Configuration, click **Add Scan Config**.
Add Scan Config pop-up window appears.



Add Scan Config

Name :

Comment :

Base :

● Empty, static and fast ○ Full and fast

**Name:** Enter a name for the Scan Configuration.

**Comment:** Enter a descriptive comment for the Scan Configuration.

**Base:** Select a base scan of your preference. There are two options available:

- **Empty, static, and fast:** Select this scan configuration to scan the target by using a particular scan plugin or family. For example, if you want to scan a target for only CISCO vulnerabilities, you can edit the scan configuration and select all plugins or few plugins for the CISCO family.
- **Full and fast:** Select this scan configuration to scan the target by using all scan plugin families.

After filling all the fields and selecting a base scan configuration, click **Add Scan Config**. The new Scan Configuration will be added to the Scan Config list.

## Actions

Clicking icons in the Actions column lets you take actions regarding a Scan Config.

- 🗑 Delete Scan Config
- 📝 Edit Scan Config
- ❐ Clone Scan Config

The Scan Config assigned to a Target cannot be edited or deleted unless you assign it a different Scan Config.

- 📝 Edit Scan Config (in use)
- 🗑 Delete Scan Config (in use)

In order to edit or delete such a Scan Config,

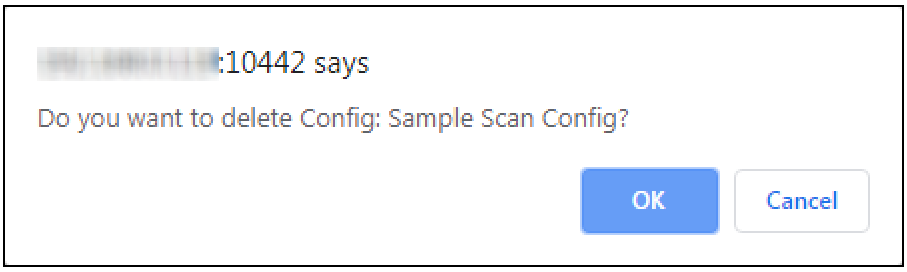
1. Go to **Scan > Task**.
   Current Tasks list appears.
2. Find the Task to which the specific Scan Config is assigned and then in the Actions column, click 📝 (Edit Task).
   Edit Task pop-up window appears.
3. Click the **Scanner and Config** tab**.**
4. Click the **Scan Config** dropdown, select a different Scan Config, and then click **Update Task**.

As the Task is assigned a different Scan Config, you can now edit or delete the specific Scan Config.

# Deleting a Scan Config

To delete a Scan Config, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete Config: Sample Scan Config?

2. Click **OK**.
   The Scan configuration will be deleted.

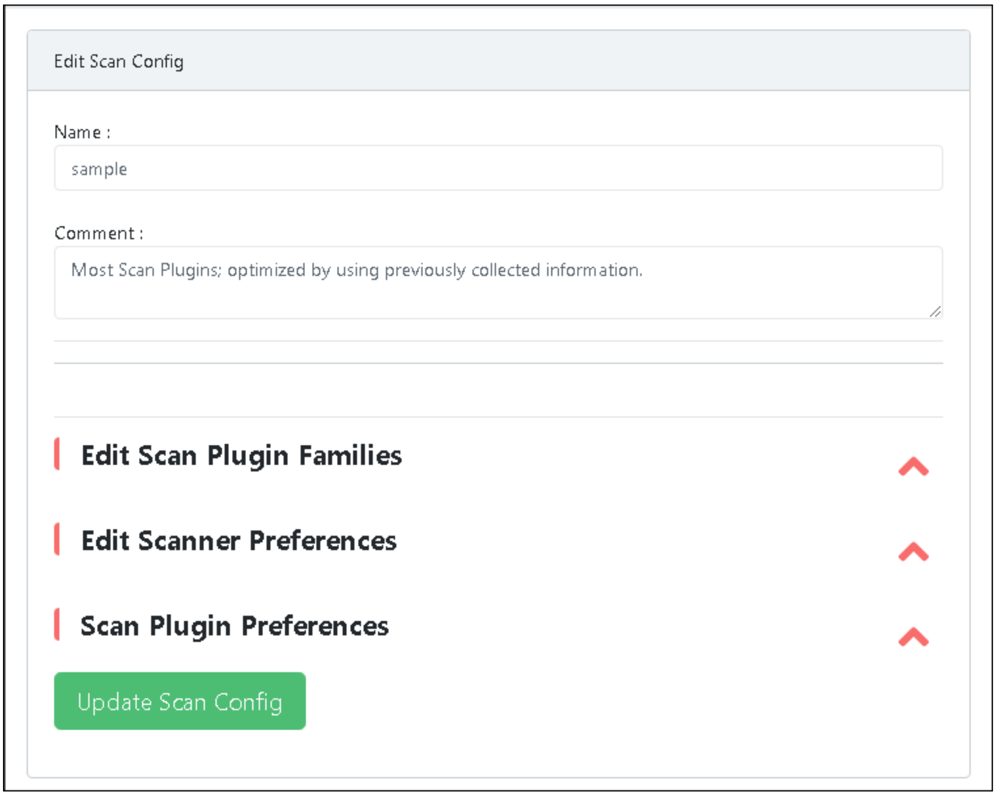
# Cloning a Scan Config

To clone a Scan Config, click ❐ in the **Actions** column. The Scan Config will be cloned instantly.

# Editing a Scan Config

To edit a Scan Config, follow the steps given below:

1. In the **Actions** column, click 📝.
   Edit Scan Config pop-up window appears.



Edit Scan Config

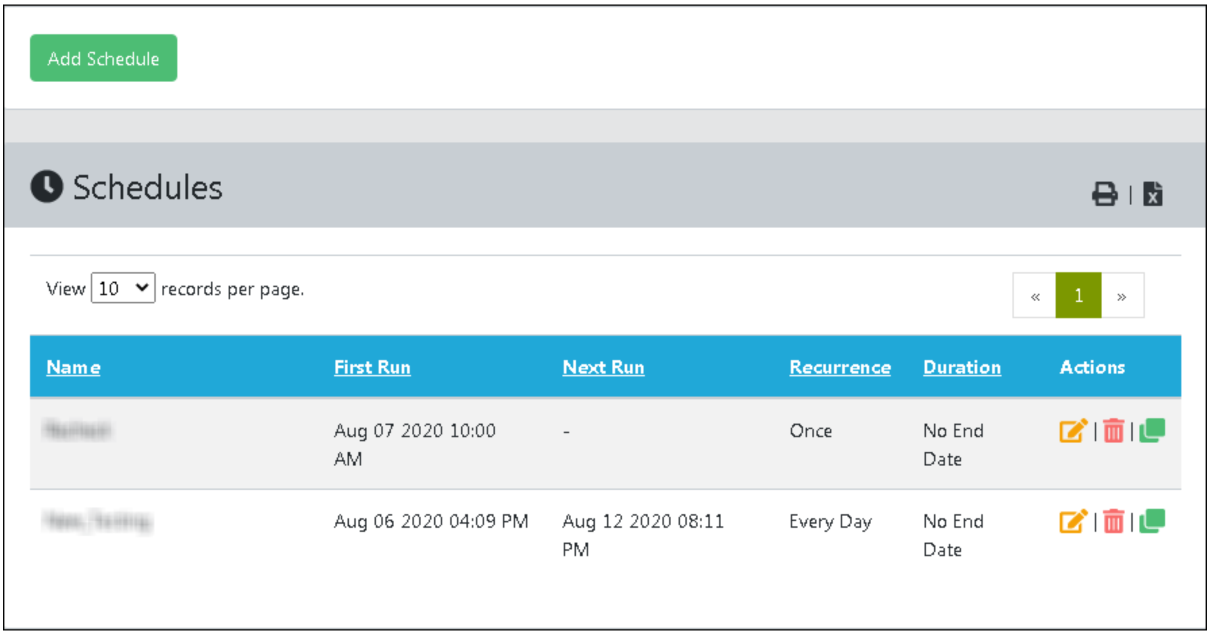
Name : sample

Comment : Most Scan Plugins; optimized by using previously collected information.

2. Make the necessary changes and then click **Update Scan Config**.
   The Scan Config will be updated.

# Schedule

The Schedule submodule lets you create a schedule and run a task according to your customized timings.



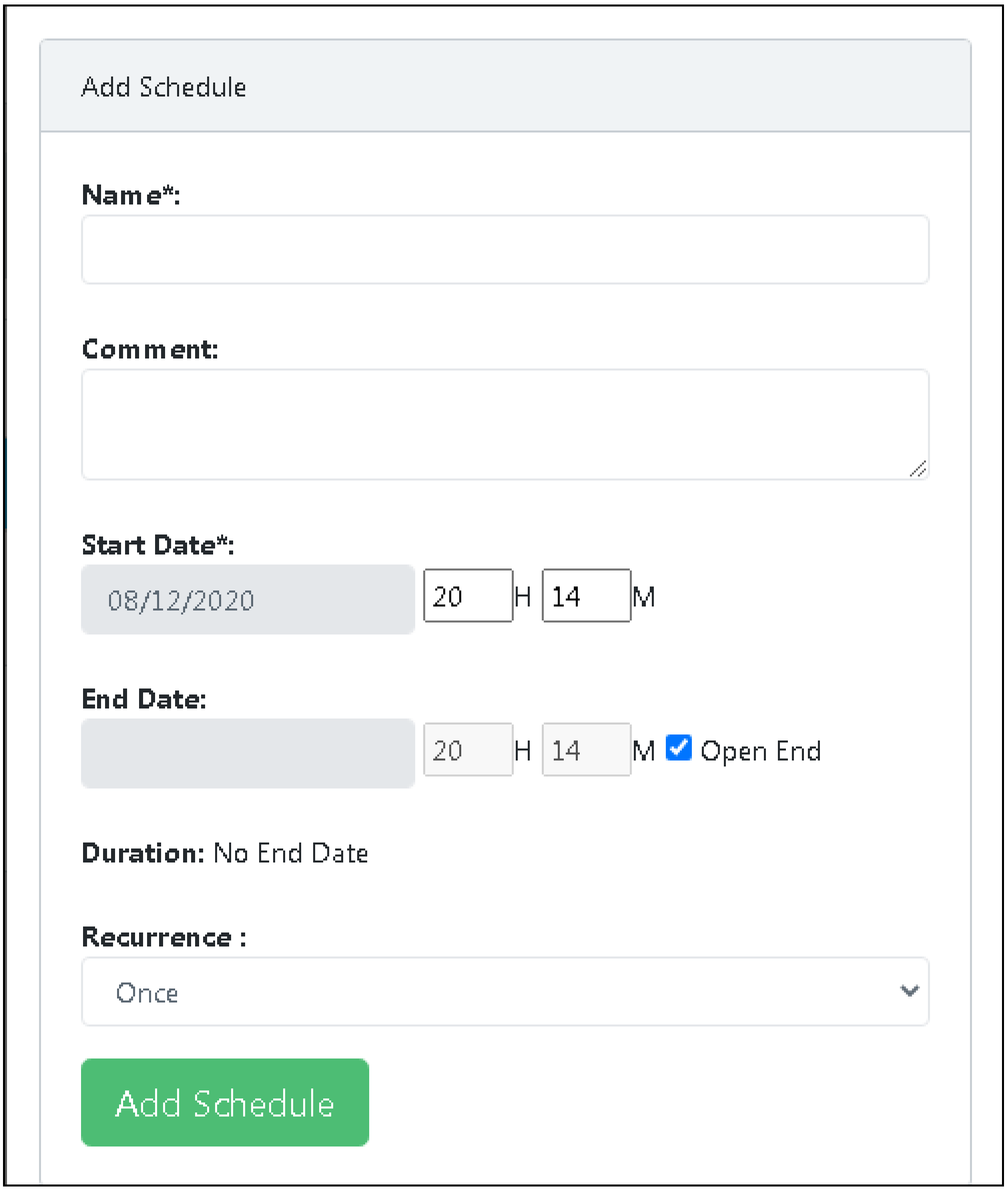
Schedules

View 10 records per page.

| Name | First Run | Next Run | Recurrence | Duration | Actions |
|---|---|---|---|---|---|
| [redacted] | Aug 07 2020 10:00 AM | - | Once | No End Date | ✎ \| 🗑 \| ⧉ |
| [redacted] | Aug 06 2020 04:09 PM | Aug 12 2020 08:11 PM | Every Day | No End Date | ✎ \| 🗑 \| ⧉ |

# Adding a Schedule

To add a Schedule, click **Add Schedule**.
Add schedule pop-up window appears.



Add Schedule

Name*:

Comment:

Start Date*: 08/12/2020 20 H 14 M

End Date: 20 H 14 M ☑ Open End

Duration: No End Date

Recurrence : Once

**Name:** Enter a name for the Schedule.

**Comment:** Enter a descriptive comment for the Schedule.

**Time Zone:** Click the dropdown and select the Time Zone according to your region.

**Start Date:** Select a date and time by which you want the Schedule to run.

**End date:** Select a date and time by which you want the Schedule to end.

**Open End:** Select this checkbox if you want the Task to run at regular intervals. After selecting the checkbox, the **End Date** field will be disabled.

**Duration:** The Duration displays the number of hours for which the Schedule will run.

**Recurrence:** Click the dropdown and select the option on which you want the Schedule to recur. The following options are available.

- Once
- Hourly
- Daily
- Weekly
- Monthly
- Yearly
- Workweek (Mon-Fri)

After filling all the fields, click **Add Schedule**. The new Schedule will be added to the Schedules list.

## Actions

Clicking icons in the **Actions** column lets you take actions regarding a Schedule.

- 🗑 Delete Schedule
- ✎ Edit Schedule
- ⧉ Clone Schedule

The Schedule assigned to a Task cannot be edited or deleted unless you assign it a different Target.

- ✎ Edit Schedule (in use)
- 🗑 Delete Schedule (in use)

In order to edit or delete such a Schedule,

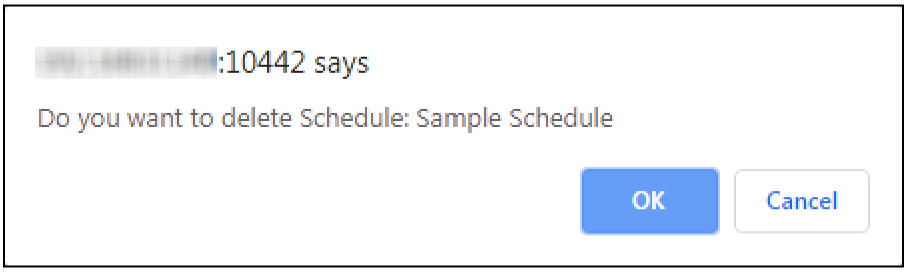
1. Go to **Scan** > **Task**.
   Current Tasks list appears.
2. Find the Task to which the specific Schedule is assigned and then in the **Actions** column, click ✎ (Edit Task).
   Edit Task pop-up window appears.
3. Click the **Target and Alerts** tab.
4. Click the **Schedule** dropdown, select a different Schedule, and then click **Update Task**.

As the Task is assigned a different Schedule, you can now edit or delete the specific Schedule.

# Deleting a Schedule

To delete a Schedule, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



[redacted]:10442 says

Do you want to delete Schedule: Sample Schedule

2. Click **OK**.
   The Schedule will be deleted.

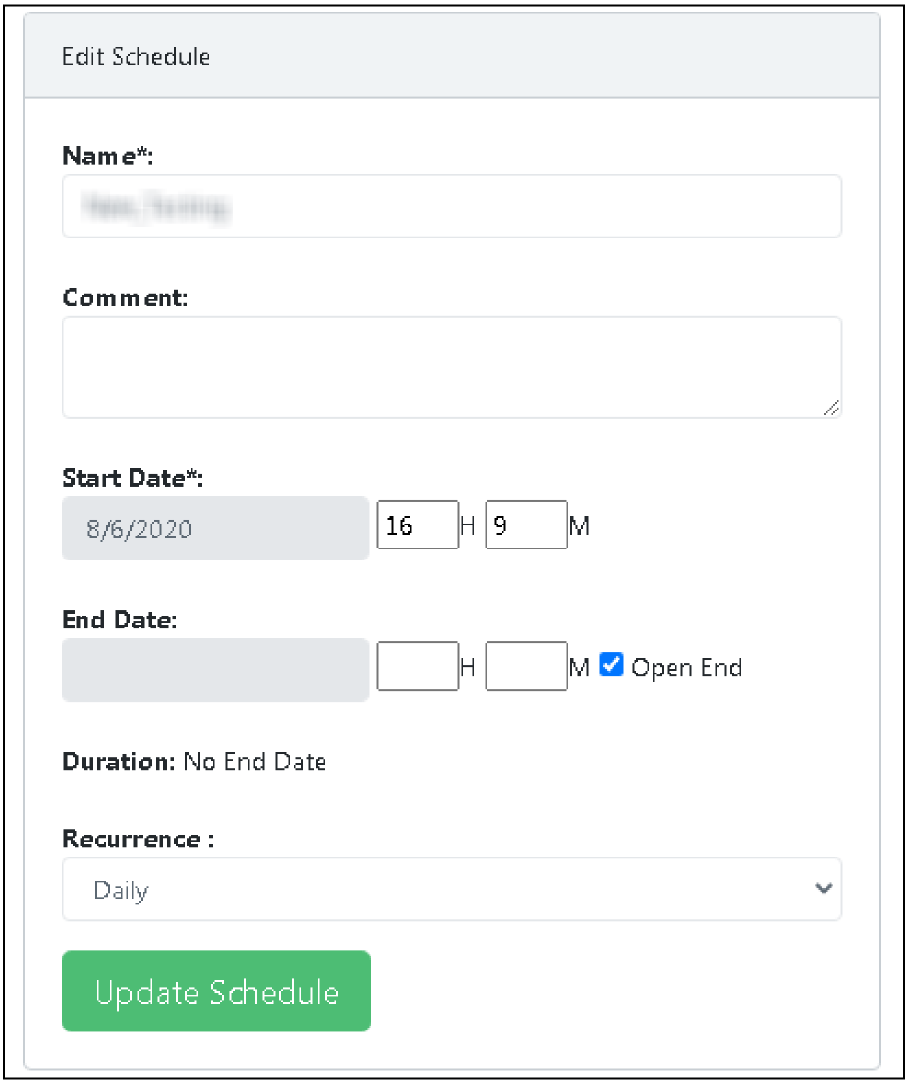
# Cloning a Schedule

To clone a Schedule, click ⧉ in the Actions column. The Schedule will be cloned instantly.

# Editing a Schedule

To edit a Schedule, follow the steps given below:

1. In the **Actions** column, click ✎.
   Edit Schedule pop-up window appears.



Edit Schedule

**Name*:** [redacted]

**Comment:**

**Start Date*:** 8/6/2020 16 H 9 M

**End Date:** H M ☑ Open End

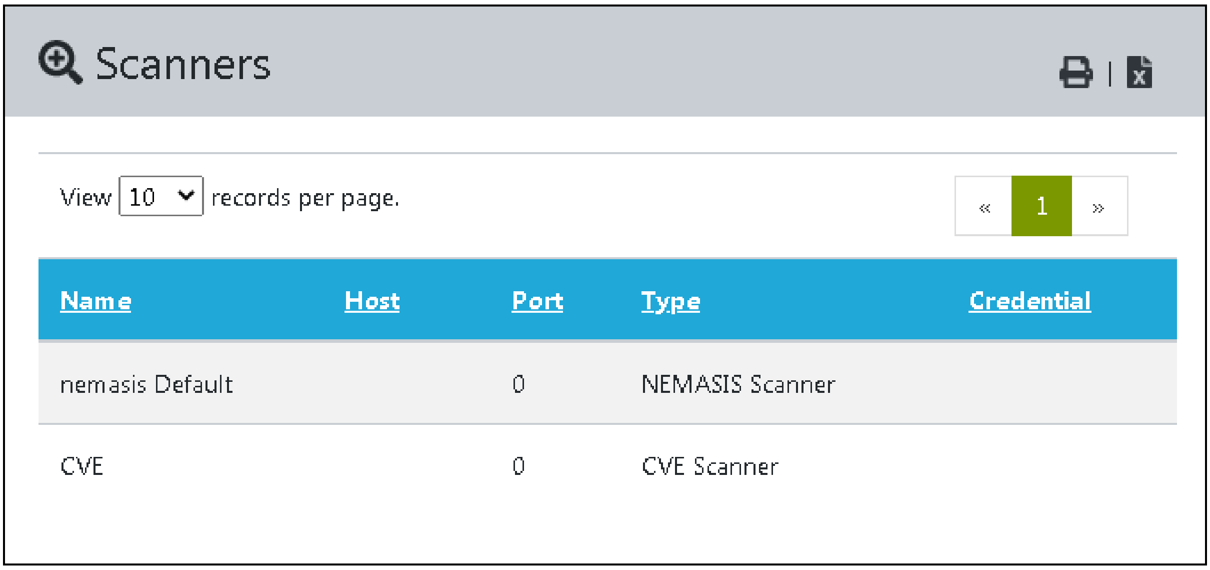
**Duration:** No End Date

**Recurrence :** Daily

2. Make the necessary changes and then click **Update Schedule**.
   The Schedule will be updated.

# Scanners

The Nemasis PRO is equipped with Nemasis Scanner and CVE Scanner engines. Both the scan engines are core programs loaded with comprehensive protection capabilities that protect systems against known threats.



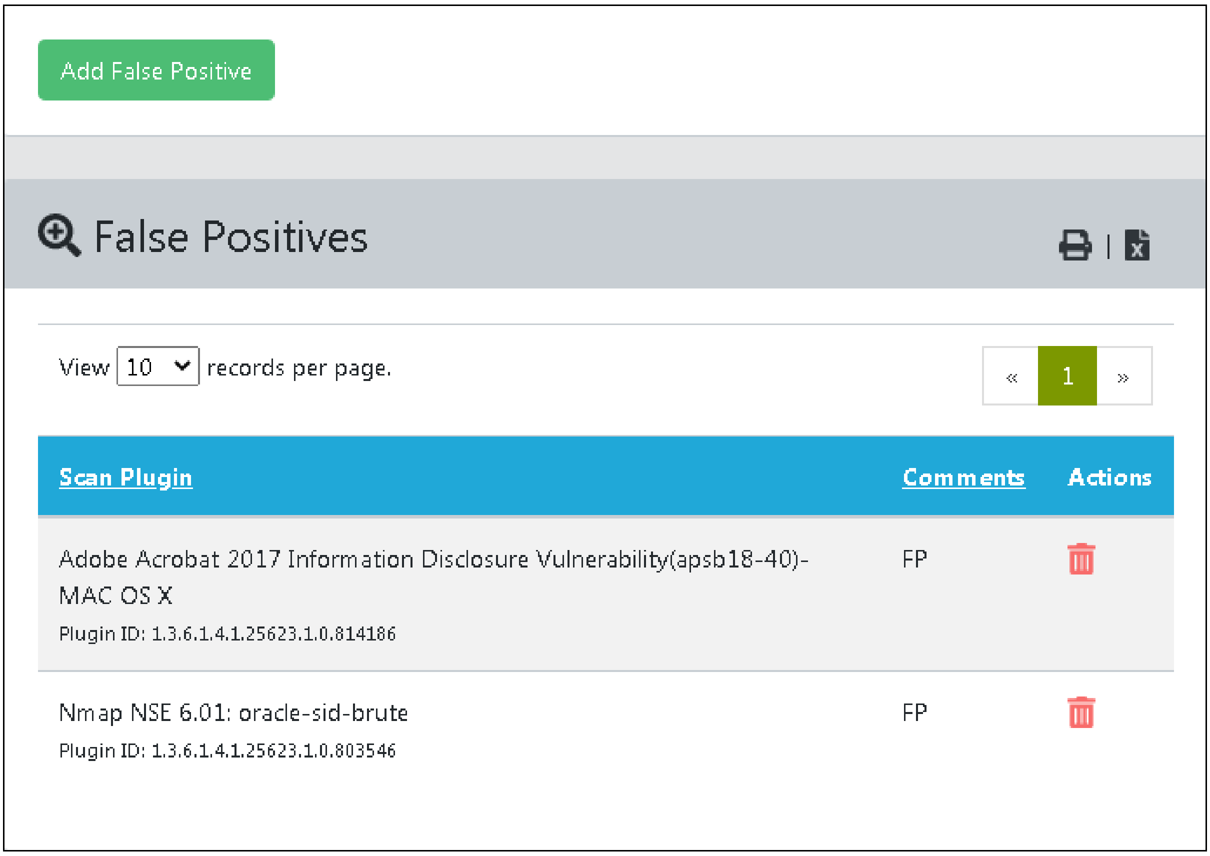
Scanners

View 10 records per page.

| Name | Host | Port | Type | Credential |
|---|---|---|---|---|
| nemasis Default |  | 0 | NEMASIS Scanner |  |
| CVE |  | 0 | CVE Scanner |  |

# False Positive

The False Positive is a scan finding that wrongly identifies a particular condition as vulnerability. This submodule lets you detect a false positive in an endpoint by selecting a Scan Plugin and severity level. It also lets you add a False Positive.



False Positives

View 10 records per page.

| Scan Plugin | Comments | Actions |
|---|---|---|
| Adobe Acrobat 2017 Information Disclosure Vulnerability(apsb18-40)-MAC OS X<br>Plugin ID: 1.3.6.1.4.1.25623.1.0.814186 | FP | 🗑 |
| Nmap NSE 6.01: oracle-sid-brute<br>Plugin ID: 1.3.6.1.4.1.25623.1.0.803546 | FP | 🗑 |

Vulnerability scanners frequently find evidence that points to a security issue. In such cases, the final prediction is impossible. But, now there are two options available.

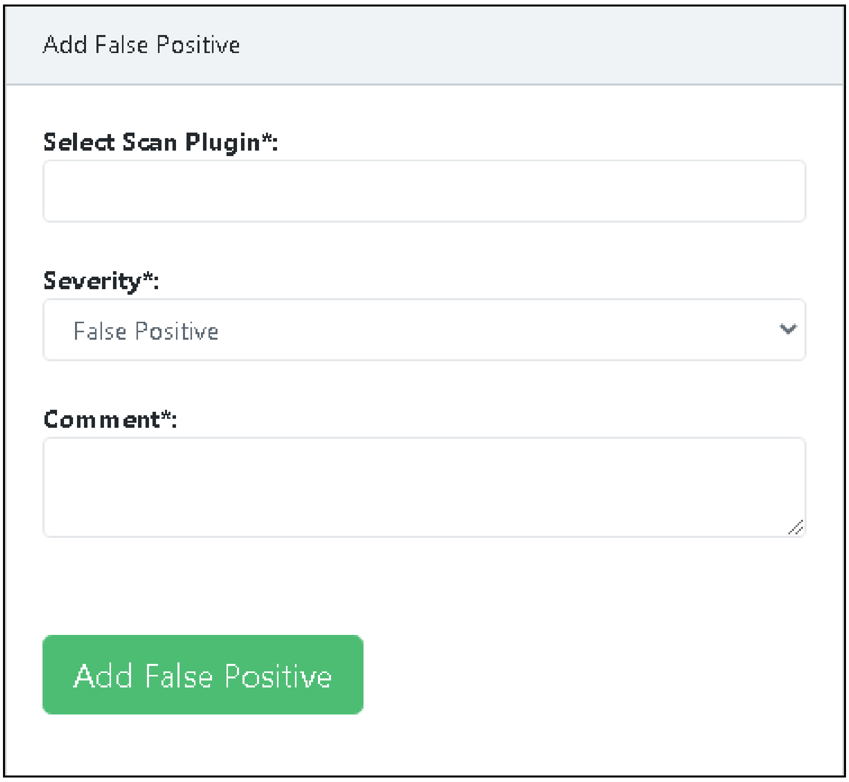
- Reporting a potential non-existent vulnerability (False Positive).
- Failing to report a potential existent vulnerability (False Negative).

A user can identify, manage, and handle False Positives, but not the False Negatives. The Nemasis PRO reports all potentially existing vulnerabilities and assists in their categorization.

This problem is common amongst Enterprise Linux distributions. For example, in version 4.4 an SSH service is installed and during a connection request, the software reports the version. The vulnerability scanner that knows of vulnerability in this particular version will identify and report it as such. Even if the vendor fixed the vulnerability and released an updated version it still reports to the outside version 4.4 and this is where vulnerability scanners fail to differentiate. If the administrator identifies such a situation, he/she can make sure that this finding is not displayed next time.

# Adding a False Positive

To add a False Positive, click **Add False Positive**.
Add False Positive pop-up window appears.



Add False Positive

Select Scan Plugin*:

Severity*: False Positive

Comment*:

**Select Scan Plugin:** Enter your finding and select the appropriate from the list.

**Severity:** You can modify the severity of the vulnerability. Click the dropdown to modify the severity of a finding. The dropdown consists of the following options:

- **High** – The finding will be given severity rating as High.
- **Medium** – The finding will be given severity rating as Medium.
- **Low** – The finding will be given severity rating as Low.
- **Log** – The finding will only be logged and no further action will be taken.
- **False Positive** – The finding will be recorded as a False Positive.

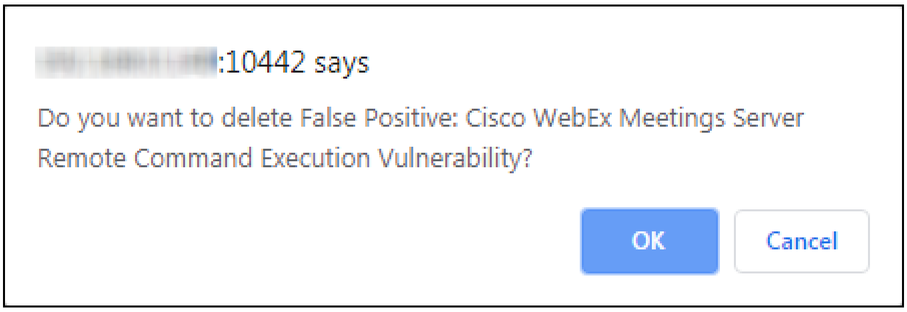
**Comment:** Enter a descriptive comment for the False Positive.

After filling all the fields, click **Add False Positive**. The new False Positive will be added to the False Positives list.

# Deleting a False Positive

To delete a False Positive, follow the steps given below:

1. In the **Actions** column, click 🗑.
   A delete confirmation prompt appears.



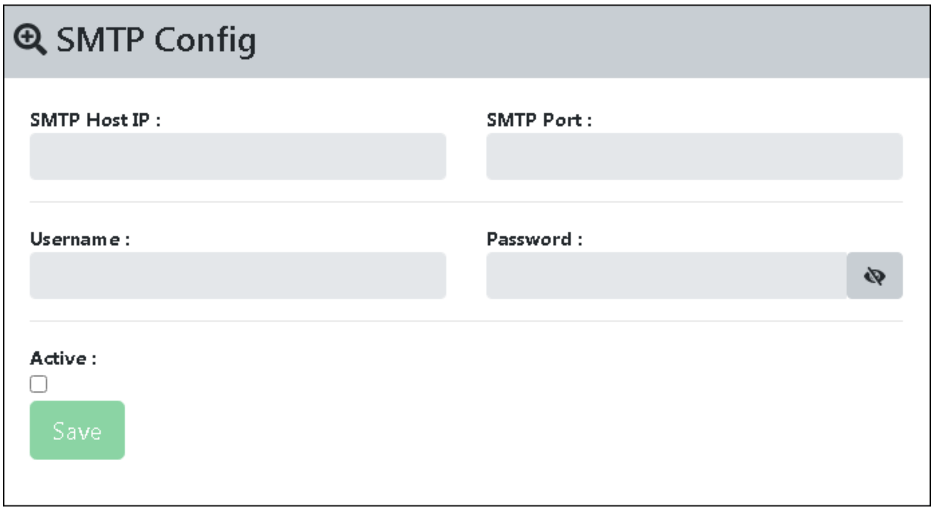
[redacted]:10442 says

Do you want to delete False Positive: Cisco WebEx Meetings Server Remote Command Execution Vulnerability?

2. Click **OK**.
   The False Positive will be deleted.

# SMTP

With the SMTP submodule, you provide SMTP server access and allow Nemasis PRO to send emails.



SMTP Config

SMTP Host IP :

SMTP Port :

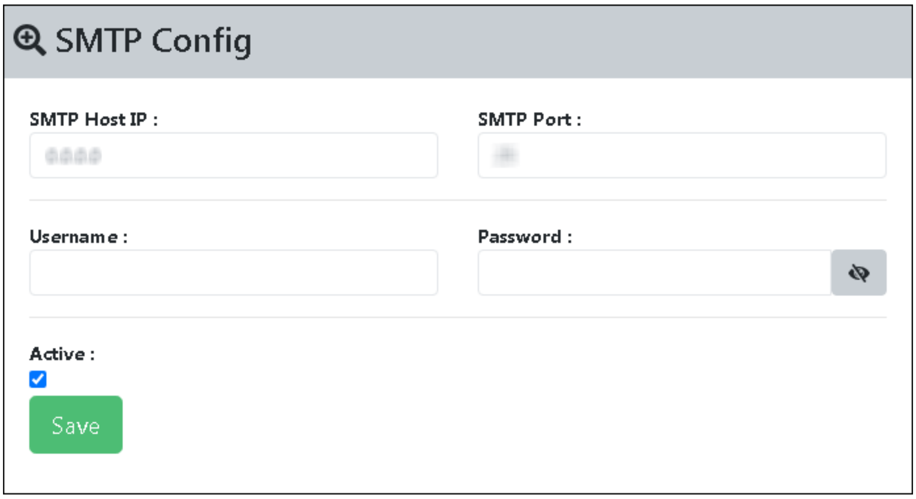
Username :

Password :

Active :

□

Select **Active** Checkbox. This will enable all the fields.



SMTP Config

SMTP Host IP :

SMTP Port :

Username :

Password :

Active :

☑

**SMTP Host IP:** Enter IP address of system on which the SMTP server is installed.

**SMTP Port:** Enter the SMTP Port number.

**Username/Password:** If required, enter your SMTP server’s login credentials in the respective fields.

- 👁 SMTP Password is visible
- 🚫 SMTP Password is hidden

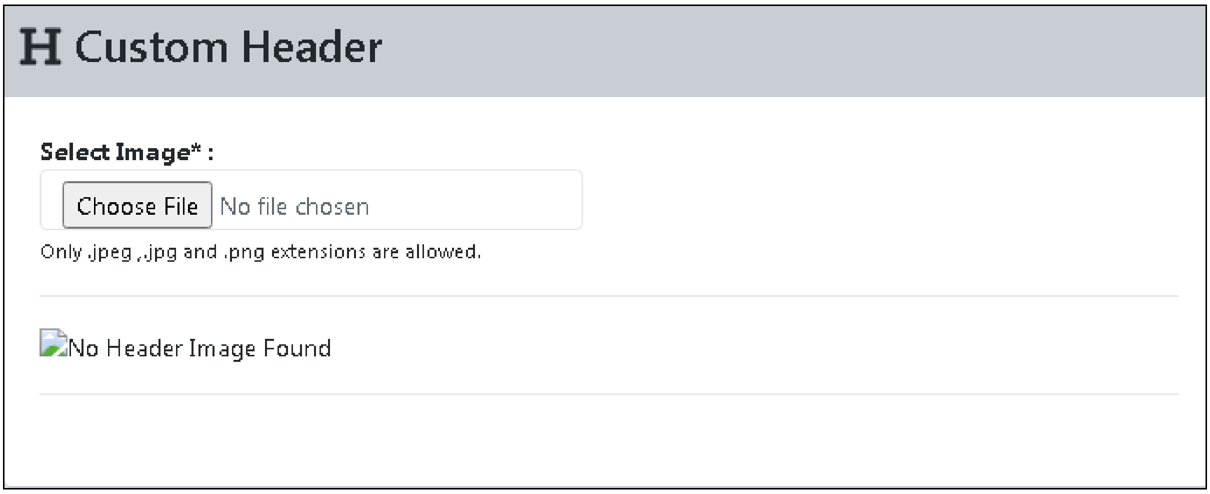
After filling all the details, click **Save**. A success message appears.

# Administration

The Administration module contains submodules which are **Customize Header** and **User Setting.**

## Customize Header

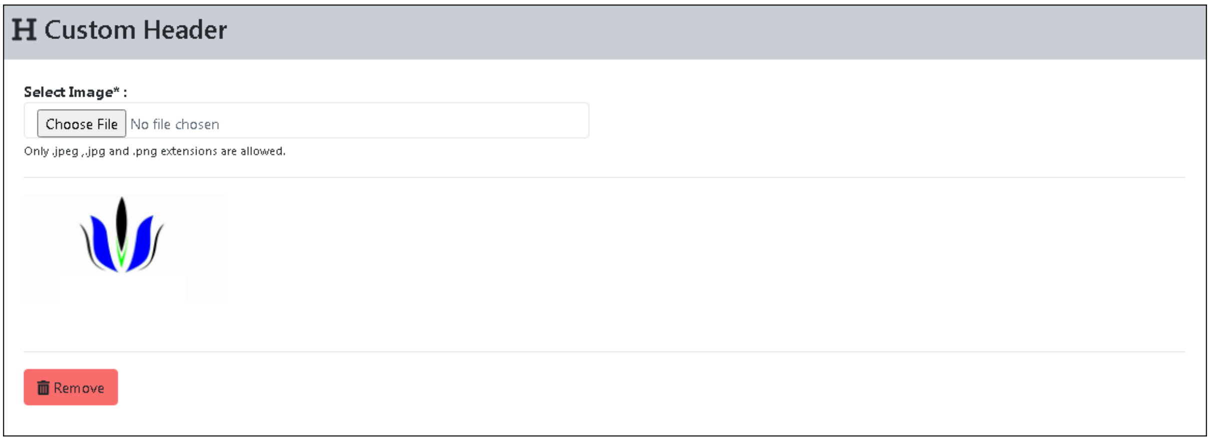
The Customize Header submodule helps you to customize the report header that appears on each page.



## Adding a Customize Header

To add a custom header, click **Choose File.**

File selection window appears. Select the header image as per requirement.



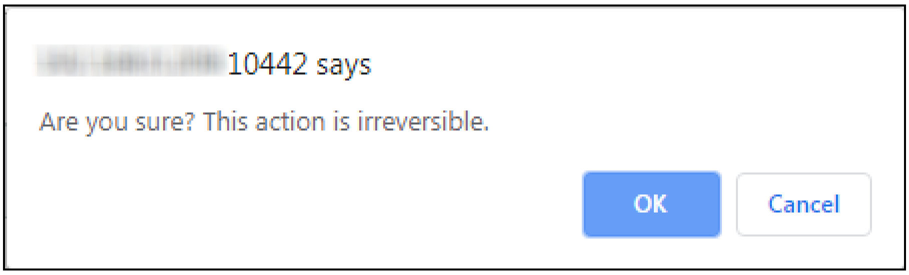
After uploading the file, the custom header appears on all future reports.

| NOTE | If the user does not set the customize header, then Nemasis PRO will generate a report with default Nemasis PRO header. |
|---|---|

# Removing the Customize Header

To delete the Custom Header, follow the steps given below:

1. To remove the custom header, click **Remove**.  
   A delete confirmation prompt appears.



[redacted] 10442 says

Are you sure? This action is irreversible.

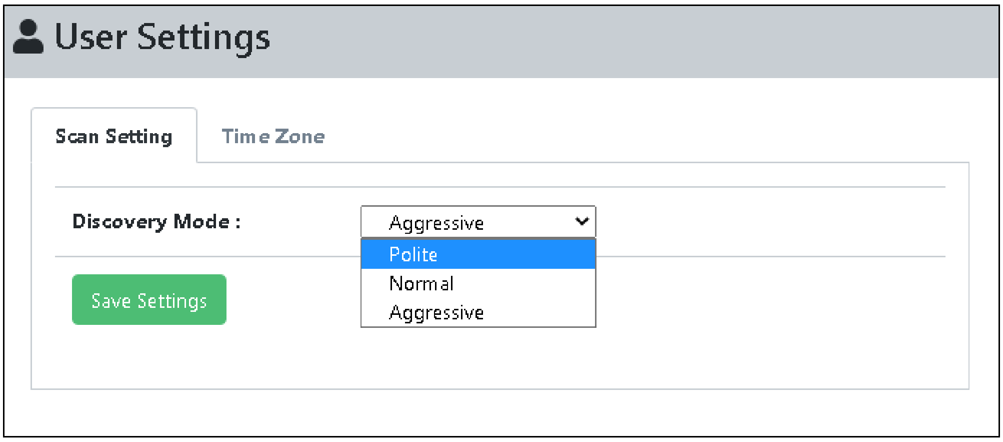
2. Click **OK**. The custom header will be deleted.

# User Settings

The User Settings submodule helps to configure the scan and time-zone settings. This consists of two tabs namely, **Scan Setting** and **Time Zone**.

## Scan Setting

This tab allows the administrator to configure the discovery mode of the scan.



User Settings

Discovery Mode : Aggressive

Nemasis PRO allows admin to set mode based on the following options:

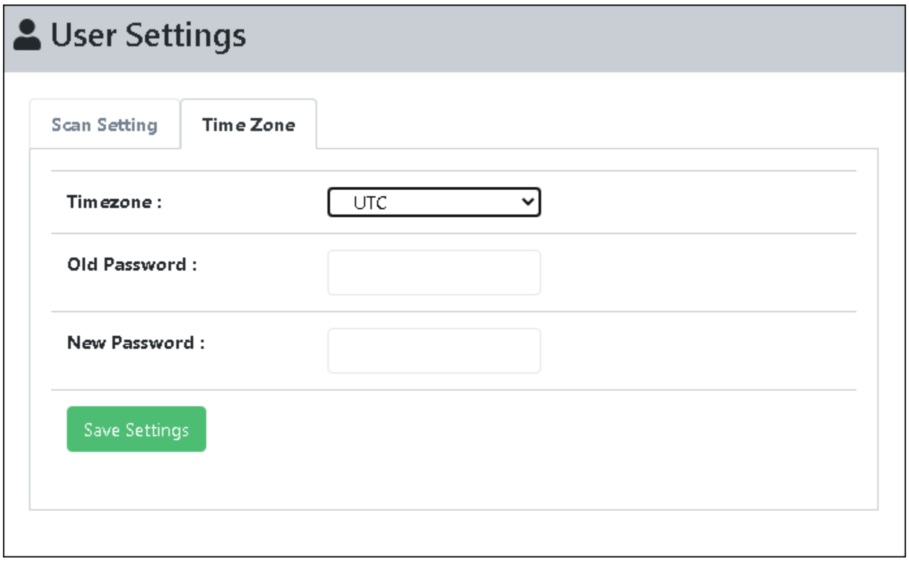
**Polite**: This option is slower than normal and intended to ease the load on the network.

**Normal**: This option is the standard scan behavior and does not affect the scan.

**Aggressive**: This option speeds up the scan and more resource-intensive. Using this option it is assumed that you are on a fast and reliable network. The scan delay is less than 10 ms.

# Time Zone

This tab allows the admin to select the time zone and also allows to change the password.



## User Settings

Timezone : UTC

Old Password :

New Password :

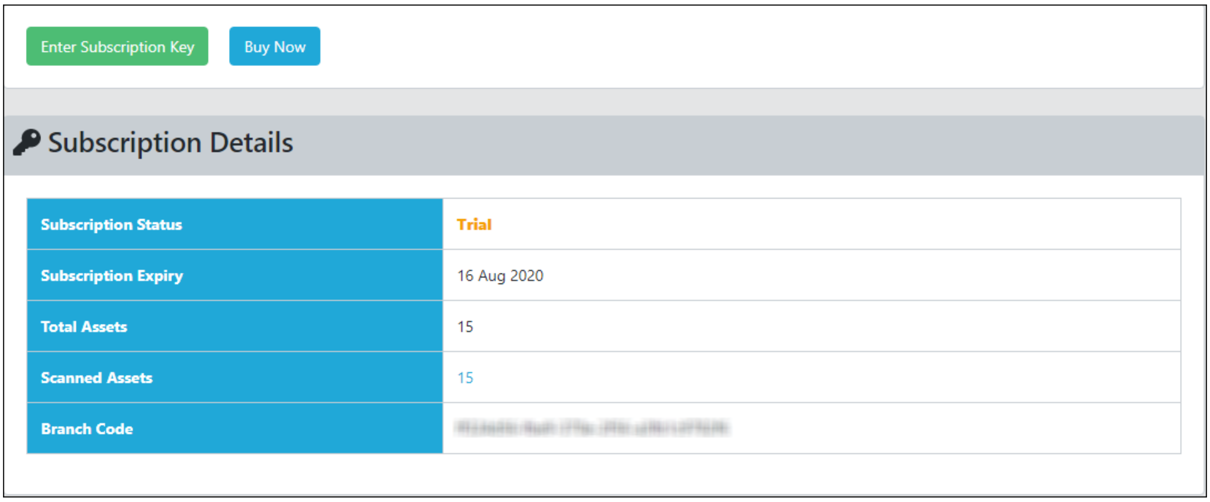
| NOTE | The **Time Zone** set by the user here will be displayed in the report generated by Nemasis PRO. |
|---|---|

# License

The License module has **Subscription Details** submodule, it consists of license information.

## Subscription Details

The Subscription Details submodule displays your license information. It shows your Subscription Status, Subscription Expiry, Total Assets, and Scanned Assets. The module also lets you enter the subscription key and buy a new license.



Subscription Details

| | |
|---|---|
| Subscription Status | Trial |
| Subscription Expiry | 16 Aug 2020 |
| Total Assets | 15 |
| Scanned Assets | 15 |
| Branch Code | [redacted] |

**Subscription Status:** It displays your subscription status (Trial, Active, or Trial Expired).

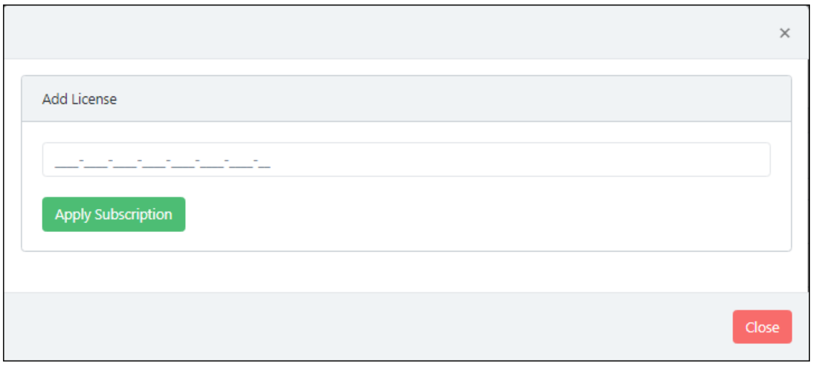
**Subscription Expiry:** It displays your subscription expiry date.

**Total Assets**: It displays the total number of assets you are allowed to scan.

**Scanned Assets:** It displays the total number of assets you have scanned. Clicking the numerical value displays a list of IP and MAC addresses you have scanned.

**Branch Code**: It will display the branch code that identifies the system.

**Enter Subscription Key:** To enter the subscription key for Nemasis PRO, click **Enter Subscription Key**. Add License pop-up window appears.



Enter the license key and then click **Apply Subscription**. A success message appears informing about successful registration.

**Buy Now:** The Trial version is valid for seven days and lets you scan 15 assets. If you have scanned 15 assets and want to scan more assets, you will have to buy a new license. To buy a new license, click **Buy Now**.

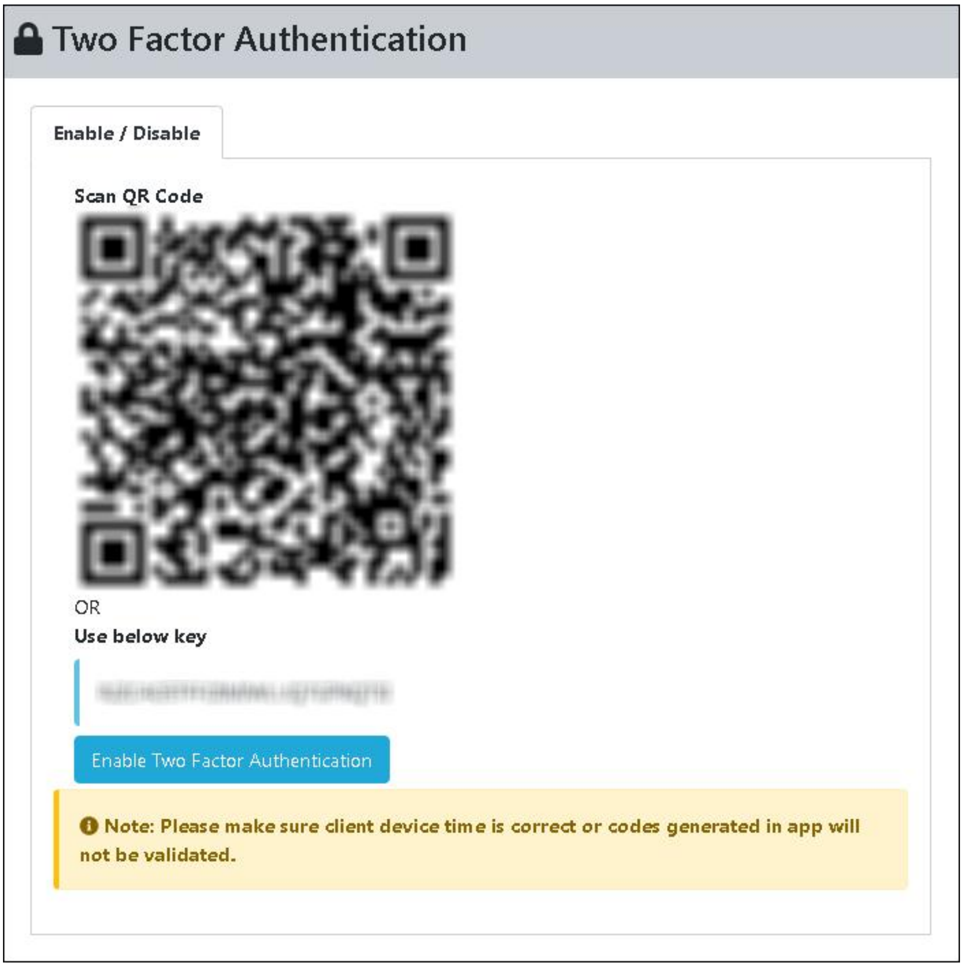
| | |
|---|---|
| **NOTE** | Nemasis PRO license will be for unlimited IPs (asset) for a particular period of time. Each asset can be scanned only 5 times. |

# Manage Instance

The Manage Instance module lets you to import and export the Nemasis PRO instance. It also has Two Factor Authentication along with lets user to get offline updates. The Manage Instance contains three submodules which are **Two Factor Auth. (2FA)**, **Import & Export**, and **Offline Update**.

## Two Factor Auth. (2FA)

The 2FA submodule lets user to add an extra layer of protection to the Nemasis PRO instance. This can be enabled by the admin of the system.



Two Factor Authentication

Scan QR Code

OR

Use below key

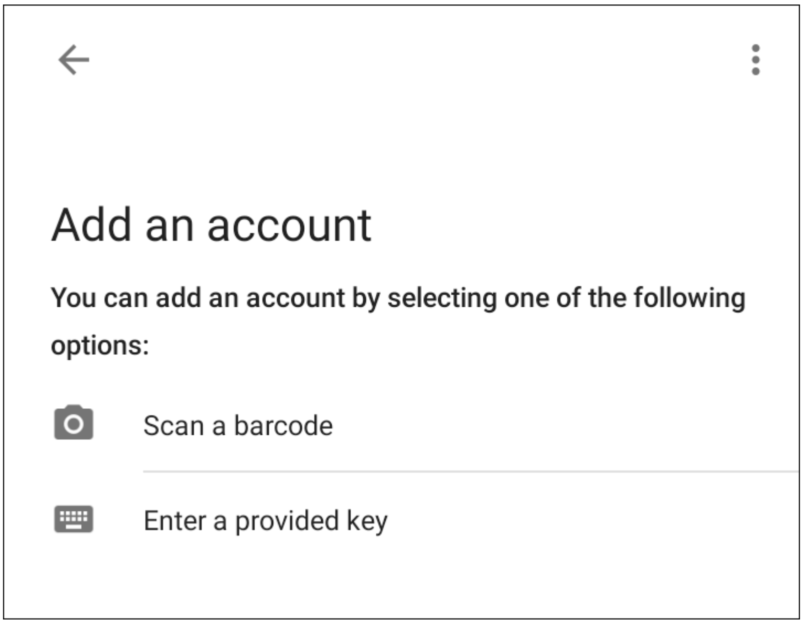
[redacted]

Note: Please make sure client device time is correct or codes generated in app will not be validated.

# Enabling 2FA

To enable 2FA, follow the following steps:

1. In the 2FA screen, scan the QR code or insert the code provided on the Nemasis PRO Console in the Authenticator app.



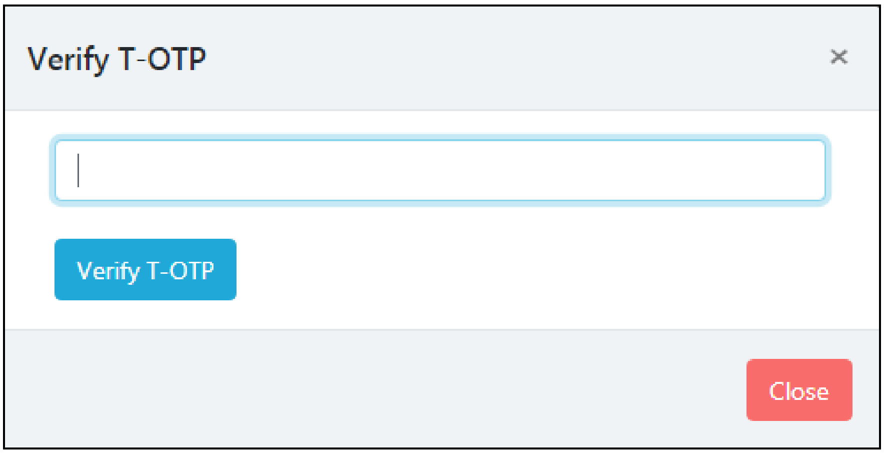
Add an account

You can add an account by selecting one of the following options:

Scan a barcode

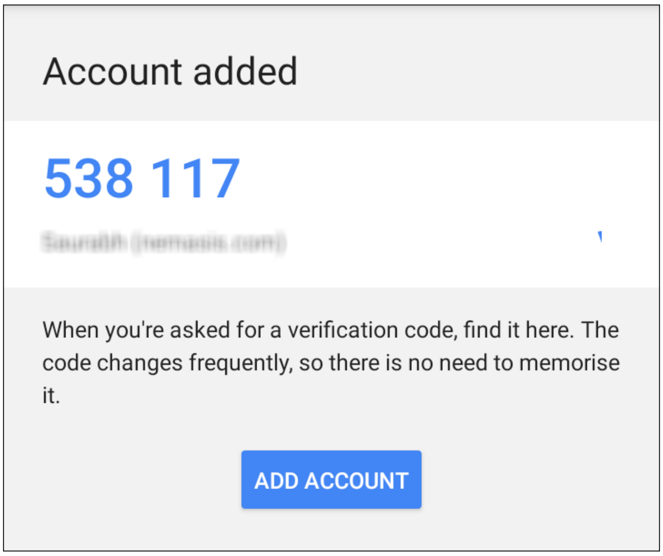
Enter a provided key

2. After scanning or entering the code, **Verify T-OTP** screen pops-up.



Verify T-OTP

3. Enter the OTP received on the Authenticator app.



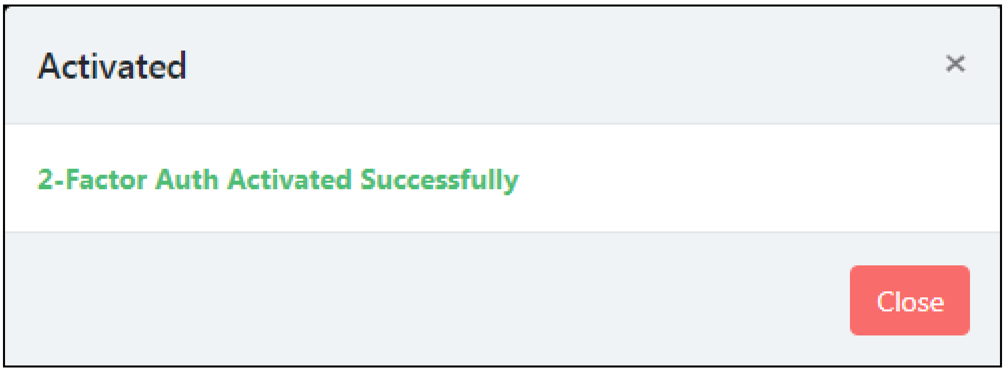
Account added

538 117

[redacted]

When you're asked for a verification code, find it here. The code changes frequently, so there is no need to memorise it.

4. After entering OTP, the 2FA feature will be enabled on the Nemasis PRO Instance with a success message.



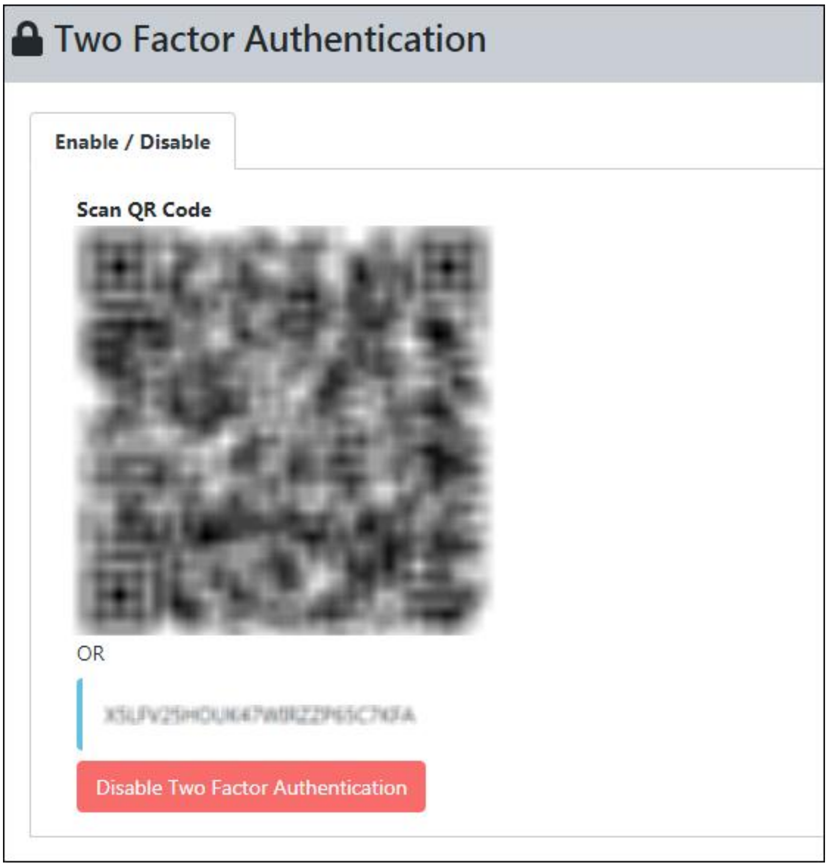
Activated

2-Factor Auth Activated Successfully

# Disabling 2FA

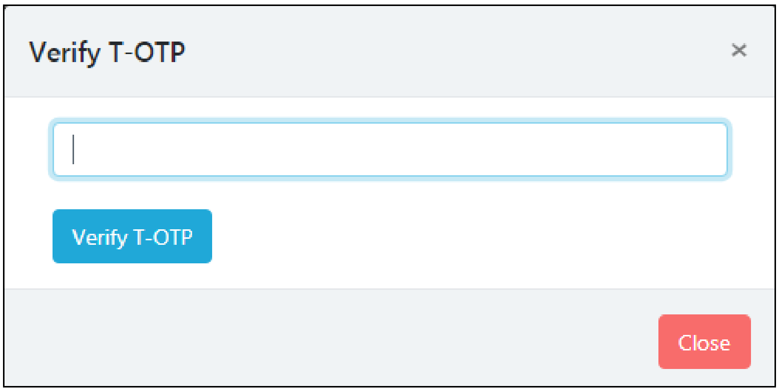
To disable 2FA, follow the following steps:

1. Go to the Two Factor Authentication page, click on **Disable Two Factor Authentication**.

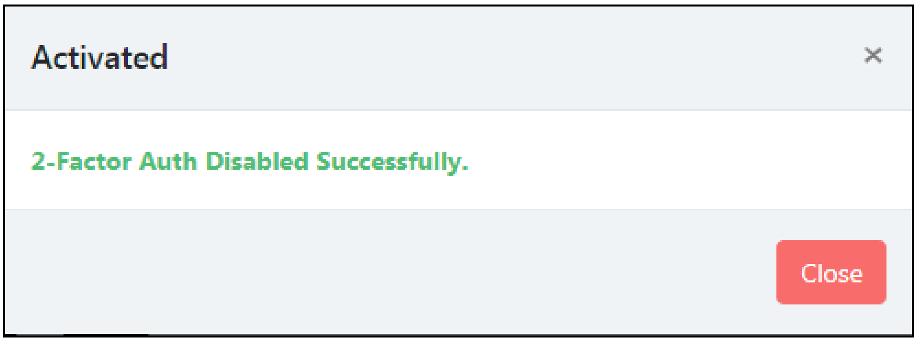


Two Factor Authentication

2. **Verify T-OTP** window pops-up.



3. After entering the OTP received. Click **Verify T-OTP**, the 2FA will be disabled with success message.



Activated

2-Factor Auth Disabled Successfully.

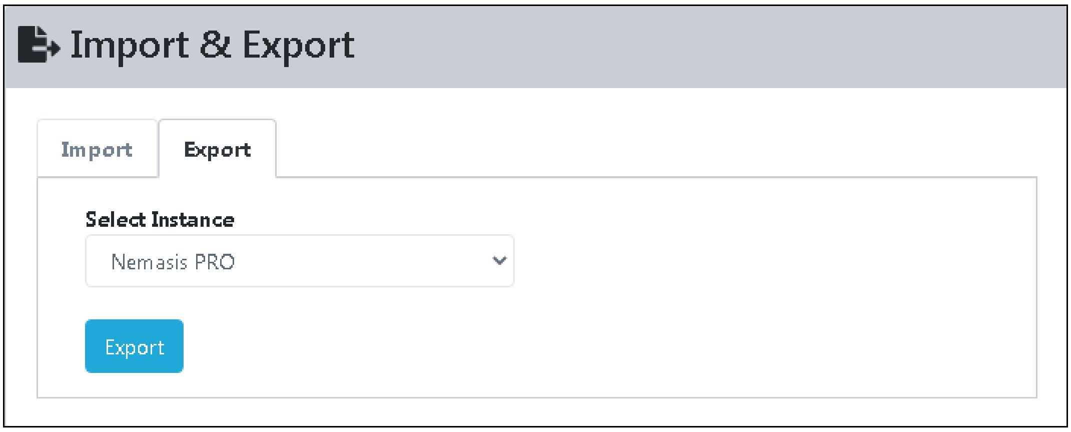
# Import & Export

The Import & Export submodule lets user to import and export the Nemasis PRO instance. This feature helps the organization to create a backup of the data of the instance and used in case of any disaster management or system failure.

## Exporting an Instance

To export a Nemasis PRO instance, follow the following steps:

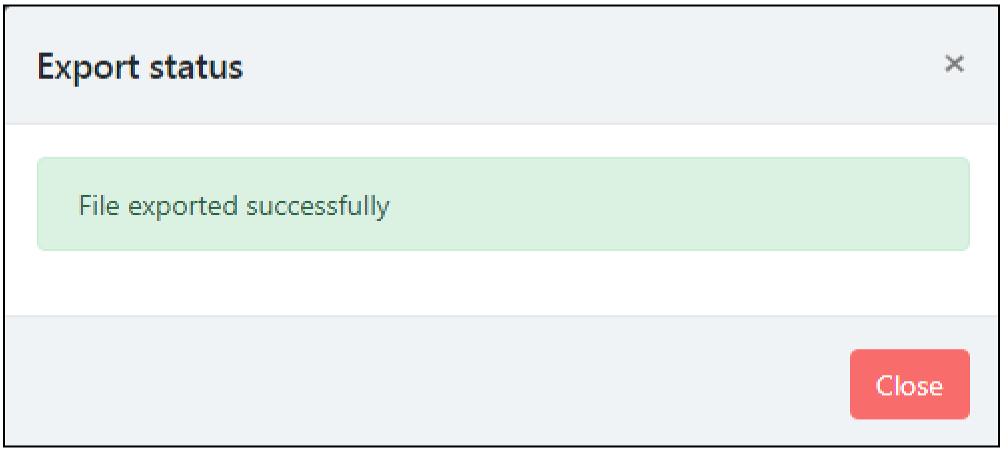
1. Select Instance Nemasis PRO from the **Export Setting** tab.



Import & Export

Select Instance: Nemasis PRO

2. After selecting the instance, click **Export**.
3. Once, the export is completed, you will get a successful message.



Export status

File exported successfully

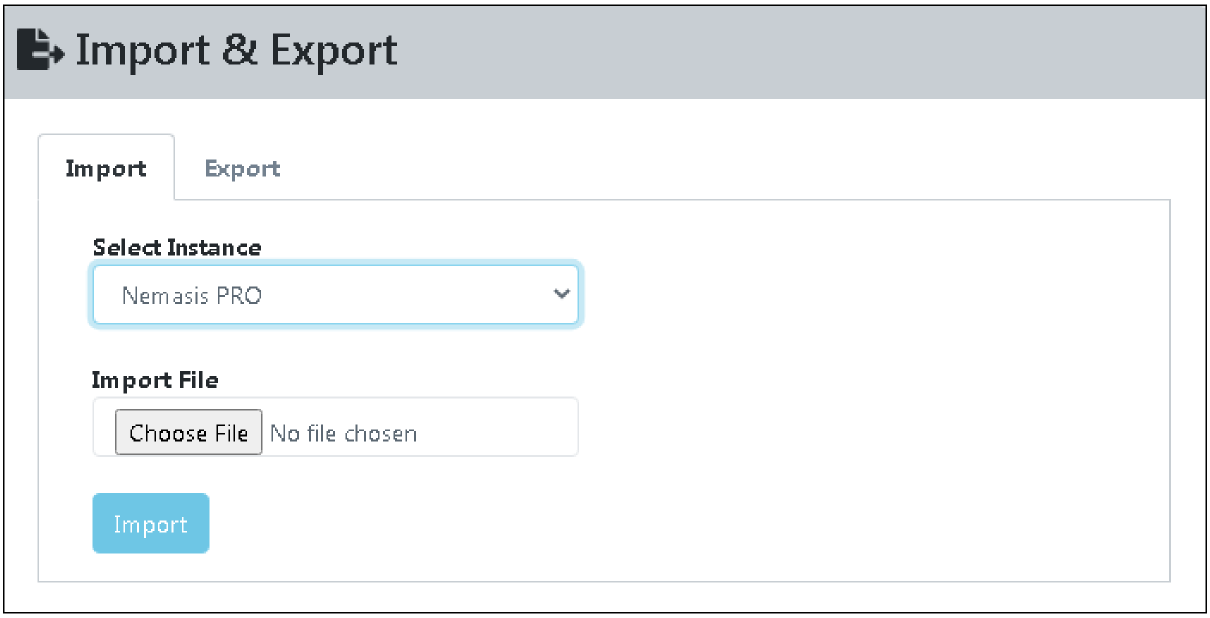
**4.** After the file is exported is successful, you can download the file by clicking

Click here to download exported file.

# Importing an instance

To import a Nemasis PRO instance, follow the following steps:

1. To import the instance, **Select Instance** from the dropdown menu (Nemasis PRO).

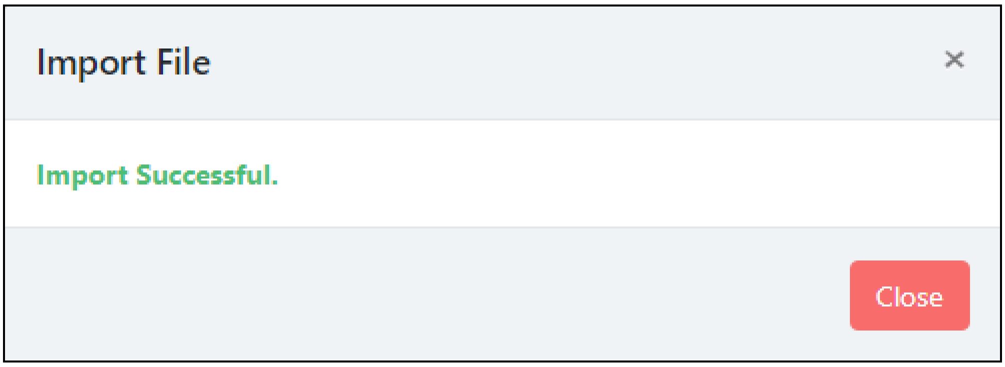


Import & Export

Select Instance: Nemasis PRO

Import File: No file chosen

2. After selecting the instance, choose the file to import. Click **Import** button
3. Once, the import is completed, you will get a successful pop-up.



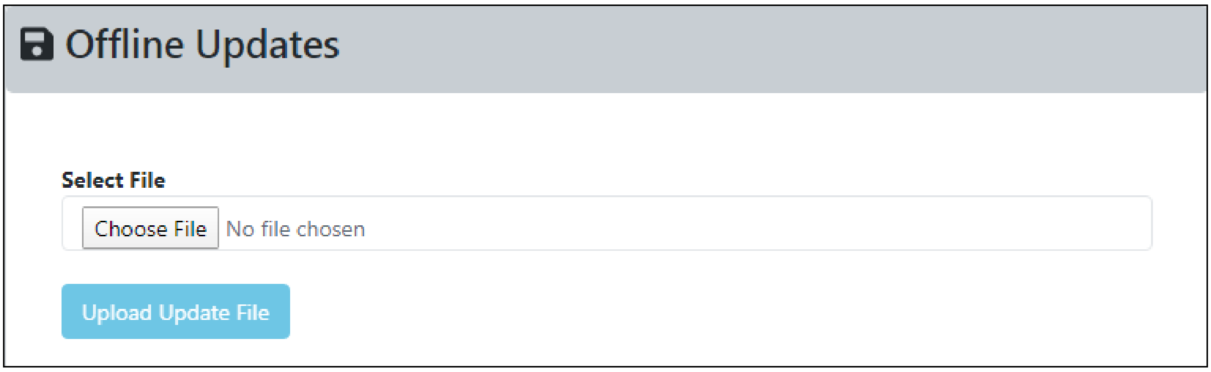
Import File

Import Successful.

# Offline Updates

The **Offline Updates** submodule helps users to update Nemasis PRO through offline mode for the air-gapped system. User can download the patch from other systems which is connected to the internet and can upload the patch to the Nemasis PRO instance.

With Offline Updates, you can update/upgrade the Nemasis PRO instance even if the trial period is over or license has expired.



| | |
|---|---|
| **NOTE** | Depending upon the component change, a running task may get interrupted. |

# Uploading Offline Updates

To upload the offline updates, perform the following steps:

1. Go to the link provided below, and then download the available update patch (in ZIP format).
2. After downloading the patch, click on the **Upload Update File**. This will update the Nemasis PRO instance through offline mode.

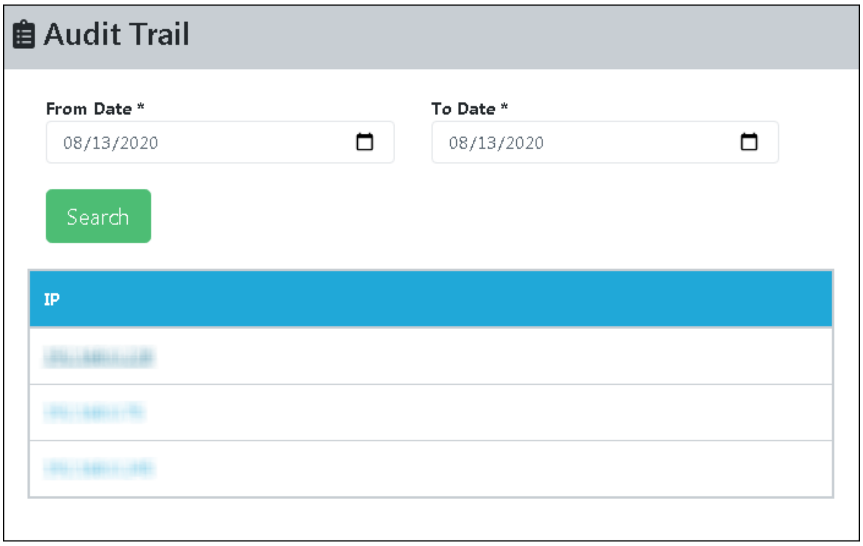
| | |
|---|---|
| **NOTE** | Link for the Offline Update:<br>**https://download1.mwti.net/nemasis/nemasis_update.zip** |

# Audit Trail

You can view the audit by using the IP address of the asset. You can also filter the audit based on the date and month on which audit was performed.

## Search Audit Trail

1. Select the range date in the **From Date** and **To Date** fields.
2. Click **Search**. You will get the list of audit reports of different IPs.



Audit Trail

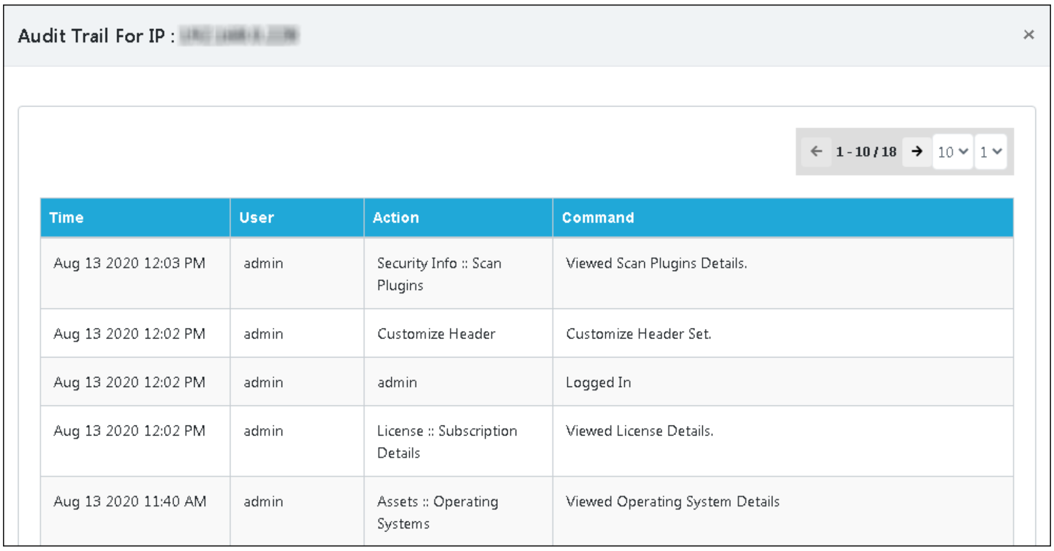
From Date * 08/13/2020

To Date * 08/13/2020

Search

| IP |
|---|
| [redacted] |
| [redacted] |
| [redacted] |

3. Click on the IP address for which you want to view the audit, you will get the detailed view of the audit.



Audit Trail For IP : [redacted]

| Time | User | Action | Command |
|---|---|---|---|
| Aug 13 2020 12:03 PM | admin | Security Info :: Scan Plugins | Viewed Scan Plugins Details. |
| Aug 13 2020 12:02 PM | admin | Customize Header | Customize Header Set. |
| Aug 13 2020 12:02 PM | admin | admin | Logged In |
| Aug 13 2020 12:02 PM | admin | License :: Subscription Details | Viewed License Details. |
| Aug 13 2020 11:40 AM | admin | Assets :: Operating Systems | Viewed Operating System Details |

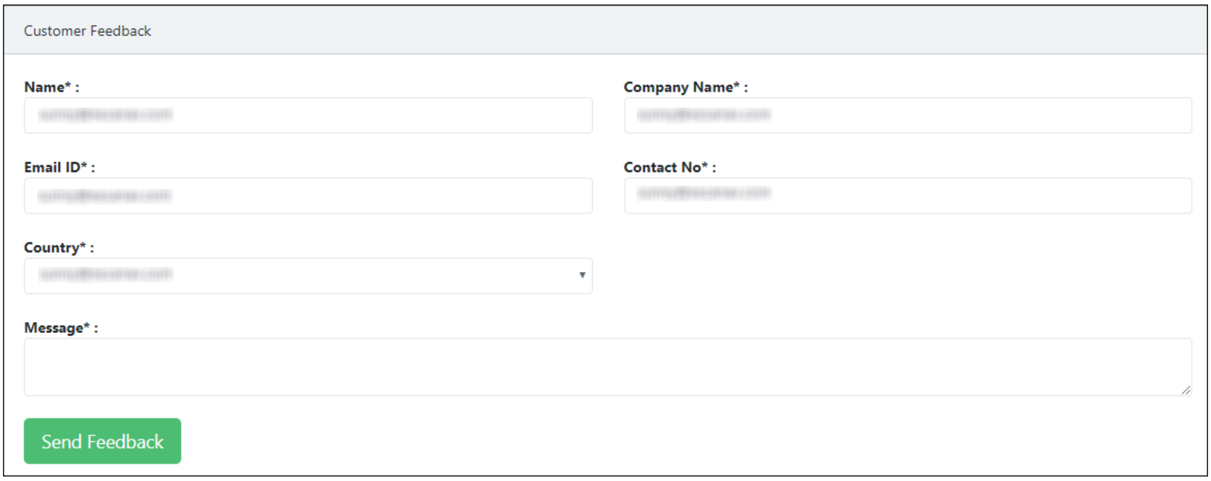
4. Users can view details like time, user, action, and command in the audit trail.

# Help & Support

The Help and Support module contains **Feedback** and **Support Request** submodules.

## Feedback

The Feedback submodule lets you send feedback about Nemasis PRO.



Customer Feedback

Name* :

Company Name* :

Email ID* :

Contact No* :

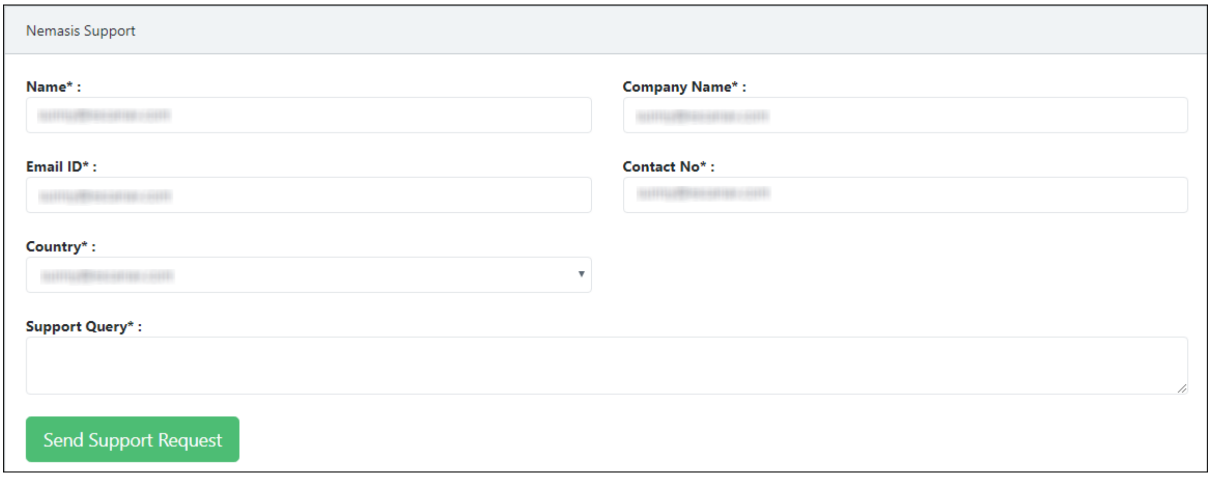
Country* :

Message* :

Your personal details are auto-filled by Nemasis PRO. Enter your feedback in the Message field and then click **Send Feedback**.

## Support Request

The Support Request submodule lets you send a support request.



Nemasis Support

Name* :

Company Name* :

Email ID* :

Contact No* :

Country* :

Support Query* :

Your personal details are auto-filled by Nemasis PRO. Enter your message in the Support Query field and then click **Send Support Request**. After receiving the support request, the Nemasis PRO Support Team will get in touch with you as soon as possible.

# Contact Us

We offer 24x7 free online technical support to our customers through email and live chat. We also provide free telephonic support to our customers during our business hours.

Before you contact the technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Ensure that you have the following information when you contact technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software, and network changes if any carried out
- Step by step description of error/situation
- Screenshots, error messages and log files
- Step by step description of troubleshooting if any attempted

In case you want the Technical Support team to take a remote connection:

- Root password set during Nemasis PRO installation
- IP address of the Nemasis PRO installed endpoint

## Chat Support

The Nemasis PRO technical support team is available round-the-clock to assist you with your queries. You can contact our support team via live chat by clicking **here**.

## E-mail Support

If you have any queries, suggestions, and comments regarding Nemasis PRO or this User Guide, please write to us at support@nemasisva.com